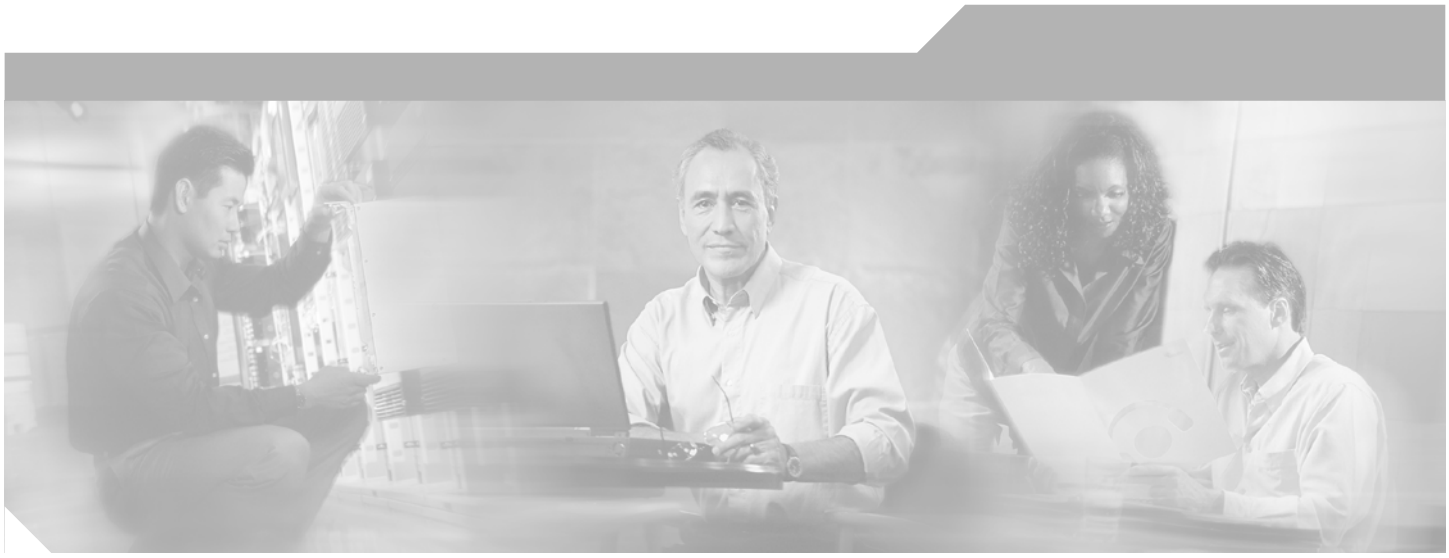
CISCO SYSTEMS



Catalyst 6500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド

Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide

リリース 12.2(18)SXF とリビルド、および以前のリリース

Text Part Number: OL-3999-08-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。

Catalyst 6500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド リリース 12.2SXF とリビルド、および以前のリリース

はじめに

ここでは、『*Catalyst 6500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド リリース 12.2SXF*』の対象読者、マニュアルの構成、および手順や情報を記述するための表記法について説明します。

対象読者

このマニュアルは、Catalyst 6500 シリーズ スイッチの設定およびメンテナンスを担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	製品の概要	Catalyst 6500 シリーズ スイッチの概要について説明します。
第 2 章	コマンドライン インターフェイス（CLI）	Command-Line Interface（CLI; コマンドライン インターフェイス）について説明します。
第 3 章	スイッチの初期設定	基本的な設定の実行方法について説明します。
第 4 章	Supervisor Engine 720 の設定	Supervisor Engine 720 の設定方法について説明します。
第 5 章	Supervisor Engine 32 の設定	Supervisor Engine 32 の設定方法について説明します。
第 6 章	Supervisor Engine 2 およびスイッチ ファブリック モジュール（SFM）の設定	Supervisor Engine 2 およびスイッチ ファブリック モジュールの設定について説明します。
第 7 章	NSF with SSO スーパーバイザ エンジンの冗長構成の設定	NSF with SSO スーパーバイザ エンジンの冗長構成を設定する手順について説明します。

章	タイトル	説明
第 8 章	Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定	Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成を設定する手順について説明します。
第 9 章	インターフェイスの設定	LAN インターフェイス上で、特定のレイヤに限定されない機能を設定する手順について説明します。
第 10 章	レイヤ 2 スイッチング用 LAN ポートの設定	レイヤ 2 機能（Virtual LAN（VLAN; 仮想 LAN）トランクなど）をサポートするように LAN インターフェイスを設定する手順について説明します。
第 11 章	Flex Link の設定	Flex Link を設定する手順について説明します。
第 12 章	EtherChannel の設定	レイヤ 2 およびレイヤ 3 EtherChannel ポート バンドルを設定する手順について説明します。
第 13 章	VLAN トランキング プロトコル（VTP）の設定	VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を設定する手順について説明します。
第 14 章	仮想 LAN（VLAN）の設定	VLAN を設定する手順について説明します。
第 15 章	プライベート VLAN の設定	プライベート VLAN を設定する手順について説明します。
第 16 章	Cisco IP Phone サポートの設定	Cisco IP Phone のサポートを設定する手順について説明します。
第 17 章	IEEE 802.1Q トンネリングの設定	IEEE 802.1Q トンネリングを設定する手順について説明します。
第 18 章	レイヤ 2 プロトコル トンネリングの設定	レイヤ 2 プロトコル トンネリングを設定する手順について説明します。
第 19 章	標準準拠 IEEE Multiple Spanning Tree（MST）の設定	標準準拠 IEEE Multiple Spanning Tree（MST）を設定する手順について説明します。
第 20 章	スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定	Spanning Tree Protocol（STP; スパニング ツリー プロトコル）および先行標準 IEEE 802.1s Multiple Spanning Tree（MST）プロトコルを設定する手順について説明します。
第 21 章	オプションのスパニング ツリー プロトコル（STP）機能の設定	STP の PortFast、UplinkFast、および BackboneFast 機能を設定する手順について説明します。
第 22 章	レイヤ 3 インターフェイスの設定	レイヤ 3 機能をサポートするように LAN インターフェイスを設定する手順について説明します。
第 23 章	単一方向イーサネット（UDE）および単一方向リンク ルーティング（UDLR）の設定	Unidirectional Ethernet（UDE; 単一方向イーサネット）および Unidirectional Link Routing（UDLR; 単一方向のリンク ルーティング）を設定する手順について説明します。
第 24 章	ポリシー フィーチャ カード（PFC）3BXL および PFC3B モード マルチプロトコル ラベル スイッチング（MPLS）の設定	PFC3BXL または PFC3B Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を設定する方法について説明します。

章	タイトル	説明
第 25 章	IPv4 マルチキャスト VPN（MVPN）サポートの設定	IPv4 Multicast Virtual Private Network（MVPN; マルチキャスト バーチャル プライベート ネットワーク）サポートを設定する手順について説明します。
第 26 章	IP ユニキャスト レイヤ 3 スイッチングの設定	IP ユニキャスト レイヤ 3 スイッチングを設定する手順について説明します。
第 27 章	IPv6 マルチキャスト PFC3 および DFC3 レイヤ 3 スイッチングの設定	IPv6 Multicast Multilayer Switching（MMLS; マルチキャスト マルチレイヤ スイッチング）を設定する手順について説明します。
第 28 章	IPv4 マルチキャスト レイヤ 3 スイッチングの設定	IPv4 マルチキャスト マルチレイヤ スイッチング（MMLS）を設定する手順について説明します。
第 29 章	IPv6 マルチキャスト トラフィック用の Multcast Listener Discovery version 2（MLDv2）スヌーピングの設定	Multicast Listener Discovery version 2（MLDv2）スヌーピングを設定する手順について説明します。
第 30 章	IPv4 マルチキャスト トラフィック用インターネット グループ管理プロトコル（IGMP）スヌーピングの設定	Internet Group Management Protocol（IGMP）スヌーピングを設定する手順について説明します。
第 31 章	Protocol Independent Multicast（PIM）スヌーピングの設定	Protocol Independent Multicast（PIM）スヌーピングを設定する手順について説明します。
第 32 章	Router-Port Group Management Protocol（RGMP）の設定	Router-Port Group Management Protocol（RGMP）を設定する手順について説明します。
第 33 章	ネットワーク セキュリティの設定	Catalyst 6500 シリーズ スイッチ固有のネットワーク セキュリティ機能を設定する手順について説明します。
第 34 章	Cisco IOS ACL サポートの概要	Catalyst 6500 シリーズ スイッチが Cisco IOS Access Control List（ACL; アクセス制御リスト）をサポートする手順について説明します。
第 35 章	VLAN アクセス制御リスト（VACL）の設定	VLAN ACL（VACL）を設定する手順について説明します。
第 36 章	サービス拒絶（DoS）からの保護の設定	Denial of Service（DoS; サービス拒絶）からの保護を設定する手順について説明します。
第 37 章	Dynamic Host Configuration Protocol（DHCP）スヌーピングの設定	Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する手順について説明します。
第 38 章	ダイナミック ARP 検査の設定	Dynamic ARP Inspection（DAI; ダイナミック ARP 検査）を設定する手順について説明します。
第 39 章	トラフィック ストーム制御の設定	トラフィック ストーム制御を設定する手順について説明します。
第 40 章	不明なユニキャスト/マルチキャスト フラッディングのブロック	Unknown Unicast Flood Blocking（UUFB; 不明なユニキャスト フラッディングのブロック）を設定する手順について説明します。
第 41 章	PFC QoS の設定	Quality of Service（QoS; サービス品質）を設定する手順について説明します。
第 42 章	PFC3BXL または PFC3B モード MPLS QoS の設定	MPLS QoS を設定する手順について説明します。

章	タイトル	説明
第 43 章	PFC QoS 統計データ エクスポートの設定	PFC QoS 統計データ エクスポートを設定する手順について説明します。
第 44 章	Cisco IOS ファイアウォール フィーチャ セットの設定	Cisco IOS ファイアウォール フィーチャ セットを設定する手順について説明します。
第 45 章	Network Admission Control（NAC）の設定	Network Admission Control（NAC）を設定する手順について説明します。
第 46 章	IEEE 802.1X ポートベースの認証の設定	IEEE 802.1X ポートベースの認証を設定する手順について説明します。
第 47 章	ポート セキュリティの設定	ポート セキュリティを設定する手順について説明します。
第 48 章	CDP の設定	Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）を設定する手順について説明します。
第 49 章	単一方向リンク検出（UDLD）の設定	UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する手順について説明します。
第 50 章	NetFlow の設定	NetFlow テーブルの設定方法について説明します。
第 51 章	NetFlow データ エクスポート（NDE）の設定	NetFlow Data Export（NDE; NetFlow データ エクスポート）を設定する手順について説明します。
第 52 章	ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定	Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を設定する手順について説明します。
第 53 章	SNMP ifIndex の持続性の設定	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ifIndex の持続性を設定する手順について説明します。
第 54 章	電源管理および環境モニタ	電源管理および環境モニタ機能を設定する手順について説明します。
第 55 章	総合オンライン診断の設定	オンライン診断を設定する手順、および診断テストを実施する手順について説明します。
第 56 章	Web Cache Communication Protocol（WCCP）による Web キャッシュ サービスの設定	Web Cache Communication Protocol（WCCP）を設定する手順について説明します。
第 57 章	ユーティリティの使用上位 N	Top N ユーティリティの使用方法について説明します。
第 58 章	レイヤ 2 traceroute ユーティリティの使用	レイヤ 2 traceroute ユーティリティの使用方法について説明します。
付録 A	オンライン診断テスト	オンライン診断テストの使用方法に関する推奨事項について説明します。
付録 B	略語	このマニュアルで使用している略語の定義を示します。

関連資料

Catalyst 6500 シリーズ スイッチの関連資料は、次のとおりです。

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Cisco IOS Master Command List*, Release 12.2SX
- *Catalyst 6500 Series Switch Cisco IOS System Message Guide*, Release 12.2SX
- *Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*
- *Cisco IOS コンフィギュレーション ガイドおよびコマンド リファレンス* - Catalyst 6500 シリーズ スイッチのマニュアルで説明されていない Cisco IOS ソフトウェア機能を設定する場合には、次のマニュアルを使用してください。
  - 『*Configuration Fundamentals Configuration Guide*』
  - 『*Configuration Fundamentals Command Reference*』
  - 『*Bridging and IBM Networking Configuration Guide*』
  - 『*Bridging and IBM Networking Command Reference*』
  - 『*Interface Configuration Guide*』
  - 『*Interface Command Reference*』
  - 『*Network Protocols Configuration Guide*』Part 1、2、3
  - 『*Network Protocols Command Reference*』Part 1、2、3
  - 『*Security Configuration Guide*』
  - 『*Security Command Reference*』
  - 『*Switching Services Configuration Guide*』
  - 『*Switching Services Command Reference*』
  - 『*Voice, Video, and Home Applications Configuration Guide*』
  - 『*Voice, Video, and Home Applications Command Reference*』
  - 『*Software Command Summary*』
  - 『*Software System Error Messages*』
  - 『*Debug Command Reference*』
  - 『*Internetwork Design Guide*』
  - 『*Internetwork Troubleshooting Guide*』
  - 『*Configuration Builder Getting Started Guide*』

  Cisco IOS コンフィギュレーション ガイドおよびコマンド リファレンスは、次の URL から入手できます。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm
- MIB（管理情報ベース）については、次の URL を参照してください。

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

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、コマンド オプションおよびキーワードは**太字**で示しています。
イタリック体	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。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、**太字の `screen` フォント**で示しています。
イタリック体の `screen` フォント	ユーザが値を指定する引数は、*イタリック体の `screen` フォント*で示しています。
⟶	このポインタは、例の中の重要な行を強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワード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）は、次のように表しています。

（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。

注意は、次のように表しています。

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。

マニュアルの入手方法およびテクニカル サポート

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

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

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

製品の概要

この章で説明する内容は、次のとおりです。

サポートされるハードウェアおよびソフトウェア

Catalyst 6500 シリーズ スイッチがサポートするシャーシ、モジュール、およびソフトウェア機能の詳細については、『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm

ユーザ インターフェイス

Release 12.2SX では、次のインターフェイスを使用する設定をサポートします。

- Command-Line Interface（CLI; コマンドライン インターフェイス）- 第 2 章「コマンドライン インターフェイス（CLI）」を参照してください。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2 および『*Command Reference*』を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm
- Cisco IOS Web ブラウザ インターフェイス - 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using the Cisco Web Browser」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf005.html
- Embedded Cisco View - 「Embedded CiscoView サポートの設定」（P.1-2）を参照してください。

Embedded CiscoView サポートの設定

ここでは、Embedded CiscoView サポートの設定について説明します。

Embedded CiscoView の概要

Embedded CiscoView ネットワーク管理システムとは、スイッチのグラフィック表示と、GUI ベースの管理およびコンフィギュレーション インターフェイスを提供するために、HTTP および SNMP を使用する Web ベースのインターフェイスです。次の URL にある Embedded CiscoView の Java Archive（JAR）ファイルをダウンロードできます。

http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi

Embedded CiscoView のインストールおよび設定

Embedded CiscoView をインストールするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dir device_name`	装置の内容を表示します。 初めて Embedded CiscoView をインストールする場合、または CiscoView ディレクトリが空の場合、ステップ 4 へスキップします。
ステップ 2	`Router# delete device_name:cv/*`	CiscoView ディレクトリから既存のファイルを削除します。
ステップ 3	`Router# squeeze device_name:`	ファイルシステム内にスペースを確保します。
ステップ 4	`Router# archive tar /xtract tftp://ip_address_of_tftp_server/ciscoview.tar device_name:cv`	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上の tar ファイルから CiscoView ディレクトリに、CiscoView ファイルを抽出します。
ステップ 5	`Router# dir device_name:`	装置の内容を表示します。 冗長構成では、冗長スーパーバイザ エンジンのファイル システムごとに ステップ 1 ～ ステップ 5 を繰り返します。
ステップ 6	`Router# configure terminal`	グローバル 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	`Router(config)# ip http server`	HTTP Web サーバをイネーブルにします。
ステップ 8	`Router(config)# snmp-server community string ro`	読み取り専用操作用に、SNMP パスワードを設定します。
ステップ 9	`Router(config)# snmp-server community string rw`	読み取りおよび書き込み操作用に、SNMP パスワードを設定します。

（注）　スイッチの Web ページにアクセスするデフォルト パスワードは、スイッチのイネーブル レベル パスワードです。

スイッチへの Web アクセスの詳細については、次の URL にある IOS の『*Configuration Fundamentals Configuration Guide*』の「Using the Cisco Web Browser」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf005.html

Embedded CiscoView 情報の表示

Embedded CiscoView 情報を表示するには、次の EXEC コマンドを入力します。

コマンド	目的
`Router# show ciscoview package`	Embedded CiscoView ファイルに関する情報を表示します。
`Router# show ciscoview version`	Embedded CiscoView のバージョンを表示します。

PFC および DFC によりハードウェアでサポートされるソフトウェア機能

ここでは、Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）、Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）、Distributed Forwarding Card 3（DFC3）、および Distributed Forwarding Card（DFC）で提供されているハードウェア サポートについて説明します。

- 「PFC3、PFC2、DFC3、および DFC によりハードウェアでサポートされるソフトウェア機能」（P.1-3）
- 「PFC3 および DFC3 によりハードウェアでサポートされるソフトウェア機能」（P.1-4）

PFC3、PFC2、DFC3、および DFC によりハードウェアでサポートされるソフトウェア機能

PFC3、PFC2、DFC3、および DFC は、Cisco IOS ソフトウェア機能に次のハードウェア サポートを提供します。

- レイヤ 3 ポートおよび VLAN インターフェイスの Access Control List（ACL; アクセス制御リスト）
  - 入出力標準 ACL および拡張 ACL のアクションを、許可および拒否します。

    （注）　ACL ロギングを必要とするフローは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）のソフトウェアで処理されます。

  - MPLS インターフェイスを除き、セッション内の最初のパケットよりあとの再帰 ACL フローが、MSFC のソフトウェアで処理されます。
  - ダイナミック ACL フロー

    （注）　アイドル タイムアウトは MSFC のソフトウェアで処理されます。

ACL の PFC および DFC サポートの詳細については、第 34 章「Cisco IOS ACL サポートの概要」を参照してください。

ACL 設定の詳細については、次の URL にある『Cisco IOS Security Configuration Guide』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm

- VLAN ACL（VACL）- VACL を設定するには、第 35 章「VLAN アクセス制御リスト（VACL）の設定」を参照してください。
- **match ip address**、**set ip next-hop**、**ip default next-hop** Policy-Based Routing（PBR; ポリシー ベース ルーティング）キーワードを使用するルート マップ シーケンス用の PBR。

  PBR の設定については、次の URL にある『*Cisco IOS Quality of Service Solutions Configuration Guide*』Release 12.2 の「Classification」、「Configuring Policy-Based Routing」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfpbr.htm

  （注）　MSFC3 アドレスが PBR ACL 範囲内にある場合、MSFC3 にアドレス指定されたトラフィックは MSFC3 に転送されずに、ハードウェアでポリシー ルーティングされます。MSFC3 にアドレス指定されたトラフィックをポリシー ルーティングしないようにするには、MSFC3 にアドレス指定されたトラフィックを拒否するように PBR ACL を設定します。

- MPLS インターフェイス上を除く TCP インターセプト - TCP インターセプトを設定するには、「TCP インターセプトの設定」（P.33-2）を参照してください。
- ファイアウォール フィーチャ セット イメージでは、次の機能が可能です。
  - Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）- PFC は、CBAC が MSFC ソフトウェアに適用されている MSFC に対して CBAC を必要とするフローを方向付ける NetFlow テーブルにエントリを追加します。
  - 認証プロキシ - MSFC での認証後、PFC は認証ポリシー用の TCAM サポートを提供します。
  - Port-to-Application Mapping（PAM; ポート ツー アプリケーション マッピング）- PAM は MSFC のソフトウェアで実行されます。

  ファイアウォール機能を設定するには、第 44 章「Cisco IOS ファイアウォール フィーチャ セットの設定」を参照してください。
- ハードウェア補助の NetFlow アグリゲーション - 次の URL を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1081085

PFC3 および DFC3 によりハードウェアでサポートされるソフトウェア機能

PFC3 および DFC3 は、Cisco IOS ソフトウェア機能に次のハードウェア サポートを提供します。

- ハードウェアの双方向 Protocol Independent Multicast（PIM）- 「IPv4 双方向 PIM の機能概要」（P.28-8）を参照してください。
- 複数パスのユニキャスト Reverse Path Forwarding（RPF）チェック - ユニキャスト RPF チェックを設定するには、「ユニキャスト RPF チェックの設定」（P.33-2）を参照してください。

- MPLS インターフェイス上を除く、IPv4 ユニキャストおよびマルチキャスト トラフィックの Network Address Translation（NAT; ネットワーク アドレス変換）

  次のハードウェア補助の NAT 情報に注意してください。

  - UDP トラフィックの NAT は、PFC3BXL モードまたは PFC3B モードでのみサポートされます。
  - PFC3 は、マルチキャスト トラフィックの NAT をサポートしません。
  - PFC3 は、長さを指定するルート マップが設定されている NAT をサポートしません。
  - インターフェイスで NAT および NDE を設定する場合、PFC3 はフラグメント化されたパケット内のトラフィックをすべて MSFC3 に送信して、ソフトウェアで処理させます（CSCdz51590）。

  NAT を設定する方法については、次の URL にある『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」、「Configuring IP Addressing」、「Configuring Network Address Translation」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfipadr.htm#1042290

  Denial of Service（DoS; サービス拒絶）攻撃または設定ミスにより、莫大な量の NAT トラフィックが MSFC3 に送信されないようにするには、次の URL で説明されている **mls rate-limit unicast acl** {**ingress** | **egress**} コマンドを入力します。

  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_m2.html#mls_rate-limit_unicast_acl

  （CSCea23296）

- Release12.2(18)SXE 以降のリリースでの、IPv4 Multicast over Point-to-Point Generic Routing Encapsulation（GRE; 総称ルーティング カプセル他）トンネル - 次の URL にあるマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflogin.htm

  Release 12.2(18)SXE よりも前のリリースでは、IPv4 Multicast over point-to-point GRE トンネルが MSFC 上のソフトウェアでサポートされています。

（注） PFC3 は、**tunnel key** コマンドで設定されるトンネル用にハードウェアを加速しません。

- GRE トンネリングおよび IP トンネリングの IP - PFC3 および DFC3 は、次の **tunnel** コマンドをサポートします。
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  MSFC3 のソフトウェアで処理されるその他のサポート対象トンネリング タイプ

  tunnel ttl コマンド（デフォルト 255）は、カプセル化されたパケットの Time to Live（TTL）を設定します。

tunnel tos コマンドが存在する場合は、パケットがカプセル化されるときの Type of Service（ToS; サービス タイプ）バイトを設定します。**tunnel tos** コマンドが存在せず Quality of Service（QoS; サービス品質）がイネーブルでない場合、パケットの ToS バイトが、パケットをカプセル化するときの ToS バイトを設定します。**tunnel tos** コマンドが存在せず QoS がイネーブルの場合、PFC QoS により変更されたパケットの ToS バイトが、パケットをカプセル化するときの ToS バイトを設定します。

GRE トンネリングおよび IP トンネリングの IP を設定するには、次のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflogin.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/irfshoip.htm

tunnel tos および **tunnel ttl** コマンドを設定するには、次のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s_tos.htm

次のトンネル情報に注意してください。

- ハードウェア補助の各トンネルには固有の送信元が必要です。ハードウェア補助のトンネルは、宛先が異なっていても送信元を共有できません。ループバック インターフェイスにあるセカンダリ アドレスを使用するか、複数のループバック インターフェイスを作成します（CSCdy72539）。
- 各トンネル インターフェイスは、内部 VLAN を 1 つ使用します。
- 各トンネル インターフェイスは、ルータ MAC（メディア アクセス制御）アドレスごとに追加のルータ MAC アドレス エントリ 1 つを使用します。
- PFC3A は、トンネル インターフェイスで PFC QoS 機能をサポートしていません。
- PFC3B および PFC3BXL は、トンネル インターフェイスで PFC QoS 機能をサポートします。
- MSFC3 は、トンネル インターフェイスの出力機能で設定されたトンネルをサポートします。出力機能例として、出力 Cisco IOS ACL、NAT（内部から外部への変換）、TCP インターセプト、CBAC、暗号化が挙げられます。

CHAPTER 2

コマンドライン インターフェイス（CLI）

この章では、Cisco IOS リリース 12.2SX でサポートされているスイッチの設定に使用する、Command-Line Interface（CLI; コマンドライン インターフェイス）について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

この章で説明する内容は、次のとおりです。

CLI へのアクセス

ここでは、CLI にアクセスする手順について説明します。

EIA/TIA-232 コンソール インターフェイス経由で CLI にアクセスする場合

（注）　EIA/TIA-232 は、EIA（米国電子工業会）および TIA（米国電気通信工業会）によって認定される以前は、Recommended Standard 232（RS-232）と呼ばれていました。

EIA/TIA-232 コンソール インターフェイスの接続を使用して、初期設定を行います。コンソール インターフェイスのケーブル接続手順については、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

コンソールを接続するには、次の作業を行います。

	コマンド	目的
ステップ 1	Return キーを押します。	プロンプトを表示します。
ステップ 2	`Router> enable`	イネーブル モードを開始します。
ステップ 3	`Password: password` `Router#`	イネーブル モードの開始を完了します。
ステップ 4	`Router# quit`	作業が完了したら、セッションを終了します。

コンソールに接続すると、次のように表示されます。

```
Press Return for Console prompt

Router> enable
Password:
Router#
```

Telnet を使用して CLI にアクセスする場合

（注）　スイッチに Telnet で接続するには、事前に IP アドレスを設定する必要があります（「IPv4 ルーティングおよびアドレスの設定」（P.22-4）を参照）。

スイッチは最大 8 つの Telnet セッションを同時にサポートできます。Telnet セッションは、アイドル状態のまま **exec-timeout** コマンドに指定されている時間が経過すると、自動的に切断されます。

スイッチに Telnet 接続するには、次の作業を行います。

	コマンド	目的
ステップ 1	**telnet** {*hostname* | *ip_addr*}	アクセス対象のスイッチに、リモート ホストから Telnet 接続します。

ステップ 2	`Password: password`
	
	`Router#`
		認証を開始します。
		（注）　パスワードを設定していない場合は、Return キーを押します。

ステップ 3	`Router> enable`	イネーブル モードを開始します。
ステップ 4	`Password: password` `Router#`	イネーブル モードの開始を完了します。
ステップ 5	`Router# quit`	作業が完了したら、セッションを終了します。

次に、スイッチとの Telnet セッションをオープンする例を示します。

```
unix_host% telnet Router_1
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.

User Access Verification

Password:
Router_1> enable
Password:
Router_1#
```

コマンドラインの処理

コマンドには、大文字と小文字の区別はありません。また、コマンドおよびパラメータは、現在使用可能な他のコマンドまたはパラメータと区別できる文字数まで省略可能です。プロンプトでは、ヒストリバッファに保存されている直前に入力した 20 個のコマンドをスクロールして、コマンドをそのまま入力したり編集して使用したりできます。表 2-1 に、コマンドの入力と編集に使用できるキーボード ショートカットの一覧を示します。

表 2-1　　キーボード ショートカット

キーストローク	目的
Ctrl+B または 左矢印キー[1]	カーソルを 1 文字分だけ後退させます。
Ctrl+F または 右矢印キー [1]	カーソルを 1 文字分だけ進めます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	コマンドラインの末尾にカーソルを移動します。
Esc、**B**	単語 1 つ分だけカーソルを後退させます。
Esc、**F**	単語 1 つ分だけカーソルを進めます。

1. 矢印キーは、VT100 などの ANSI 互換端末に限り有効です。

ヒストリ置換

ヒストリ バッファには、直前に入力した 20 個のコマンドが保存されます。特別な省略コマンドを使用して、再入力せずに保存されているコマンドにアクセスすることができます。表 2-2 に、ヒストリ置換コマンドを示します。

表 2-2　ヒストリ置換コマンド

コマンド	目的
Ctrl+P または上矢印キー[1]	直前に入力されたコマンドから始めて、ヒストリ バッファに保管されているコマンドを呼び出します。キー シーケンスを繰り返すと、さらに古いコマンドが順に呼び出されます。
Ctrl+N または下矢印キー [1]	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、ヒストリ バッファ内のより新しいコマンドに戻ります。キー シーケンスを繰り返すと、さらに新しいコマンドが順に呼び出されます。
`Router# show history`	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。

1. 矢印キーは、VT100 などの ANSI 互換端末に限り有効です。

Cisco IOS コマンド モード

（注）　Cisco IOS コマンド モードの詳細については、次の URL にある『Cisco IOS *Configuration Fundamentals Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html

Cisco IOS ユーザ インターフェイスには、多数のモードがあります。使用できるコマンドの種類は、現在どのモードにいるかによって変わってきます。システム プロンプトに疑問符（?）を入力すると、そのモードで使用できるコマンドの一覧が表示されます。「Cisco IOS コマンド リストおよび構文の表示」（P.2-6）を参照してください。

スイッチ上でセッションを開始すると、ユーザ モード（別名ユーザ EXEC モード）から始まります。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。すべてのコマンドを使用できるようにするには、イネーブル EXEC モードを開始する必要があります。イネーブル EXEC モードにアクセスするには、通常、パスワードの入力が必要です。イネーブル EXEC モードでは、任意の EXEC コマンドを入力できるほか、グローバル コンフィギュレーション モードにアクセスできます。

コンフィギュレーション モードでは、実行コンフィギュレーションの変更を行うことができます。コンフィギュレーションを保存すると、再起動後もそれらのコマンドが保存されます。最初にグローバル コンフィギュレーション モードを開始する必要があります。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、サブインターフェイス コンフィギュレーション モード、および各種プロトコル固有のモードを開始できます。

（注）　Release 12.1(11b)E 以降では、コンフィギュレーション モードで、コマンドの前に **do** キーワードを入力することによって、EXEC モード レベル コマンドを入力できます。

ROM モニタ モードは、スイッチを正常に起動できない場合に使用される独立したモードです。たとえば、スイッチの起動時に有効なシステム イメージが見つからない場合、またはスイッチのコンフィギュレーション ファイルが壊れている場合に、スイッチで ROM モニタ モードが開始されることがあります。「ROM モニタのコマンドライン インターフェイス」（P.2-8）を参照してください。

表 2-3 で、使用頻度の高い Cisco IOS モードについて説明します。

表 2-3　使用頻度の高い Cisco IOS コマンド モード

モード	用途	アクセス方法	プロンプト
ユーザ EXEC	リモート装置への接続、端末の一時的な設定変更、基本的なテストの実行、およびシステム情報の表示	ログインします。	`Router>`
イネーブル EXEC	動作パラメータの設定。イネーブル コマンド セットには、**configure** コマンドのほかにユーザ EXEC モードのコマンドが含まれます。このコマンドを使用して、別のコマンド モードにアクセスします。	ユーザ EXEC モードで、**enable** コマンドおよびイネーブル パスワードを入力します。	`Router#`
グローバル コンフィギュレーション	システム全体に作用する機能の設定	イネーブル EXEC モードで、**configure terminal** コマンドを入力します。	`Router(config)#`
インターフェイス コンフィギュレーション	インターフェイス別に使用できるさまざまな機能があります。インターフェイス コマンドを実行すると、インターフェイスの動作がイネーブルになるか、または変更されます。	グローバル コンフィギュレーション モードで、**interface** *type slot/port* コマンドを入力します。	`Router(config-if)#`
コンソール コンフィギュレーション	直接接続されたコンソールまたは Telnet 接続による仮想端末から、このコンフィギュレーション モードを使用してコンソール インターフェイスを設定します。	グローバル コンフィギュレーション モードで、**line console 0** コマンドを入力します。	`Router(config-line)#`

ユーザが入力するコマンドは、Cisco IOS コマンド インタープリタ（別名 EXEC）によって認識および実行されます。コマンドを入力する際、他のコマンドと区別がつく文字数だけを入力し、コマンドおよびキーワードを省略できます。たとえば、**show** コマンドは **sh**、**configure terminal** コマンドは **config t** に省略できます。

exit と入力すると、スイッチは 1 つ前のレベルに戻ります。コンフィギュレーション モードを完全に終了してイネーブル EXEC モードに戻るには、**Ctrl+Z** を押します。

Cisco IOS コマンド リストおよび構文の表示

どのコマンド モードでも、疑問符（?）を入力することにより、使用できるコマンドのリストを表示できます。

```
Router> ?
```

特定の文字シーケンスで始まるコマンドのリストを表示するには、それらの文字を入力し、そのあとに疑問符（?）を入力します。スペースは入れません。この形式のヘルプは、ユーザに代わって 1 つの単語を完成させるので、ワード ヘルプといいます。

```
Router# co?
collect  configure  connect  copy
```

キーワードまたは引数のリストを表示するには、キーワードまたは引数の代わりに疑問符を入力します。疑問符の前にスペースを 1 つ入れてください。この形式のヘルプは、すでに入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードまたは引数を表示するので、コマンド構文ヘルプといいます。

次に、例を示します。

```
Router# configure ?
  memory              Configure from NV memory
  network             Configure from a TFTP network host
  overwrite-network   Overwrite NV memory from TFTP network host
  terminal            Configure from the terminal
  <cr>
```

前に入力したコマンドを再表示するには、上矢印キーまたは **Ctrl+P** を押します。上矢印キーを続けて押すことにより、直前に入力したコマンドを 20 個まで表示できます。

ヒント　コマンドの入力において問題が生じた場合は、システム プロンプトを確認するとともに、疑問符（?）を入力して使用できるコマンドのリストを表示してください。コマンド モードが間違っているか、間違った構文を使用している可能性があります。

1 つ前のモードに戻るには、**exit** を入力します。どのモードでも、**Ctrl+Z** を押すか、または **end** コマンドを入力すると、直接イネーブル EXEC モードに戻ります。

CLI のセキュリティ

CLI へのアクセスのセキュリティは、許可されていないユーザがコンフィギュレーション設定を表示したり設定に変更を加えたりして、ネットワークの安定性を損なったり、ネットワーク セキュリティを侵害したりすることを防止します。以下のセキュリティ機能の 1 つまたは複数を設定することにより、スイッチのための強力で柔軟なセキュリティ スキームを作成できます。

- イネーブル EXEC コマンドへのアクセス保護

  少なくとも、ユーザ EXEC IOS コマンド モードとイネーブル EXEC IOS コマンド モードに別々のパスワードを設定してください。ユーザ名とパスワードの組み合わせを設定して CLI セッションへのアクセスを特定のユーザだけに制限することにより、セキュリティのレベルをさらに高めることができます。詳細については、次の URL にある「Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices」を参照してください。

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_sec_4cli.html

- RADIUS、TACACS+、または Kerberos でのスイッチ アクセスの制御

  一元管理されたスケーラブルなセキュリティ スキームのために、Remote Authentication Dial-In User Service（RADIUS）、Terminal Access Controller Access-Control System Plus（TACACS+）、Kerberos のいずれかを実行する外部セキュリティ サーバによる認証と許可の取得をユーザに要求することができます。

  RADIUS の詳細については、次の URL にある「Configuring RADIUS」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrad.html

  TACACS+ の詳細については、次の URL にある「Configuring TACACS+」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

  Kerberos の詳細については、次の URL にある「Configuring Kerberos」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html

- SSH または HTTPS を使用した安全な接続の設定

  Secure Shell（SSH）クライアントを使用するか、または HTTP over Secure Socket Layer（HTTPS）をサポートするブラウザを使用すれば、スイッチとの間で暗号化された接続を確立して、コンフィギュレーション セッションが盗聴されるのを防ぐことができます。

  SSH の詳細については、次の URL にある「Configuring Secure Shell」を参照してください。

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_secure_shell_ps6017_TSD_Products_Configuration_Guide_Chapter.html

  HTTPS の詳細については、次の URL にある「HTTPS - HTTP Server and Client with SSL 3.0」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftsslsht.html

- SCP を使用しての安全なコンフィギュレーション ファイルのコピー

  Secure Copy Protocol（SCP）を使用すれば、暗号化されたファイル転送を実行して、スイッチとの間でコンフィギュレーション ファイルまたはイメージ ファイルをコピーする際の盗聴を防ぐことができます。SCP の詳細については、次の URL にある「Secure Copy」を参照してください。

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_ps6017_TSD_Products_Configuration_Guide_Chapter.html

CLI のセキュリティに関するその他の情報については、次の URL にある「Cisco IOS Security Configuration Guide: Securing User Services, Release 12.2SX」を参照してください。

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_2sx/sec_securing_user_services_12.2sx_book.html

ROM モニタのコマンドライン インターフェイス

ROM モニタは、プラットフォームの電源投入時、リセット時、または重大な例外が発生したときに実行される ROM ベースのプログラムです。ROM モニタ モードが開始されるのは、スイッチが有効なソフトウェア イメージを見つけることができなかった場合、NVRAM（不揮発性 RAM）内のコンフィギュレーションが壊れていた場合、またはコンフィギュレーション レジスタが ROM モニタ モードを開始するように設定されていた場合です。ROM モニタ モードで、フラッシュ メモリ、ネットワーク サーバ ファイル、またはブートフラッシュから、ソフトウェア イメージを手動でロードできます。

スイッチを再起動し、起動から 60 秒以内に **Break** キーを押して、ROM モニタ モードを開始することもできます。

（注） コンフィギュレーション レジスタの設定で、**Break** キーがオフに設定されているかどうかに関係なく、再起動から 60 秒間は常に **Break** キーが有効です。

端末サーバから ROM モニタ モードにアクセスするには、エスケープによって Telnet プロンプトを表示し、端末エミュレーション プログラムで **send break** コマンドを入力し、ROM モニタ モードを開始します。

ROM モニタ モードが開始されると、プロンプトが rommon 1> になります。疑問符（**?**）を入力すると、使用できる ROM モニタ コマンドが表示されます。

ROM モニタ コマンドの詳細については、*Cisco IOS Master Command List*, Release 12.2SX を参照してください。

CHAPTER 3

スイッチの初期設定

この章では、Catalyst 6500 シリーズ スイッチを初期設定する手順の情報について説明します。これは、次のマニュアルに記載されている管理情報および手順を補足するためのものです。

- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm
- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Command Reference*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
- http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

デフォルト設定

表 3-1 に、デフォルト設定を示します。

表 3-1　　デフォルト設定

機能	デフォルト値
管理用接続	ユーザ モード
グローバル情報	次の値は設定されていません。 • システム名 • システムの連絡先 • ロケーション
システム クロック	システム クロック タイムには値が設定されていません。
パスワード	ユーザ モードまたはイネーブル モードのパスワードは設定されていません（**Return** キーを押してください）。
プロンプト	`Router>`

スイッチの設定

ここでは、スイッチを設定する手順について説明します。

- 「セットアップ機能または setup コマンドの使用」（P.3-2）
- 「コンフィギュレーション モードの使用」（P.3-10）
- 「実行コンフィギュレーションを保存する前の確認」（P.3-11）
- 「実行コンフィギュレーションの保存」（P.3-12）
- 「設定の確認」（P.3-12）
- 「デフォルト ゲートウェイの設定」（P.3-12）
- 「スタティック ルートの設定」（P.3-13）
- 「BOOTP サーバの設定」（P.3-14）

セットアップ機能または setup コマンドの使用

ここでは、セットアップ機能および **setup** コマンドについて説明します。

- 「セットアップの概要」（P.3-3）
- 「グローバル パラメータの設定」（P.3-3）
- 「インターフェイスの設定」（P.3-8）

セットアップの概要

スイッチを最初に起動すると、セットアップ機能が自動的に開始されます（初回起動時の **setup** コマンドの機能は、何も設定されていないシステム機能と同じ状態です）。イネーブル プロンプト（#）で **setup** コマンドを入力することにより、セットアップ機能を実行できます。

setup コマンドを入力すると、**setup** コマンド プロセスで現在のデフォルトのシステム設定が角カッコ（[ ]）で囲まれて表示されます。表示される一連の質問に応答して変更を行います。

たとえば、セットアップ機能を使用すると、次のように表示されます。

```
Configuring interface FastEtherent3/1:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
```

setup コマンドを使用すると、次のように表示されます。

```
Configuring interface FastEthernet4/1:
  Is this interface in use?[yes]: yes
  Configure IP on this interface?[yes]: yes
```

グローバル パラメータの設定

セットアップ機能を初めて起動するか、または **setup** コマンドを初めて入力すると、グローバル パラメータを設定するように求められます。グローバル パラメータは、システム全体の設定値を制御します。

スイッチを起動し、グローバル パラメータを入力するには、次の作業を行います。

ステップ 1　スーパーバイザ エンジン上のコンソール インターフェイスにコンソール端末を接続し、システムを起動してユーザ EXEC プロンプト（Router>）を表示します。

Catalyst 6500 シリーズ スイッチを起動すると、次のように表示されます（設定によっては、実際の出力内容がこの例と完全には一致しない場合があります）。

```
System Bootstrap, Version 6.1(2)
Copyright (c) 1994-2000 by cisco Systems, Inc.
c6k_sup2 processor with 131072 Kbytes of main memory

rommon 1 > boot disk0:c6sup22-jsv-mz.121-5c.EX.bin

Self decompressing the image : ##################################################
################################################################################
################################################################################
################################################################################
################################################################################
 [OK]

               Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706
```

```
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_sp Software (c6sup2_sp-SPV-M), Version 12.1(5c)EX, EARLY DEPLOYM
ENT RELEASE SOFTWARE (fc1)
Synced to mainline version: 12.1(5c)
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 28-Mar-01 18:36 by hqluong
Image text-base: 0x30020980, data-base: 0x306B8000

Start as Primary processor

00:00:05: %SYS-3-LOGGER_FLUSHING: System pausing to ensure console debugging out
put.

00:00:03: Currently running ROMMON from S (Gold) region
00:00:05: %OIR-6-CONSOLE: Changing console ownership to route processor



System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Cat6k-MSFC2 platform with 131072 Kbytes of main memory

rommon 1 > boot

Self decompressing the image : ##################################################
################################################################################
## [OK]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco Internetwork Operating System Software
IOS (tm) MSFC2 Software (C6MSFC2-BOOT-M), Version 12.1(3a)E4, EARLY DEPLOYMENT R
ELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Sat 14-Oct-00 05:33 by eaarmas
Image text-base: 0x30008980, data-base: 0x303B6000

cisco Cat6k-MSFC2 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
X.25 software, Version 3.0.0.
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).


Press RETURN to get started!
```

（注） コンフィギュレーション スクリプトの最初の 2 つのセクション（バナーおよび搭載ハードウェア）は、システムの初回起動時に限り表示されます。それ以降に **setup** コマンド機能を使用するときは、次のシステム コンフィギュレーション ダイアログからセットアップ スクリプトが始まります。

```
--- 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
```

（注） ここで示す出力例は、一例です。システムの設定によっては、実際の出力内容がこれらの例とは完全に一致しない場合があります。

ステップ 2　コンフィギュレーション ダイアログを開始するかどうか、現在のインターフェイス サマリーを表示するかどうかの質問に対して、**yes** と入力するか **Return** キーを押します。**Return** キーを押すと、デフォルト（yes）が使用されます。

```
Would you like to enter the initial configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:
```

（セットアップ機能で）**yes** と応答したあとの出力例を示します。スイッチの初回起動時、つまりまだ何も設定していない場合には、次のように表示されます。

```
Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      unassigned      YES TFTP   administratively down down

GigabitEthernet1/1         unassigned      YES TFTP   administratively down down

GigabitEthernet1/2         unassigned      YES TFTP   administratively down down

GigabitEthernet3/1         unassigned      YES TFTP   administratively down down

GigabitEthernet3/2         unassigned      YES TFTP   administratively down down

GigabitEthernet3/3         unassigned      YES TFTP   administratively down down

GigabitEthernet3/4         unassigned      YES TFTP   administratively down down

GigabitEthernet3/5         unassigned      YES TFTP   administratively down down

GigabitEthernet3/6         unassigned      YES TFTP   administratively down down

GigabitEthernet3/7         unassigned      YES TFTP   administratively down down

GigabitEthernet3/8         unassigned      YES TFTP   administratively down down

(Additional displayed text omitted from this example.)
```

一部のインターフェイスがすでに設定されているスイッチの場合には、（setup コマンド機能で）**yes** と応答すると、次のように表示されます。

```
Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      unassigned      YES TFTP   administratively down down

GigabitEthernet1/1         172.20.52.34    YES NVRAM  up                    up

GigabitEthernet1/2         unassigned      YES TFTP   administratively down down

GigabitEthernet3/1         unassigned      YES TFTP   administratively down down

GigabitEthernet3/2         unassigned      YES TFTP   administratively down down

GigabitEthernet3/3         unassigned      YES TFTP   administratively down down

GigabitEthernet3/4         unassigned      YES TFTP   administratively down down

GigabitEthernet3/5         unassigned      YES TFTP   administratively down down

GigabitEthernet3/6         unassigned      YES TFTP   administratively down down

GigabitEthernet3/7         unassigned      YES TFTP   administratively down down

GigabitEthernet3/8         unassigned      YES TFTP   administratively down down

<...output truncated...>
```

ステップ 3　インターフェイス上でサポートするプロトコルを選択します。IP インストレーションに限り、大部分の質問に対してデフォルト値をそのまま使用することができます。

次に、IP を使用する最小限の設定を示します。ステップ 8 まで続きます。

```
Configuring global parameters:

  Enter host name [Router]: Router
```

ステップ 4　次のように表示されたら、イネーブル シークレット パスワードを入力します（このパスワードは、今後使用するので覚えておいてください）。

```
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: barney
```

ステップ 5　次のように表示されたら、イネーブル パスワード入力します（このパスワードは、今後使用するので覚えておいてください）。

```
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: wilma
```

ユーザ EXEC レベルで使用できるコマンドは、イネーブル EXEC レベルで使用できるコマンドの一部です。大部分のイネーブル EXEC コマンドは、動作パラメータを設定するコマンドなので、これらのコマンドが不正に使用されないように、パスワードで保護する必要があります。

イネーブル EXEC コマンドにアクセスするには、正しいパスワードを入力する必要があります。ブート ROM モニタから実行する場合、ブート ROM レベルによっては、正しいイネーブル パスワードが使用される場合があります。

イネーブルとイネーブル シークレット パスワードは、セキュリティを強化するために異なるパスワードを設定する必要があります。セットアップ スクリプト中はイネーブルとイネーブル シークレット パスワード両方に同じパスワードを入力できます。ただし、別のパスワードを入力する必要があることを示す警告メッセージを受信します。

（注） イネーブル シークレット パスワードには、1 ～ 25 文字の英数字（大文字と小文字）を組み合わせて使用できます。イネーブル パスワードには、任意の数の英数字（大文字と小文字）を組み合わせて使用できます。どちらのパスワードでも、先頭文字に数字は使用できません。パスワードの中にスペースを使用することもできます。たとえば、「two words」は有効なパスワードです。先行スペースは無視されますが、後続スペースは認識されます。

ステップ 6　次のように表示されたら、仮想端末パスワードを入力します（このパスワードは、今後使用するので覚えておいてください）。

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: bambam
```

ステップ 7　ほとんどの場合、IP ルーティングを使用することになります。その場合、内部ルーティング プロトコルを選択する必要があります。たとえば、Enhanced Interior Gateway Routing Protocol（EIGRP）です。

IP を設定する場合は **yes**（デフォルト）と入力するか、**Return** キーを押し、続いて、EIGRP を選択します。

```
Configure IP? [yes]:
Configure EIGRP routing? [yes]:
Your IGRP autonomous system number [1]: 301
```

ステップ 8　Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）でネットワークを管理する場合は **yes**、そうでない場合は **no** と入力します。

```
Configure SNMP Network Management? [yes]:
Community string [public]:
```

SNMP の詳細および設定手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2 内の「Cisco IOS System Management」、「Configuring SNMP Support」

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Command Reference*』Release 12.2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

設定した内容を確認するために、次のような出力およびステップ 3 ～ 8 で選択したコンフィギュレーション パラメータの全リストが表示されます。これらのパラメータおよびデフォルトは、コンソール端末に出力された順序に従って表示されます。

```
The following configuration command script was created:

hostname router
enable secret 5 $1$S3Lx$uiTYg2UrFK1U0dgWdjvxw.
enable password lab
line vty 0 4
password lab
no snmp-server
```

```
!
ip routing eigrp 301

!
interface Vlan1
shutdown
no ip address
!
interface GigabitEthernet1/1
shutdown
no ip address
!
interface GigabitEthernet1/2
shutdown
no ip address
!
.
<...output truncated...>
.!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
% You can enter the setup, by typing setup at IOS command prompt
Router#
```

グローバル パラメータの設定手順は、以上で完了です。セットアップ機能は、引き続きインターフェイスの設定処理に進みます（次の「インターフェイスの設定」を参照）。

インターフェイスの設定

ここでは、外部ネットワーク経由での通信を可能にするために、インストールされているインターフェイスを（セットアップ機能または **setup** コマンド機能によって）設定する手順について説明します。インターフェイス パラメータを設定するには、インターフェイス ネットワーク アドレス、サブネット マスク情報、設定対象のプロトコルが必要です （使用できる各モジュールに関する詳しいインターフェイス設定手順については、モジュールに付属の各コンフィギュレーション ノートを参照してください）。

（注） ここで示す出力例は、一例です。システムの設定によっては、実際の出力内容がこれらの例とは完全に一致しない場合があります。

インターフェイスを設定するには、次の作業を行います。

ステップ 1　ギガビット イーサネット インターフェイスの設定に関するプロンプトで、要件を満たす適切な応答を入力します。アドレスおよびサブネット マスクは、使用しているネットワークのものを入力してください。

```
Do you want to configure GigabitEthernet1/1 interface? [no]: yes
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.20.52.34
    Subnet mask for this interface [255.255.0.0] : 255.255.255.224
    Class B network is 172.20.0.0, 27 subnet bits; mask is /27
```

ステップ 2　その他のインターフェイス タイプの場合は、要件を満たす適切な応答をプロンプトに入力します。

```
Do you want to configure FastEthernet5/1  interface? [no]: y
  Configure IP on this interface? [no]: y
    IP address for this interface: 172.20.52.98
    Subnet mask for this interface [255.255.0.0] : 255.255.255.248
    Class B network is 172.20.0.0, 29 subnet bits; mask is /29
```

設定するインターフェイスごとに、このステップを繰り返します。ステップ 3 に進み、コンフィギュレーション パラメータを確認します。

インストールされている最後のインターフェイスに関するコンフィギュレーション ダイアログに応答すれば、インターフェイスの設定は完了です。

ステップ 3　コンソール端末に表示されるコンフィギュレーション パラメータの全リストを確認します。このリストの最後に、次の質問が表示されます。

```
Use this configuration? [yes/no]:
```

no と応答すると、イネーブル プロンプト（#）に戻ります。その場合は **setup** コマンドを再入力して、コンフィギュレーションを再入力する必要があります。**yes** と応答すると、次のように実行コンフィギュレーションが NVRAM（不揮発性 RAM）に保存されます。

```
Use this configuration? [yes/no]: yes
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!
```

Return キーを押すと、次のプロンプトが表示されます。

```
Router>
```

システムのグローバル パラメータおよびインターフェイス パラメータの設定手順は、以上で完了です。この時点で、インターフェイスは、限られた用途に使用できます。

初期設定したあとに現在保存されている設定パラメータを変更する場合、**setup** コマンドを入力します。より複雑な設定を実行するには、コンフィギュレーション モードを開始して **configure** コマンドを使用します。スイッチの現在のステートを確認するには、**show version** コマンドを使用します。このコマンドを使用すると、ソフトウェアのバージョンおよびインターフェイスが次のように表示されます。

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPLOY)
Synced to mainline version: 12.1(5c)
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 28-Mar-01 17:52 by hqluong
Image text-base: 0x30008980, data-base: 0x315D0000

ROM: System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
BOOTFLASH: c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPL)

Router uptime is 2 hours, 33 minutes
System returned to ROM by power-on (SP by power-on)
Running default software

cisco Catalyst 6000 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
```

```
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Virtual Ethernet/IEEE 802.3  interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2
Router#
```

インターフェイスの詳しい設定手順については、次の URL にある『*Cisco IOS Interface Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/index.htm

コンフィギュレーション モードの使用

セットアップ機能を使用しない場合は、次の手順で、コンフィギュレーション モードからスイッチを設定することができます。

ステップ 1　スーパーバイザ エンジンのコンソール インターフェイスに、コンソール端末を接続します。

ステップ 2　初期ダイアログを開始するかどうかの質問に対して、**no** と応答し、ユーザ動作モードを開始します。

```
Would you like to enter the initial dialog? [yes]: no
```

ステップ 3　数秒後に、ユーザ EXEC プロンプト（Router>）が表示されます。**enable** と入力して、イネーブル モードを開始します。

```
Router> enable
```

（注）　設定の変更は、イネーブル モード以外では実行できません。

プロンプトがイネーブル EXEC プロンプト（#）に変わります。

```
Router#
```

ステップ 4　プロンプト（#）に **configure terminal** コマンドを入力して、コンフィギュレーション モードを開始します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

プロンプトに **interface** *type slot/interface* コマンドを入力して、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。

```
Router(config)# interface fastethernet 5/1
Router(config-if)#
```

どちらのコンフィギュレーション モードでも、設定を任意に変更することができます。コンフィギュレーション モードを終了するには、**end** コマンドを入力します。

ステップ 5　設定を保存します（「実行コンフィギュレーションの保存」（P.3-12）を参照）。

これで最小限のスイッチ設定が行われ、入力した設定を使用してスイッチを起動できるようになりました。コンフィギュレーション コマンドのリストを表示するには、プロンプトで **?** を入力するか、コンフィギュレーション モードで **help** キーを押します。

実行コンフィギュレーションを保存する前の確認

入力した設定値または変更内容を確認するには、イネーブル EXEC プロンプト（#）で **show running-config** コマンドを入力します。

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

Current configuration:
Current configuration : 3441 bytes
!
version 12.1
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Router
!
boot buffersize 522200
boot system flash disk0:c6sup22-jsv-mz.121-5c.EX.bin
enable password lab
!
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
no ip finger
!
cns event-service server
!
<...output truncated...>
!
interface FastEthernet3/3
 ip address 172.20.52.19 255.255.255.224
!
<...output truncated...>
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad mop telnet rlogin udptn nasi
!
end
Router#
```

実行コンフィギュレーションの保存

入力した設定または変更を NVRAM のスタートアップ コンフィギュレーションに保存するには、イネーブル EXEC プロンプト（#）で **copy running-config startup-config** コマンドを入力します。

```
Router# copy running-config startup-config
```

このコマンドは、コンフィギュレーション モードで入力した設定値を保存します。この作業を行わないと、次回システムをリロードするときに設定が消失します。

設定の確認

NVRAM に保存されている情報を表示するには、**show startup-config** EXEC コマンドを入力します。**show running-config** EXEC コマンドを入力した場合と同様の情報が表示されます。

デフォルト ゲートウェイの設定

（注） スイッチがデフォルト ゲートウェイを使用するのは、ルーティングが設定されていない場合に限られます。

スイッチにルーティング プロトコルが設定されていない場合に、別のサブネットにデータを送信するには、デフォルト ゲートウェイを設定します。デフォルト ゲートウェイには、同じサブネット内のルータ上のインターフェイスの IP アドレスを指定する必要があります。

デフォルト ゲートウェイを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip default-gateway A.B.C.D`	デフォルト ゲートウェイを設定します。
ステップ 2	`Router# show ip route`	デフォルト ゲートウェイが IP ルーティング テーブルに正しく表示されていることを確認します。

次に、デフォルト ゲートウェイを設定し、その設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip default-gateway 172.20.52.35
Router(config)# end
3d17h: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip route
Default gateway is 172.20.52.35

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
Router#
```

スタティック ルートの設定

Telnet ステーションまたは SNMP ネットワーク管理ワークステーションがスイッチと異なるネットワークに存在し、かつルーティング プロトコルが設定されていない場合、エンド ステーションが存在するネットワークに対応するスタティック ルーティング テーブル エントリを追加する必要がある場合があります。

スタティック ルートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **ip route** *dest_IP_address mask* {*forwarding_IP* | **vlan** *vlan_ID*}	スタティック ルートを設定します。
ステップ 2	Router# **show running-config**	スタティック ルートの設定を確認します。

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.10.5.10 のワークステーションへのスタティック ルートを設定する例を示します。このとき、サブネット マスクと転送先ルータの IP アドレス 172.20.3.35 を使用します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip route 171.10.5.10 255.255.255.255 172.20.3.35
Router(config)# end
Router#
```

次に、**show running-config** コマンドを使用して、前に設定したスタティック ルートの設定を確認する例を示します。

```
Router# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.10.5.10 255.255.255.255 172.20.3.35
no ip http server
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Router#
```

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.20.5.3 のワークステーションへのスタティック ルートを設定する例を示します。このとき、スイッチはサブネット マスクを使用し VLAN 1 に接続されています。

```
Router# configure terminal
Router(config)# ip route 171.20.5.3 255.255.255.255 vlan 1
Router(config)# end
Router#
```

次に、**show running-config** コマンドを使用して、前に設定したスタティック ルートの設定を確認する例を示します。

```
Router# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.20.52.3 255.255.255.255 Vlan1
no ip http server
!
!
x25 host z
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Router#
```

BOOTP サーバの設定

Bootstrap Protocol（BOOTP）は、インターフェイスの MAC（メディア アクセス制御）アドレスおよび IP アドレスを BOOTP サーバ コンフィギュレーション ファイルに追加することにより、自動的に IP アドレスを割り当てます。スイッチは起動時に、BOOTP サーバから IP アドレスを自動的に取得します。

スイッチが BOOTP 要求を実行するのは、現在の IP アドレスが 0.0.0.0 に設定されている場合だけです（0.0.0.0 は、新しいスイッチ、または **erase** コマンドを使用して startup-config ファイルを削除したスイッチのデフォルトの IP アドレスです）。

スイッチが BOOTP サーバから自身の IP アドレスを取り出せるようにするには、最初にスイッチの MAC アドレスを判別し、その MAC アドレスを BOOTP サーバ上の BOOTP コンフィギュレーション ファイルに追加する必要があります。BOOTP サーバ コンフィギュレーション ファイルを作成するには、次の作業を行います。

ステップ 1　ワークステーションに BOOTP サーバ コードをインストールします（まだインストールしていない場合）。

ステップ 2　シャーシのラベルから、MAC アドレスを判別します。

ステップ 3　BOOTP コンフィギュレーション ファイル（通常、/usr/etc/bootptab）に、各スイッチに対応するエントリを追加します。エントリを入力するたびに **Return** キーを押し、各エントリ間に空白行を入れます。ステップ 4 の BOOTP コンフィギュレーション ファイルの例を参照してください。

ステップ 4　**reload** コマンドを入力して、再起動し BOOTP サーバから IP アドレスを自動的に要求します。

次に、エントリを追加した BOOTP コンフィギュレーション ファイルの例を示します。

```
# /etc/bootptab: database for bootp server (/etc/bootpd)
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
#       first field -- hostname
#                       (may be full domain name and probably should be)
#
#       hd -- home directory
#       bf -- bootfile
#       cs -- cookie servers
#       ds -- domain name servers
#       gw -- gateways
#       ha -- hardware address
#       ht -- hardware type
#       im -- impress servers
#       ip -- host IP address
#       lg -- log servers
#       lp -- LPR servers
#       ns -- IEN-116 name servers
#       rl -- resource location protocol servers
#       sm -- subnet mask
#       tc -- template host (points to similar host entry)
#       to -- time offset (seconds)
#       ts -- time servers
#
<information deleted>
#
###############################################################################
# Start of individual host entries
###############################################################################
Router:         tc=netcisco0:   ha=0000.0ca7.ce00:      ip=172.31.7.97:
dross:          tc=netcisco0:   ha=00000c000139:        ip=172.31.7.26:
<information deleted>
```

イネーブル EXEC コマンドへのアクセス保護

ここでは、システム コンフィギュレーション ファイルおよびイネーブル EXEC コマンドへのアクセスを制御する方法について説明します。

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 EXEC モードへのアクセスを制御するスタティック パスワードを設定または変更する手順は、次のとおりです。

コマンド	目的
`Router(config)# enable password password`	イネーブル EXEC モードの新しいパスワードを設定するか、または既存のパスワードを変更します。

次に、イネーブル EXEC モードでイネーブル パスワードを「lab」に設定する例を示します。

```
Router# configure terminal
Router(config)# enable password lab
Router(config)#
```

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

enable password コマンドおよび enable secret コマンドの使用

ネットワークで送受信されるパスワードまたは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されるパスワードについて、セキュリティをさらに強化するには、**enable password** または **enable secret** コマンドを使用します。どちらのコマンドも、イネーブル モード（デフォルト）または指定された権限レベルにアクセスするためにユーザが入力する必要のある暗号化パスワードを設定します。**enable secret** コマンドの使用を推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にできません。

スイッチがイネーブル パスワードを要求するように設定するには、次のいずれかの作業を行います。

コマンド	目的
`Router(config)# enable password [level level] {password | encryption-type encrypted-password}`	イネーブル EXEC モードを開始するためのパスワードを設定します。
`Router(config)# enable secret [level level] {password | encryption-type encrypted-password}`	不可逆的な暗号化方式を使用して保存される、シークレット パスワードを設定します（**enable password** コマンドおよび **enable secret** コマンドを両方とも設定した場合、ユーザはイネーブル シークレット パスワードを入力しなければなりません）。

どちらのコマンドでも、**level** オプションを使用して、特定の権限レベルにアクセスするためのパスワードを定義できます。レベルを指定してパスワードを設定したあと、権限レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

service password-encryption コマンドをイネーブルにしている場合は、入力したパスワードが暗号化されます。**more system:running-config** コマンドを使用してパスワードを表示すると、パスワードは暗号化形式で表示されます。

暗号化タイプを指定する場合は、暗号化パスワード（別の Catalyst 6500 シリーズ スイッチ コンフィギュレーションからコピーした暗号化パスワード）を指定する必要があります。

（注）　暗号化パスワードを忘れた場合には、回復はできません。NVRAM を消去し、新しいパスワードを設定する必要があります。パスワードを忘れた場合には、「イネーブル パスワードを忘れた場合の回復方法」（P.3-20）を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

回線パスワードの設定または変更

回線上のパスワードを設定または変更する手順は、次のとおりです。

コマンド	目的
`Router(config-line)# password password`	イネーブル レベルの新しいパスワードを設定するか、または既存のパスワードを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

イネーブル EXEC モードに対する TACACS+ パスワード保護の設定

TACACS+ の詳細については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Authentication, Authorization, and Accounting（AAA）」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/index.htm
- 次の URL にある『*Cisco IOS Security Command Reference*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

TACACS+ プロトコルを設定してユーザがイネーブル EXEC モードにアクセスできるかどうかを判別するには、次の作業を行います。

コマンド	目的
`Router(config)# enable use-tacacs`	イネーブル EXEC モードに対する、TACACS 形式のユーザ ID およびパスワード チェック メカニズムを設定します。

イネーブル EXEC モードに TACACS パスワード保護を設定すると、**enable** EXEC コマンドでは、新しいユーザ名とパスワードの両方が要求されます。この情報は認証のために TACACS+ サーバに送信されます。拡張 TACACS+ を使用している場合は、既存の UNIX ユーザ識別コードも TACACS+ サーバに送信されます。

注意　**enable use-tacacs** コマンドを入力する場合は、**tacacs-server authenticate enable** コマンドも入力する必要があります。入力しない場合、イネーブル EXEC モードを開始できません。

（注）　拡張 TACACS を使用せずに **enable use-tacacs** コマンドを使用すると、有効なユーザ名およびパスワードを使用すれば誰でもイネーブル EXEC モードにアクセスできることになり、セキュリティの問題が発生する可能性があります。スイッチは、**enable** コマンドの入力によるクエリーと拡張 TACACS なしのログイン試行との違いを判別できないので、この問題が発生します。

パスワードの暗号化

プロトコル アナライザでパケットを調べる（パスワードを読み取る）ことができるので、パスワードを暗号化するように Cisco IOS ソフトウェアを設定することによって、アクセス セキュリティを強化することができます。暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。

パスワードを暗号化するように Cisco IOS ソフトウェアを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# service password-encryption`	パスワードを暗号化します。

暗号化は、現在の設定が保存されるとき、またはパスワードが設定されるときに行われます。パスワードの暗号化は、認証キー 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アクセス パスワード、および Border Gateway Protocol（BGP）ネイバ パスワードを含む、すべてのパスワードに適用されます。**service password-encryption** コマンドを使用すると、許可されていないユーザがコンフィギュレーション ファイルのパスワードを表示することが不可能になります。

注意　**service password-encryption** コマンドでは、高度なネットワーク セキュリティは提供されません。このコマンドを使用する場合は、その他のネットワーク セキュリティ手段も講じる必要があります。

暗号化パスワードを忘れた場合、パスワードの回復はできません（元のパスワードを取り戻すことはできません）。ただし、暗号化パスワードを忘れても、スイッチの制御を取り戻すことはできます。パスワードを忘れた場合には、「イネーブル パスワードを忘れた場合の回復方法」（P.3-20）を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

複数の権限レベルの設定

Cisco IOS ソフトウェアには、パスワード セキュリティのモードがデフォルトで 2 つあります。ユーザ EXEC モードおよびイネーブル EXEC モードです。各モードに、最大 16 個の階層レベルからなるコマンドを設定することができます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザが **clear line** コマンドにアクセスできるようにするには、このコマンドにレベル 2 セキュリティを割り当て、レベル 2 パスワードを幅広く配布します。**configure** コマンドにアクセスできるユーザを限定したい場合には、このコマンドにレベル 3 セキュリティを割り当て、限られたユーザだけにパスワードを配布します。

ここでは、追加のセキュリティ レベルを設定する方法について説明します。

コマンドの権限レベルの設定

コマンドの権限レベルを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# privilege mode level level command`	コマンドの権限レベルを設定します。
ステップ 2	`Router(config)# enable password level level [encryption-type] password`	権限レベルにアクセスするためのイネーブル パスワードを指定します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

回線のデフォルト権限レベルの変更

特定の回線または回線グループのデフォルト権限レベルを変更するには、次の作業を行います。

コマンド	目的
`Router(config-line)# privilege level level`	回線のデフォルトの権限レベルを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および権限レベルの設定の表示」（P.3-20）を参照してください。

権限レベルへのログイン

特定の権限レベルにログインするには、次の作業を行います。

コマンド	目的
`Router# enable level`	指定された権限レベルにログインします。

権限レベルの終了

特定の権限レベルを終了するには、次の作業を行います。

コマンド	目的
`Router# disable level`	指定した権限レベルを終了します。

パスワード、アクセス レベル、および権限レベルの設定の表示

パスワード、アクセス レベル、および権限レベルの設定を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show running-config`	パスワードおよびアクセス レベルの設定を表示します。
ステップ 2	`Router# show privilege`	権限レベルの設定を表示します。

次に、パスワードおよびアクセス レベルの設定を表示する例を示します。

```
Router# show running-config
<...output truncated...>
enable password lab
<...output truncated...>
```

次に、権限レベルの設定を表示する例を示します。

```
Router# show privilege
Current privilege level is 15
Router#
```

イネーブル パスワードを忘れた場合の回復方法

イネーブル パスワードを忘れた場合に、回復するには、次の作業を行います。

ステップ 1　コンソール インターフェイスに接続します。

ステップ 2　スイッチがコンフィギュレーション メモリ（NVRAM）を読み込まずに起動するように設定します。

ステップ 3　システムを再起動します。

ステップ 4　イネーブル モードにアクセスします（パスワードを設定していない場合、パスワードなしでアクセスできます）。

ステップ 5　パスワードを表示または変更するか、または設定を消去します。

ステップ 6　スイッチが通常どおり NVRAM を読み込んで起動するように再設定します。

ステップ 7　システムを再起動します。

（注）　パスワードを回復するには、Break 信号が必要です。使用する端末または PC 端末エミュレータで、Break 信号を発行する方法を知っている必要があります。たとえば ProComm の場合、Alt+B キーを押して Break 信号を生成します。Windows 端末セッションでは、**Break** キーを押すか、または **Ctrl** キーと **Break** キーを同時に押します。

スーパーバイザ エンジンのスタートアップ コンフィギュレーションの変更

ここでは、スーパーバイザ エンジンのスタートアップ コンフィギュレーションの機能と、コンフィギュレーション レジスタおよび BOOT 変数を変更する手順について説明します。

スーパーバイザ エンジンのブート コンフィギュレーションの概要

ここでは、スーパーバイザ エンジンにおけるブート コンフィギュレーションの動作について説明します。

スーパーバイザ エンジンの起動プロセスの概要

スーパーバイザ エンジンの起動プロセスには、2 種類のソフトウェア イメージが関係します。ROM モニタとスーパーバイザ エンジン ソフトウェアです。スイッチを起動またはリセットすると、ROM モニタ コードが実行されます。NVRAM に保存されている設定に応じて、スーパーバイザ エンジンは ROM モニタ モードのままになる場合と、スーパーバイザ エンジン ソフトウェアをロードする場合とがあります。

ユーザが設定できる 2 種類のパラメータによって、スイッチの起動方式が決まります。コンフィギュレーション レジスタと BOOT 環境変数です。コンフィギュレーション レジスタについては、「ブート フィールドの変更および boot コマンドの使用」（P.3-23）を参照してください。BOOT 環境変数については、「スタートアップ システム イメージの指定」（P.3-26）を参照してください。

ROM モニタの概要

ROM モニタは、起動時、リセット時、または重大な例外が発生したときに実行されます。ROM モニタ モードが開始されるのは、スイッチが有効なソフトウェア イメージを見つけることができなかった場合、NVRAM の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROM モニタ モードを開始するように設定されていた場合です。ROM モニタ モードでは、ブートフラッシュ装置またはフラッシュ PC カードから、ソフトウェア イメージを手動でロードできます。

（注）　ROM モニタ コマンドの構文および使用方法の詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

スイッチを再起動し、起動から 60 秒以内に **Break** キーを押して、ROM モニタ モードを開始することもできます。端末サーバから接続している場合は、エスケープによって Telnet プロンプトを表示し、**send break** コマンドを入力すると、ROM モニタ モードが開始されます。

（注）　コンフィギュレーション レジスタの設定で **Break** キーがディセーブルに設定されているかどうかに関係なく、再起動から 60 秒間は常に **Break** キーが有効です。

ROM モニタの機能は、次のとおりです。

- 電源投入時の信頼性テスト
- ハードウェアの初期化
- 起動力（手動による起動および自動起動が可能）
- デバッグ ユーティリティおよびクラッシュ分析
- モニタ呼び出しインターフェイス（EMT コール - ROM モニタは EMT コールを使用して、実行ソフトウェア イメージに情報および一部の機能を提供します）
- ファイル システム（ROM モニタは、単純なファイル システムを認識し、ダイナミックにリンクされたファイル システム ライブラリ（MONLIB）によって新しく作成されたファイル システムをサポートします）
- 例外処理

ソフトウェア コンフィギュレーション レジスタの設定

スイッチは 16 ビットのソフトウェア コンフィギュレーション レジスタを使用します。このコンフィギュレーション レジスタに特定のシステム パラメータを設定できます。ソフトウェア コンフィギュレーション レジスタの設定値は、NVRAM に保存されます。

ソフトウェア コンフィギュレーション レジスタの設定値を変更する目的として次の場合があります。

- 起動元およびデフォルトのブート ファイル名を選択する場合
- ブレーク機能をイネーブルまたはディセーブルにする場合
- ブロードキャスト アドレスを制御する場合
- コンソール端末のボーレートを設定する場合
- フラッシュ メモリからオペレーティング ソフトウェアをロードする場合
- パスワードを回復する場合
- ブートストラップ プログラム プロンプトで **boot** コマンドを使用して手動でシステムを起動できるようにする場合
- システム ブートストラップ ソフトウェア（ブート イメージ）、またはオンボード フラッシュ メモリ上のデフォルトのシステム イメージから自動的に起動し、NVRAM 上のコンフィギュレーション ファイル内の **boot system** コマンドを読み込むように強制的に設定する場合

表 3-2 に、各ソフトウェア コンフィギュレーション メモリ ビットの意味を示します。表 3-3 に、ブート フィールドの定義を示します。

注意　推奨するコンフィギュレーション レジスタ設定は、0x2102 です。Break をイネーブルにする設定を実行し、コンソール接続を使用して Break シーケンスを送信する場合、スイッチは ROMMON になります。

表 3-2　ソフトウェア コンフィギュレーション レジスタ ビットの意味

ビット番号[1]	16 進数	意味
00 ～ 03	0x0000 ～ 0x000F	ブート フィールド（表 3-3 を参照）
06	0x0040	システム ソフトウェアに NVRAM の内容を無視させます。
07	0x0080	OEM[2] ビットをイネーブルにします。
08	0x0100	Break をディセーブルにします。
09	0x0200	セカンダリ ブートストラップを使用します。
10	0x0400	すべてゼロで IP ブロードキャストを行います。
11 ～ 12	0x0800 ～ 0x1000	コンソールの回線速度（デフォルトは 9600 ボー）
13	0x2000	ネットワークでの起動が失敗した場合に、デフォルトのフラッシュ ソフトウェアを起動します。
14	0x4000	IP ブロードキャストでネットワーク番号を使用しません。
15	0x8000	診断メッセージをイネーブルにして、NVRAM の内容を無視します。

1. コンフィギュレーション レジスタの出荷時デフォルト値は、0x2102 です。
2. OEM = Original Equipment Manufacturer（相手先商標製造会社）

表 3-3　ブート フィールド（コンフィギュレーション レジスタ ビット 00 ～ 03）の説明

ブート フィールド	意味
00	システム ブートストラップ プロンプトのまま待機します。
01	オンボード フラッシュ メモリ上で最初に検出されたシステム イメージを起動します。
02 ～ 0F	ネットワークでの起動に使用するデフォルトのファイル名を指定します。デフォルトのファイル名を上書きする boot system コマンドをイネーブルにします。

ブート フィールドの変更および boot コマンドの使用

コンフィギュレーション レジスタのブート フィールドにより、スイッチが OS（オペレーティング システム）イメージをロードするかどうかを決定し、ロードする場合はシステム イメージをどこから取得するかを決定します。ここでは、コンフィギュレーション レジスタのブート フィールドの使用方法および設定手順と、コンフィギュレーション レジスタのブート フィールドを変更する場合の手順について説明します。

ソフトウェア コンフィギュレーション レジスタのビット 0 ～ 3 が、ブート フィールドを形成します。

（注）　システムおよびスペア製品のコンフィギュレーション レジスタの出荷時デフォルト設定は、0x2102 です。

ブート フィールドを 0 または 1（0-0-0-0 または 0-0-0-1）に設定すると、システムはシステム コンフィギュレーション ファイルの起動命令を無視して、次の動作を行います。

- ブート フィールドが 0 に設定されている場合は、システム ブートストラップ プログラムまたは ROM モニタで **boot** コマンドを開始することによって、手動で OS を起動する必要があります。
- ブート フィールドが 1 に設定されている場合は、オンボード ブートフラッシュ Single In-line Memory Module（SIMM）で最初に検出されたイメージを起動します。

- ブート フィールド全体が 0-0-1-0 ～ 1-1-1-1 の範囲の値である場合には、スイッチはスタートアップ コンフィギュレーション ファイルの **boot system** コマンドで指定されるシステム イメージをロードします。

boot コマンドは単独でも入力できますが、フラッシュ メモリに保存されたファイル名、ネットワーク サーバからの起動に使用するファイル名など、追加の起動命令を入力することもできます。ファイル名または他の起動命令を指定せずに **boot** コマンドを使用すると、システムはデフォルトのフラッシュ イメージ（オンボード フラッシュ メモリ上の最初のイメージ）から起動します。また、特定のフラッシュ イメージから起動するように指定することもできます（**boot system flash** *filename* コマンドを使用します）。

さらに、**boot** コマンドを使用して、スーパーバイザ エンジン上のフラッシュ PC カード スロット 0 またはスロット 1 に搭載されたフラッシュ PC カード上のイメージを起動することもできます。ブート フィールドを 0 または 1 以外のビット パターンに設定すると、システムはその結果得られる数値を使用して、ネットワークでの起動に使用するファイル名を作成します。

必要な起動機能に応じて、ブート フィールドを設定する必要があります。

ブート フィールドの変更

ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更できます。ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show version`	現在のコンフィギュレーション レジスタ設定値を判別します。
ステップ 2	`Router# configure terminal`	terminal オプションを選択して、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	`Router(config)# config-register value`	希望するシステム イメージのスイッチのロード方法に応じて、既存のコンフィギュレーション レジスタの設定値を変更します。
ステップ 4	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# reload`	再起動して、変更を有効にします。

スイッチ上で Cisco IOS が稼動しているときにコンフィギュレーション レジスタを変更するには、次の作業を行います。

ステップ 1　**enable** コマンドおよびパスワードを入力して、イネーブル レベルを開始します。

```
Router> enable
Password:
Router#
```

ステップ 2　EXEC モード プロンプト（#）で **configure terminal** コマンドを次のように入力します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

ステップ 3　コンフィギュレーション レジスタを 0x2102 に設定します。

```
Router(config)# config-register 0x2102
```

config-register *value* 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 レジスタの内容を設定します。*value* は、先頭が 0x の 16 進数です（表 3-2（P.3-23）を参照）。

ステップ 4　コンフィギュレーション モードを終了するには、**end** コマンドを入力します。新しい設定値がメモリに保存されます。ただし、新しい設定値を有効にするにはシステムを再起動してシステム ソフトウェアをリロードする必要があります。

ステップ 5　**show version** EXEC コマンドを入力して、現在有効なコンフィギュレーション レジスタ値、および次回のリロード時に使用されるコンフィギュレーション レジスタ値を表示します。この値は、出力の最終行で次のように表示されます。

```
Configuration register is 0x141 (will be 0x2102 at next reload)
```

ステップ 6　設定を保存します。

「実行コンフィギュレーションの保存」（P.3-12）を参照してください。ただし、コンフィギュレーション レジスタの変更を有効にするには、コンソールから **reload** コマンドを入力するなどの方法でシステムをリロードする必要があります。

ステップ 7　システムを再起動します。

システムを起動すると、新しいコンフィギュレーション レジスタ値が有効になります。

コンフィギュレーション レジスタ設定値の確認

現在のコンフィギュレーション レジスタ設定値を確認するには、**show version** EXEC コマンドを使用します。コンフィギュレーション レジスタのブート フィールド値を確認するには、ROM モニタ モードで **o** コマンドを使用します。

コンフィギュレーション レジスタ設定値を確認するには、次の作業を行います。

コマンド	目的
`Router# show version | include Configuration register`	コンフィギュレーション レジスタ設定値を表示します。

次に示す **show version** コマンドの出力例では、現在のコンフィギュレーション レジスタは、スイッチがオペレーティング システム イメージを自動的にロードしないように設定されていることがわかります。スイッチは ROM モニタ モードを開始し、ユーザによる ROM モニタ コマンドの入力を待ちます。新しい設定値を使用すると、スイッチはスタートアップ コンフィギュレーション ファイル内のコマンド、またはネットワーク サーバに保存されているデフォルトのシステム イメージから、システム イメージをロードします。

```
Router1# show version | include Configuration register
Configuration register is 0x2102
Router#
```

スタートアップ システム イメージの指定

スタートアップ コンフィギュレーション ファイルまたは BOOT 環境変数に複数のブート コマンドを入力して、システム イメージをロードするバックアップ方法を提供することができます。

（注）
- システム ソフトウェア イメージは、**sup-bootflash:**、**disk0:**、または **disk1:** 装置に保管します（**disk1:** は Supervisor Engine 720 だけが搭載）。
- Supervisor Engine 2 内の非 ATA-Flash PC カードは **slot0:** です。非 ATA-Flash PC カードは、Release 12.2SX イメージには小さすぎます。
- システム ソフトウェア イメージは **bootflash:** 装置には保管しないでください。この装置は Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上にあり、ブート時にはアクセスできません。

BOOT 環境変数については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』にある「Loading and Maintaining System Images and Microcode」の「Specify the Startup System Image in the Configuration File」でも説明されています。

フラッシュ メモリの概要

ここではフラッシュ メモリについて説明します。

- 「フラッシュ メモリの機能」（P.3-26）
- 「セキュリティ機能」（P.3-27）
- 「フラッシュ メモリの設定プロセス」（P.3-27）

（注）　ここでは、ブートフラッシュ装置およびリムーバブル フラッシュ メモリ カードの両方を説明します。

フラッシュ メモリの機能

フラッシュ メモリ コンポーネントを使用すると、次の操作を行うことができます。

- TFTP によるシステム イメージのフラッシュ メモリへのコピー
- rcp によるシステム イメージのフラッシュ メモリへのコピー
- フラッシュ メモリからの自動または手動によるシステムの起動
- TFTP または rcp によるフラッシュ メモリ イメージのネットワーク サーバへのコピー
- フラッシュ メモリに保存されたシステム ソフトウェア イメージからのスイッチの手動による起動、または自動起動

セキュリティ機能

フラッシュ メモリ コンポーネントは、次のセキュリティ機能をサポートします。

- フラッシュ メモリ カードには、データを保護するための書き込み保護スイッチがあります。フラッシュ PC カードにデータを書き込むには、このスイッチを *unprotected* にセットする必要があります。
- フラッシュ メモリに保存されたシステム イメージを変更できるのは、コンソール端末のイネーブル EXEC レベルからに限られます。

フラッシュ メモリの設定プロセス

スイッチがフラッシュ メモリから起動するように設定するには、次の作業を行います。

ステップ 1　TFTP または rcp を使用して、フラッシュ メモリにシステム イメージをコピーします。次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』Release 12.2 の「Cisco IOS File Management」、「Loading and Maintaining System Images」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt2/fcf008.htm

ステップ 2　フラッシュ メモリ内の目的のファイルからシステムが自動的に起動するように設定します。コンフィギュレーション レジスタ値を変更しなければならない場合があります。コンフィギュレーション レジスタを変更する方法については、「ブート フィールドの変更および boot コマンドの使用」（P.3-23）を参照してください。

ステップ 3　設定を保存します。

ステップ 4　システムの電源をオフ / オンしてシステムを再起動して、すべて正常に動作しているかどうかを確認します。

CONFIG_FILE 環境変数

クラス A フラッシュ ファイル システムでは、初期化（スタートアップ）に使用するコンフィギュレーション ファイルのファイル システムおよびファイル名を、CONFIG_FILE 環境変数で指定します。有効なファイル システムとしては、**nvram:**、**disk0:**、および **sup-bootflash:** があります。

ファイル管理の詳しい設定手順については、次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

CONFIG_FILE 環境変数をスタートアップ コンフィギュレーションに保存すると、スイッチは起動時にこの変数をチェックし、初期化に使用するコンフィギュレーション ファイルの場所およびファイル名を調べます。

CONFIG_FILE 環境変数が存在しない場合、またはこの変数がヌルである場合（初回起動時など）には、スイッチは NVRAM コンフィギュレーションを初期化に使用します。スイッチで NVRAM に問題が検出された場合、またはチェックサム エラーが発生した場合には、スイッチは **setup** モードを開始します。**setup** コマンド機能の詳細については、「セットアップ機能または setup コマンドの使用」（P.3-2）を参照してください。

環境変数の制御

環境変数の制御は ROM モニタが行いますが、特定のコマンドを使用して環境変数を作成、変更、または表示することができます。BOOT 環境変数を作成または変更するには、**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。

BOOT 環境変数の詳しい設定手順については、『*Configuration Fundamentals Configuration Guide*』にある「Loading and Maintaining System Images and Microcode」の「Specify the Startup System Image in the Configuration File」を参照してください。CONFIG_FILE 変数の詳しい設定手順については、『*Configuration Fundamentals Configuration Guide*』にある「Modifying, Downloading, and Maintaining Configuration Files」の「Specify the Startup Configuration File」を参照してください。

（注）　**boot system** グローバル コンフィギュレーション コマンドの実行は、実行コンフィギュレーションだけに影響します。環境変数の設定値を ROM モニタの制御下に置き、環境変数を正しく機能させるには、この設定値をスタートアップ コンフィギュレーションに保存する必要があります。環境変数を実行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に保存するには、**copy system:running-config nvram:startup-config** コマンドを使用します。

BOOT 環境変数の内容を表示するには、**show bootvar** コマンドを使用します。このコマンドは、スタートアップ コンフィギュレーション内のこれらの変数の設定値を表示しますが、実行コンフィギュレーションの設定がスタートアップ コンフィギュレーションの設定と違っている場合には、実行コンフィギュレーション内の設定値も表示します。

次に、環境変数を確認する例を示します。

```
Router# show bootvar
BOOT variable = disk0:,1;sup-bootflash:,1;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2102
Router#
```

CHAPTER 4

Supervisor Engine 720 の設定

この章では、Catalyst 6500 シリーズ スイッチに Supervisor Engine 720 を設定する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。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 3 スロット シャーシの場合、スロット 1 またはスロット 2 のいずれかに Supervisor Engine 720 を取り付けます。
- 6 スロット シャーシまたは 9 スロット シャーシの場合、スロット 5 またはスロット 6 のいずれかに Supervisor Engine 720 を取り付けます。
- 13 スロット シャーシの場合、スロット 7 またはスロット 8 のいずれかに Supervisor Engine 720 を取り付けます。

Supervisor Engine 720 でのブートフラッシュまたはブートディスクの使用

すべての 12.2SX リリースでは、Supervisor Engine 720 64 MB ブートフラッシュ装置（**sup-bootflash:**）をサポートしています。Release 12.2(18)SXE5 とリビルドおよび Release 12.2(18)SXF とリビルドでは、WS-CF-UPG= をサポートしています。これにより、ブートフラッシュ装置は CompactFlash アダプタおよび 512 MB CompactFlash カード（**sup-bootdisk:**）に変更されます。次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_17277.htm

Supervisor Engine 720 でのスロットの使用

Supervisor Engine 720 には、CompactFlash Type II スロットが 2 つ搭載されています。CompactFlash Type II スロットは、シスコシステムズで販売されている CompactFlash Type II フラッシュ PC カードをサポートしています。アクティブ Supervisor Engine 720 上のスロットのキーワードは、**disk0:** および **disk1:** です。冗長 Supervisor Engine 720 上のスロットのキーワードは、**slavedisk0:** および **slavedisk1:** です。

Supervisor Engine 720 ポートの設定

Supervisor Engine 720 ポート 1 には、Small Form-Factor Pluggable（SFP）コネクタが搭載されていますが、固有の設定オプションはありません。

Supervisor Engine 720 ポート 2 には、RJ-45 コネクタおよび SFP コネクタ（デフォルト）が搭載されています。RJ-45 コネクタを使用するには、設定を変更する必要があります。

Supervisor Engine 720 のポート 2 を設定して、RJ-45 コネクタまたは SFP コネクタを使用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet` *slot/2*	設定するイーサネット ポートを選択します。
ステップ 2	`Router(config-if)# media-type {rj45 | sfp}`	使用するコネクタを選択します。
	`Router(config-if)# no media-type`	デフォルト設定（SFP）に戻します。

次に、スロット 5 の Supervisor Engine 720 のポート 2 を RJ-45 コネクタを使用するように設定する例を示します。

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# media-type rj45
```

スイッチ ファブリック機能の設定およびモニタ

ここでは、スイッチング モードを設定し、Supervisor Engine 720 に含まれるスイッチ ファブリック機能をモニタする手順について説明します。

- 「スイッチ ファブリックの動作の概要」（P.4-2）
- 「スイッチ ファブリック機能の設定」（P.4-4）
- 「スイッチ ファブリック機能のモニタ」（P.4-5）

スイッチ ファブリックの動作の概要

ここでは、スイッチ ファブリック機能について説明します。

- 「スイッチ ファブリック機能の概要」（P.4-3）
- 「レイヤ 3 スイッチド トラフィックの転送の決定」（P.4-3）
- 「スイッチング モード」（P.4-3）

スイッチ ファブリック機能の概要

スイッチ ファブリック機能は Supervisor Engine 720 に組み込まれ、ファブリック対応モジュール間に専用接続を確立し、これらのモジュール間で連続的なフレーム転送を行います。スイッチ ファブリック機能によって提供されるファブリック対応モジュール間の直接接続のほかに、ファブリック対応モジュールは、32 Gbps 転送バスへの直接接続も行います。

レイヤ 3 スイッチド トラフィックの転送の決定

Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）または Distributed Feature Card 3（DFC3）は次のように、レイヤ 3 スイッチド トラフィックの転送について決定します。

- PFC3 は、DFC3 が搭載されていないモジュールからスイッチに着信した各パケットの転送判断をすべて行います。
- DFC3 は、次の状況で、DFC3 対応モジュールからスイッチに着信した各パケットの転送判断をすべて行います。
  - 出力ポートが入力ポートと同じモジュールにある場合、DFC3 はパケットをローカルに転送します（パケットがモジュールの外部に送信されません）。
  - 出力ポートが別のファブリック対応モジュール上にある場合、DFC3 はパケットを出力モジュールに送信し、出力ポートから送信します。
  - 出力ポートが別のファブリック非対応モジュール上にある場合、DFC3 はパケットを Supervisor Engine 720 に送信します。Supervisor Engine 720 ファブリック インターフェイスは、パケットが出力モジュールより受信され出力ポートに送信される 32 Gbps スイッチング バスにパケットを転送します。

スイッチング モード

Supervisor Engine 720 の場合、モジュール間のトラフィック転送は、次のいずれかのモードで行われます。

- compact モード - ファブリック対応モジュールだけが搭載されている場合、スイッチはあらゆるトラフィックにこのモードを使用します。このモードでは、スイッチ ファブリック チャネルを通じて DBus ヘッダーのコンパクト版が転送され、最良のパフォーマンスが得られます。
- truncated モード - ファブリック対応モジュールとファブリック非対応モジュールの両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックにこのモードを使用します。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの初めの 64 バイト）を送信します。
- bus モード（別名 flow-through モード）- スイッチはファブリック非対応モジュール間のトラフィック、およびファブリック非対応モジュールとファブリック対応モジュール間のトラフィックにこのモードを使用します。このモードでは、すべてのトラフィックがローカル バスとスーパーバイザ エンジン バス間で送受信されます。

表 4-1 に、搭載されているファブリック対応および非対応モジュール別に、使用されるスイッチング モードを示します。

表 4-1　スイッチ ファブリック機能のスイッチング モード

モジュール	スイッチング モード
ファブリック対応モジュール間（ファブリック非対応モジュールが搭載されていない場合）	Compact[1]
ファブリック対応モジュール間（ファブリック非対応モジュールも搭載されている場合）	Truncated[2]
ファブリック対応モジュールとファブリック非対応モジュール間	Bus
ファブリック非対応モジュール間	Bus

1. **show** コマンドを実行すると、DFC3 を装着したファブリック対応モジュールの場合は dcef モードとして表示され、それ以外のファブリック対応モジュールの場合は fabric モードとして表示されます。
2. **show** コマンドを実行すると、fabric モードとして表示されます。

スイッチ ファブリック機能の設定

スイッチング モードを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# [no] fabric switching-mode allow {bus-mode | {truncated [{threshold [number]}]}}`	スイッチング モードを設定します。

スイッチング モードを設定するときには、次の情報に注意してください。

- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を可能にするには、**fabric switching-mode allow bus-mode** コマンドを入力します。
- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を禁止するには、**no fabric switching-mode allow bus-mode** コマンドを入力します。

注意　**no fabric switching-mode allow bus-mode** コマンドを入力すると、スイッチに搭載されたファブリック非対応モジュールへの電力供給が停止します。

- ファブリック対応モジュールで truncated モードの使用を可能にするには、**fabric switching-mode allow truncated** コマンドを入力します。
- ファブリック対応モジュールで truncated モードの使用を禁止するには、**no fabric switching-mode allow truncated** コマンドを入力します。
- bus モードの代わりに truncated モードを使用する場合に、事前にインストールしなければならないファブリック対応モジュールの数を設定するには、**fabric switching-mode allow truncated threshold** *number* コマンドを入力します。
- デフォルトの truncated モードのスレッシュホールドに戻すには、**no fabric switching-mode allow truncated threshold** コマンドを入力します。

スイッチ ファブリック機能のモニタ

スイッチ ファブリック機能は、モニタ用に多くの **show** コマンドをサポートしています。完全に自動化された起動シーケンスによってモジュールがオンラインになり、ポート上で接続診断テストが実行されます。

ここでは、スイッチ ファブリック機能をモニタする方法について説明します。

スイッチ ファブリック冗長ステータスの表示

スイッチ ファブリックの冗長ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric active**	スイッチ ファブリックの冗長ステータスを表示します。

```
Router# show fabric active
Active fabric card in slot 5
No backup fabric card in the system
Router#
```

ファブリック チャネルのスイッチング モードの表示

特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric switching-mode** [**module** {*slot_number* | **all**]	特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示します。

次に、モジュール 2 について、ファブリック チャネルのスイッチング モードを表示する例を示します。

```
Router# show fabric switching-mode module 2
Module Slot     Switching Mode
2                     dCEF
Router#
```

次に、全モジュールについて、ファブリック チャネルのスイッチング モードを表示する例を示します。

```
Router# show fabric switching-mode
Global switching mode is Compact
dCEF mode is not enforced for system to operate
Fabric module is not  required for system to operate
Modules are allowed to operate in bus mode
Truncated mode is allowed

Module Slot     Switching Mode
1                 Crossbar
2                     dCEF
3                     dCEF
4                     dCEF
5                 Crossbar
6                     dCEF

Router#
```

ファブリック ステータスの表示

特定のスイッチング モジュールまたは全スイッチング モジュールのファブリック ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric status** [*slot_number* | **all**]	ファブリック ステータスを表示します。

次に、全モジュールのファブリック ステータスを表示する例を示します。

```
Router# show fabric status
 slot    channel      speed              module               fabric
                                         status               status
    1          0         8G                  OK                   OK
    5          0         8G                  OK          Up- Timeout
    6          0        20G                  OK         Up- BufError
    8          0         8G                  OK                   OK
    8          1         8G                  OK                   OK
    9          0         8G       Down- DDRsync                   OK
Router#
```

ファブリック利用率の表示

特定のモジュールまたは全モジュールのファブリック利用率を表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric utilization** [*slot_number* | **all**]	ファブリック利用率を表示します。

次に、全モジュールのファブリック利用率を表示する例を示します。

```
Router# show fabric utilization all
Lo% Percentage of Low-priority traffic.
Hi% Percentage of High-priority traffic.

 slot    channel      speed  Ingress Lo%   Egress Lo%  Ingress Hi% Egress Hi%
    5          0        20G            0            0            0          0
    9          0         8G            0            0            0          0
Router#
```

ファブリック エラーの表示

特定のモジュールまたは全モジュールのファブリック エラーを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric errors** [*slot_number* | **all**]	ファブリック エラーを表示します。

次に、全モジュールのファブリック エラーを表示する例を示します。

```
Router# show fabric errors

Module errors:
 slot    channel        crc      hbeat       sync   DDR sync
    1          0          0          0          0          0
    8          0          0          0          0          0
    8          1          0          0          0          0
    9          0          0          0          0          0

Fabric errors:
 slot    channel       sync     buffer    timeout
    1          0          0          0          0
    8          0          0          0          0
    8          1          0          0          0
    9          0          0          0          0
Router#
```

CHAPTER 5

Supervisor Engine 32 の設定

この章では、Catalyst 6500 シリーズ スイッチに Supervisor Engine 32 を設定する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。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Cisco IOS ソフトウェアを使用する場合、Supervisor Engine 32 の最小必須メモリは以下のとおりです。
  - 512 MB DRAM（Supervisor Engine 32）
  - 512 MB DRAM（MSFC2A）
- Supervisor Engine 32 には、PFC3B があり、PFC3B モードで動作します。
- Supervisor Engine 32 は、WS-6503 および WS-6503-E（3 スロット）シャーシではサポートされますが、CISCO7603 シャーシではサポートされません。
- 3 スロット シャーシまたは 4 スロット シャーシの場合、スロット 1 またはスロット 2 のいずれかに Supervisor Engine 32 を取り付けます。
- 6 スロット シャーシまたは 9 スロット シャーシの場合、スロット 5 またはスロット 6 のいずれかに Supervisor Engine 32 を取り付けます。
- 13 スロット シャーシの場合、スロット 7 またはスロット 8 のいずれかに Supervisor Engine 32 を取り付けます。
- Supervisor Engine 32 は、スイッチ ファブリック接続をサポートしていません。
- Supervisor Engine 32 でサポートされているハードウェアおよびソフトウェア機能の詳細については、次の URL にある『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm

Supervisor Engine 32 のフラッシュ メモリ

Supervisor Engine 32 では、次のフラッシュ メモリをサポートします。

- **disk0:** - 1 つの外部 CompactFlash Type II スロット（CompactFlash Type II Flash PC カードをサポート）
- **sup-bootdisk:** - 256 MB 内部 CompactFlash メモリ（ROMMON からは **bootdisk:**）

Supervisor Engine 32 ポート

Supervisor Engine 32 ポートのコンソール ポートは、EIA/TIA-232（RS-232）ポートです。Supervisor Engine 32 には、現在イネーブルになっていない 2 つの Universal Serial Bus（USB）2.0 ポートもあります。

WS-SUP32-GE-3B ポート 1 ～ 8 には、Small Form-Factor Pluggable（SFP）コネクタがあり、ポート 9 には 10/100/1000 Mbps RJ-45 ポートがあります。

WS-SUP32-10GE ポート 1 および 2 には、XENPAK を受け入れる 10 ギガビット イーサネット ポートがあり、ポート 3 には 10/100/1000 Mbps RJ-45 ポートがあります。

CHAPTER 6

Supervisor Engine 2 およびスイッチ ファブリック モジュール（SFM）の設定

ここでは、Catalyst 6500 シリーズ スイッチの Supervisor Engine 2 および Switch Fabric Module（SFM; スイッチ ファブリック モジュール）の設定方法について説明します。

（注）

- Release 12.2(18)SXE および Release 12.2(18)SXE のリビルドでは、Supervisor Engine 2 をサポートしていません。
- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

Supervisor Engine 2 でのスロットの使用

Supervisor Engine 2 は、1 つの Flash PC カード（PCMCIA）スロットを備えています。

PCMCIA Advanced Technology Attachment（ATA）FlashDisk 装置の場合、アクティブ Supervisor Engine 2 のスロットのキーワードは **disk0:** で、冗長 Supervisor Engine 2 のスロットのキーワードは、**slavedisk0:** です。

非 ATA Flash PC カードの場合、アクティブ Supervisor Engine 2 のスロットのキーワードは **slot0:** で、冗長 Supervisor Engine 2 のスロットのキーワードは、**slaveslot0:** です。

スイッチ ファブリック モジュール（SFM）の機能概要

ここでは、スイッチ ファブリック モジュール（SFM）の機能について説明します。

スイッチ ファブリック モジュール（SFM）機能の概要

スイッチ ファブリック モジュール（SFM）対応モジュール間に専用接続を確立し、これらのモジュール間で連続的なフレーム転送を行います。スイッチ ファブリック モジュール（SFM）によって提供されるファブリック対応モジュール間の直接接続のほかに、ファブリック対応モジュールは、32 Gbps 転送バスへの直接接続も行います。

スイッチ ファブリック モジュール（SFM）にはコンソールがありません。前面パネルの 2 行 LCD ディスプレイに、ファブリックの利用状況、ソフトウェア リビジョン、およびシステムの基本情報が表示されます。

スイッチ ファブリック モジュール（SFM）のスロット

13 スロット シャーシの場合、スロット 7 またはスロット 8 のいずれかにスイッチ ファブリック モジュール（SFM）を取り付けます。

（注）　13 スロット シャーシの場合、スロット 9 ～ 13 だけがデュアル スイッチ ファブリック インターフェイス スイッチング モジュール（WS-X6816-GBIC など）をサポートしています。

他のシャーシの場合は、スロット 5 またはスロット 6 のいずれかにスイッチ ファブリック モジュール（SFM）を取り付けます。

スイッチ ファブリックの冗長性

最初に取り付けられたスイッチ ファブリック モジュール（SFM）が、プライマリ モジュールとして機能します。冗長性を確保するには、冗長スイッチ ファブリック モジュール（SFM）を取り付けます。2 つのスイッチ ファブリック モジュール（SFM）を同時に取り付けると、上のスロットのモジュールがプライマリ モジュールとして機能し、下のスロットのモジュールがバックアップとして機能します。上のスロットに取り付けられたモジュールをリセットすると、下のスロットのモジュールがアクティブになります。

スイッチ ファブリック モジュール（SFM）の冗長性に設定は不要です。上のスロットのモジュールがプライマリ モジュールとして機能している場合、このプライマリ モジュールで障害が発生すると、下のスロットの冗長スイッチ ファブリック モジュール（SFM）が自動的に処理を引き継ぎます。

レイヤ 3 スイッチド トラフィックの転送の決定

Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）または Distributed Feature Card（DFC）は、次のようにレイヤ 3 スイッチド トラフィックの転送について決定します。

- PFC2 は、DFC が搭載されていないモジュールからスイッチに入ってきた各パケットの転送判断をすべて行います。
- DFC は、次の状況で DFC 対応モジュールからスイッチに入ってきた各パケットの転送判断をすべて行います。
  - 出力ポートが入力ポートと同じモジュールにある場合、DFC はパケットをローカルに転送します（パケットはモジュールの外部に送信されません）。
  - 出力ポートが別のファブリック対応モジュール上にある場合、DFC は SFM 経由でパケットを出力モジュールに送信し、出力ポートから送信します。
  - 出力ポートが別のファブリック非対応モジュール上にある場合、DFC は SFM 経由でパケットを Supervisor Engine 2 に送信します。Supervisor Engine 2 ファブリック インターフェイスは、パケットが出力モジュールより受信され出力ポートに送信される 32 Gbps スイッチング バスにパケットを転送します。

スイッチング モード

スイッチ ファブリック モジュール（SFM）を取り付けた場合、モジュール間のトラフィック転送は、次のいずれかのモードで行われます。

- compact モード - ファブリック対応モジュールだけが搭載されている場合、スイッチはあらゆるトラフィックにこのモードを使用します。このモードでは、スイッチ ファブリック チャネルを通じて DBus ヘッダーのコンパクト版が転送され、最良のパフォーマンスが得られます。
- truncated モード - ファブリック対応モジュールとファブリック非対応モジュールの両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックにこのモードを使用します。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの初めの 64 バイト）を送信します。
- bus モード（別名 flow-through モード）- スイッチはファブリック非対応モジュール間のトラフィック、およびファブリック非対応モジュールとファブリック対応モジュール間のトラフィックにこのモードを使用します。このモードでは、すべてのトラフィックがローカル バスとスーパーバイザ エンジン バス間で送受信されます。

表 6-1 に、搭載されているファブリック対応および非対応モジュール別に、使用されるスイッチング モードを示します。

表 6-1　取り付けられたスイッチ ファブリック モジュール（SFM）のスイッチング モード

モジュール	スイッチング モード
ファブリック対応モジュール間（ファブリック非対応モジュールが搭載されていない場合）	Compact[1]
ファブリック対応モジュール間（ファブリック非対応モジュールも搭載されている場合）	Truncated[2]
ファブリック対応モジュールとファブリック非対応モジュール間	Bus
ファブリック非対応モジュール間	Bus

1. **show** コマンドを実行すると、DFC を装着したファブリック対応モジュールの場合は dcef モードとして表示され、それ以外のファブリック対応モジュールの場合は fabric モードとして表示されます。
2. **show** コマンドを実行すると、fabric モードとして表示されます。

スイッチ ファブリック モジュール（SFM）の設定

ここでは、スイッチ ファブリック モジュール（SFM）の設定について説明します。

（注）　コンフィギュレーション モードで EXEC モード レベルのコマンドを入力するには、コマンドの**前に do キーワード**を入力します。

スイッチング モードの設定

スイッチング モードを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# [no] fabric switching-mode allow {bus-mode | {truncated [{threshold [number]}]}}`	スイッチング モードを設定します。

スイッチング モードを設定するときには、次の情報に注意してください。

- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を可能にするには、**fabric switching-mode allow bus-mode** コマンドを入力します。
- ファブリック非対応モジュールの使用、またはファブリック対応モジュールで bus モードの使用を禁止するには、**no fabric switching-mode allow bus-mode** コマンドを入力します。

注意　**no fabric switching-mode allow bus-mode** コマンドを入力すると、スイッチに搭載されたファブリック非対応モジュールへの電力供給が停止します。

- ファブリック対応モジュールで truncated モードの使用を可能にするには、**fabric switching-mode allow truncated** コマンドを入力します。

- ファブリック対応モジュールで truncated モードの使用を禁止するには、**no fabric switching-mode allow truncated** コマンドを入力します。
- bus モードの代わりに truncated モードを使用する場合に、事前にインストールしなければならないファブリック対応モジュールの数を設定するには、**fabric switching-mode allow truncated threshold** *number* コマンドを入力します。
- デフォルトの truncated モードのスレッシュホールドに戻すには、**no fabric switching-mode allow truncated threshold** コマンドを入力します。

fabric-required モードの設定

スイッチ ファブリック モジュール（SFM）が取り付けられていない限り、すべてのスイッチング モジュールを動作させないようにする fabric-required モードを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# fabric required`	スイッチ ファブリック モジュール（SFM）が取り付けられていない場合にスイッチング モジュールを動作させないようにする fabric-required モードを設定します。
`Router(config)# no fabric required`	fabric-required モードをクリアします。

注意　スイッチ ファブリック モジュール（SFM）が取り付けられていないスイッチで **fabric required** コマンドを入力すると、スーパーバイザ エンジンを除くすべてのモジュールがオフになります。

fabric-required モードを設定する場合は、次の情報に注意してください。

- fabric-required モードが設定された状態でスイッチ ファブリック モジュール（SFM）が取り付けられていない場合にスイッチを起動すると、スーパーバイザ エンジンだけに電源が供給され、スイッチング モジュールには電源は供給されません。
- fabric-required モードが設定されているスイッチ ファブリック モジュール（SFM）搭載のスイッチが動作している場合に、スイッチ ファブリック モジュール（SFM）を取り外す、またはスイッチ ファブリック モジュール（SFM）で障害が発生すると、スイッチによってすべてのスイッチング モジュールの電源が切断され、スーパーバイザ エンジンだけがアクティブのままになります。
- fabric-required モードが設定された冗長スイッチ ファブリック モジュール（SFM）搭載のスイッチが動作している場合に、両方のスイッチ ファブリック モジュール（SFM）を取り外す、または両方のスイッチ ファブリック モジュール（SFM）で障害が発生すると、スイッチによってすべてのスイッチング モジュールの電源が切断され、スーパーバイザ エンジンだけがアクティブのままになります。

LCD メッセージの設定

LCD に表示されるメッセージを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# fabric lcd-banner d message d`	LCD に表示されるメッセージを設定します。
`Router(config)# no fabric lcd-banner`	LCD に表示されるメッセージをクリアします。

LCD に表示されるメッセージを設定する場合、次の情報に注意してください。

- *d* パラメータはデリミタです。メッセージにはデリミタを使用できません。デリミタは、ポンド記号（#）のようにユーザが選択できます。
- メッセージ テキスト中では、$(token) の形でトークンを使用できます。
  - $(hostname) - スイッチのホスト名を表示します。
  - $(domain) - スイッチのドメイン名を表示します。

スイッチ ファブリック モジュール（SFM）のモニタ

スイッチ ファブリック モジュール（SFM）は、モニタ用に多くの **show** コマンドをサポートしています。完全に自動化された起動シーケンスによってモジュールがオンラインになり、ポート上で接続診断テストが実行されます。

ここでは、スイッチ ファブリック モジュール（SFM）をモニタする方法について説明します。

- 「モジュール情報の表示」（P.6-7）
- 「スイッチ ファブリック モジュール（SFM）冗長ステータスの表示」（P.6-7）
- 「ファブリック チャネルのスイッチング モードの表示」（P.6-8）
- 「ファブリック ステータスの表示」（P.6-8）
- 「ファブリック利用率の表示」（P.6-9）
- 「ファブリック エラーの表示」（P.6-9）

（注）　スイッチ ファブリック モジュール（SFM）ではユーザによる設定は不要です。

モジュール情報の表示

モジュール情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show module** {**5** | **6** | **7** | **8**}	モジュール情報を表示します。

次に、モジュール情報を表示する例を示します。

```
Router# show module 5
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  5    0  Switching Fabric Module                WS-C6500-SFM       SAD04420JR5

Mod MAC addresses                          Hw     Fw           Sw           Status
--- ------------------------------------ ------ ------------ ------------ -------
  5  0001.0002.0003 to 0001.0002.0003   1.0    6.1(3)       6.2(0.97)    Ok
```

スイッチ ファブリック モジュール（SFM）冗長ステータスの表示

スイッチ ファブリック モジュール（SFM）の冗長ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric active**	スイッチ ファブリック モジュール（SFM）の冗長ステータスを表示します。

次に、スイッチ ファブリック モジュール（SFM）の冗長ステータスを表示する例を示します。

```
Router# show fabric active
Active fabric card in slot 5
No backup fabric card in the system
Router#
```

ファブリック チャネルのスイッチング モードの表示

特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric switching-mode** [**module** {*slot_number* | **all**]	特定のモジュールまたは全モジュールについて、ファブリック チャネルのスイッチング モードを表示します。

次に、全モジュールについて、ファブリック チャネルのスイッチング モードを表示する例を示します。

```
Router# show fabric switching-mode all
bus-only mode is allowed
Module Slot     Switching Mode
1               Bus
2               Bus
3               DCEF
4               DCEF
5               No Interfaces
6               DCEF
```

ファブリック ステータスの表示

特定のスイッチング モジュールまたは全スイッチング モジュールのファブリック ステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric status** [*slot_number* | **all**]	ファブリック ステータスを表示します。

次に、全モジュールのファブリック ステータスを表示する例を示します。

```
Router# show fabric status all
   slot    channel      module               fabric
   status               status
   1          0          OK                   OK
   3          0          OK                   OK
   3          1          OK                   OK
   4          0          OK                   OK
Router#
```

ファブリック利用率の表示

特定のモジュールまたは全モジュールのファブリック利用率を表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric utilization** [*slot_number* | **all**]	ファブリック利用率を表示します。

次に、全モジュールのファブリック利用率を表示する例を示します。

```
Router# show fabric utilization all
    slot    channel  Ingress %   Egress %
       1          0          0          0
       3          0          0          0
       3          1          0          0
       4          0          0          0
       4          1          0          0
       6          0          0          0
       6          1          0          0
       7          0          0          0
       7          1          0          0
Router#
```

ファブリック エラーの表示

特定のモジュールまたは全モジュールのファブリック エラーを表示するには、次の作業を行います。

コマンド	目的
Router# **show fabric errors** [*slot_number* | **all**]	ファブリック エラーを表示します。

次に、全モジュールのファブリック エラーを表示する例を示します。

```
Router#  show fabric errors
    slot    channel  module   module  module  fabric
                        crc    hbeat    sync    sync
       1          0       0        0       0       0
       3          0       0        0       0       0
       3          1       0        0       0       0
       4          0       0        0       0       0
       4          1       0        0       0       0
       6          0       0        0       0       0
       6          1       0        0       0       0
       7          0       0        0       0       0
       7          1       0        0       0       0
Router#
```

CHAPTER 7

NSF with SSO スーパーバイザ エンジンの冗長構成の設定

この章では、Stateful Switchover（SSO; ステートフル スイッチオーバー）機能を備えた Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）を使用してスーパーバイザ エンジンの冗長構成を設定する方法について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Release 12.2(18)SXD 以降のリリースでは、NSF with SSO をすべてのスーパーバイザ エンジンでサポートしています。
- すべてのリリースで Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）をサポートしています（第 8 章「Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定」を参照）。
- NSF with SSO は、IPv6 マルチキャスト トラフィックをサポートしていません。

この章で説明する内容は、次のとおりです。

NSF with SSO スーパーバイザ エンジンの冗長構成の概要

ここでは、NSF with SSO を使用したスーパーバイザ エンジンの冗長構成について説明します。

NSF with SSO スーパーバイザ エンジンの冗長構成の概要

（注）

- Release 12.2(18)SXD よりも前のリリースでは、冗長スーパーバイザ エンジンがスタンバイ モードにある場合、冗長スーパーバイザ エンジンの 2 つのギガビット イーサネット インターフェイスは常にアクティブです。
- Supervisor Engine 720 の Release 12.2(18)SXE 以降のリリースでは、インストールされているすべてのスイッチング モジュールに DFC がある場合、**fabric switching-mode allow dcef-only** コマンドを入力して両方のスーパーバイザ エンジンでイーサネット ポートをディセーブルにします。これにより、すべてのモジュールが dCEF モードで動作することが保証され、冗長スーパーバイザ エンジンへのスイッチオーバーが簡略化されます （CSCec05612）。
- Supervisor Engine 2 の Release12.2(18)SXD1 以降のリリースでは、インストールされているすべてのスイッチング モジュールに DFC がある場合、**fabric switching-mode allow dcef-only** コマンドを入力して冗長スーパーバイザ エンジンでイーサネット ポートをディセーブルにします。これにより、すべてのモジュールが dCEF モードで動作することが保証されます （CSCec05612）。

Catalyst 6500 シリーズ スイッチは、プライマリ スーパーバイザ エンジンが故障した場合に冗長スーパーバイザ エンジンに処理を引き継ぐことにより、耐障害性を強化することができます。Cisco NSF は、SSO と連動して、IP パケットの転送を継続しながら、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。また Catalyst 6500 シリーズ スイッチでは、冗長構成として、Route Processor Redundancy（RPR）、Route Processor Redundancy plus（RPR+）、および SRM with SSO もサポートします。これらの冗長構成モードの詳細については、第 8 章「Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定」を参照してください。

次のイベントが発生すると、スイッチオーバーが行われます。

- アクティブ スーパーバイザ エンジンでのハードウェア障害
- スーパーバイザ エンジン間のクロック同期損失
- 手動スイッチオーバー

SSO の動作

SSO は、スーパーバイザ エンジンの 1 つをアクティブに設定してもう 1 つのスーパーバイザ エンジンをスタンバイに指定し、その後これらの間で情報を同期させます。アクティブ スーパーバイザ エンジンが故障したり、スイッチから取り外されたり、またはメンテナンスのため手動でシャットダウンしたりするような場合に、アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへのスイッチ オーバーが発生します。このタイプのスイッチオーバーでは、レイヤ 2 トラフィックは中断されません。

SSO を実行しているネットワーキング装置では、アクティブ スーパーバイザ エンジンが故障したあとに冗長スーパーバイザ エンジンがいつでも制御を行えるように、両方のスーパーバイザ エンジンが同じ設定で動作していなくてはなりません。また SSO スイッチオーバーでは、Forwarding Information Base（FIB; 転送情報ベース）および隣接エントリを維持していて、スイッチオーバー後にレイヤ 3 トラフィックを転送できます。設定情報とデータ構造は、起動時やアクティブ スーパーバイザ エンジンの設定変更が発生したときに、アクティブ スーパーバイザエンジンから冗長スーパーバイザ エンジンへ同期するようになっています。2 つのスーパーバイザ エンジン間の初期同期後に、SSO は転送情報などの両者間のステート情報を維持しています。

スイッチオーバー時に、システム制御およびルーティング プロトコル実行はアクティブ スーパーバイザから冗長スーパーバイザ エンジンに転送されます。アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへの切り替えには、0 ～ 3 秒かかります。

NSF の動作

Cisco NSF は、常に SSO とともに稼動し、レイヤ 3 トラフィックの冗長機能を提供します。NSF は、SSO と連動して、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。NSF の主な目的は、スーパーバイザ エンジンのスイッチオーバー後に IP パケットの転送を継続させることです。

Cisco NSF は、ルーティングについては Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、および Intermediate System-to-Intermediate System（IS-IS）プロトコルで、転送については Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）でサポートされています。ルーティング プロトコルは NSF 機能と NSF 認識によって強化されています。つまり、これらのプロトコルを実行しているルータは、スイッチオーバーを検出し、ネットワーク トラフィックの転送を継続して、ピア装置からのルーティング情報を回復するための必要な措置を行います。ピア装置から情報を受信するのではなく、スイッチオーバー後のルーティング情報を回復するためにアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジンとの間で同期しているステート情報を使用するように、IS-IS プロトコルを設定できます。

ネットワーキング装置は、NSF 互換ソフトウェアを実行している場合に NSF を認識します。NSF をサポートするように装置を設定した場合に装置は NSF 対応になります。NSF 認識ネイバまたは NSF 対応ネイバからルーティング情報を再構築します。

スイッチオーバー中にルーティング プロトコルが Routing Information Base（RIB; ルーティング情報ベース）テーブルを再構築している間、各プロトコルは CEF に依存してパケット転送を継続します。ルーティング プロトコルが収束したあと、CEF が FIB テーブルを更新して失効したルート エントリを削除します。次に、CEF は新しい FIB 情報でライン カードを更新します。

シスコ エクスプレス フォワーディング（CEF）

NSF で重要となる要素は、パケット転送です。シスコのネットワーキング装置では、パケット転送はシスコ エクスプレス フォワーディング（CEF）で提供されます。CEF は FIB を維持し、スイッチオーバー時に使用中の FIB 情報を使用してスイッチオーバー中のパケット転送を継続します。この機能により、スイッチオーバー中のトラフィックの中断を低減することができます。

通常の NSF 動作中に、アクティブ スーパーバイザ エンジンの CEF が現行の FIB および隣接データベースを冗長スーパーバイザ エンジンの FIB および隣接データベースと同期させます。アクティブ スーパーバイザ エンジンのスイッチオーバーでは、冗長スーパーバイザ エンジンに最初からアクティブ スーパーバイザ エンジンで使用中のミラー イメージである FIB と隣接データベースがあります。インテリジェント ライン カードを使用したプラットフォームでは、ライン カードはスイッチオーバーの前後で現行の転送情報を維持します。転送エンジンを使用したプラットフォームでは、アクティブ スーパーバイザ エンジンの CEF によって送信される変更を使用して、CEF が冗長スーパーバイザ エンジンの転送エンジンを最新の状態に保ちます。ライン カードや転送エンジンは、インターフェイスやデータ パスが使用可能である限りはスイッチオーバー後も転送を継続できます。

ルーティング プロトコルがプレフィクスごとに RIB にデータを再び読み込み始めるため、CEF に対してプレフィクスごとの更新が行われます。CEF はこれを使用して FIB と隣接データベースを更新します。既存エントリと新規エントリが最新であることを示す新しいバージョン（「エポック」）番号を受信します。ライン カードや転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIB が収束すると、スーパーバイザ エンジンが信号通知を行います。ソフトウェアが、現在のスイッチオーバー エポックよりも古いエポックを持つすべての FIB と隣接エントリを削除します。これで、FIB は最新のルーティング プロトコル転送情報となるのです。

マルチキャスト MLS NSF with SSO

（注）　NSF with SSO は、IPv6 マルチキャスト トラフィックをサポートしていません。IPv6 マルチキャスト トラフィックのサポートを設定する場合、RPR または RPR+ 冗長構成を設定します。

ルータでスイッチングされるレイヤ 3 マルチキャスト トラフィックがスイッチオーバー時に廃棄されないようにするには、Multicast Multilayer Switching（MMLS; マルチキャスト マルチレイヤ スイッチング）NFS with SSO が必要です。MMLS NSF with SSO がない場合、レイヤ 3 マルチキャスト トラフィックはマルチキャスト プロトコルが収束するまでに廃棄されます。

スイッチオーバー プロセスの間、トラフィックは（前にアクティブであったスーパーバイザ エンジンの）古いデータベースを使用して転送されます。マルチキャスト ルーティング プロトコル コンバージェンスが実行されたあと、新しくアクティブになった Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）によってダウンロードされたショートカットが既存のフローと結合されて新しいショートカットとしてマーキングされます。失効したエントリは、NSF がスイッチオーバー時に機能するように、確実に新しいキャッシュへの円滑な移行を実行する間に、ゆっくりとデータベースから削除されます。

Protocol Independent Multicast（PIM）sparse（疎）モードなどのマルチキャスト ルーティング プロトコルと PIM dense（密）モードがデータ駆動型であるため、マルチキャスト パケットはプロトコルが収束できるようにスイッチオーバー中にルータにリークされます。

トラフィックは双方向 PIM などの制御駆動型プロトコルに対してソフトウェアで転送する必要がないので、スイッチはこれらのプロトコルの古いキャッシュを使用してパケットのリークを継続します。ルータは mroute キャッシュを作成して、ハードウェアにショートカットをインストールします。新しいルートを学習したあと、タイマーがトリガーされ、データベースを捜索して古いフローを消去します。

（注）　マルチキャスト NSF with SSO は、ユニキャスト プロトコルでは NSF のサポートが必要です。

ルーティング プロトコル

ルーティング プロトコルは、アクティブ スーパーバイザ エンジンのマルチレイヤ スイッチ フィーチャ カード（MSFC）上でだけ動作し、近接ルータからルーティング更新を受信します。ルーティング プロトコルは、冗長スーパーバイザ エンジンの MSFC では動作しません。スイッチオーバー後に、ルーティング プロトコルは、ルーティング テーブルの再構築に役立てるために、NSF を認識する近接装置が送信するステート情報を要求します。またこの代わりに、近接装置が NSF を認識しないような環境にある NSF 対応装置のルーティング テーブルの再構築に役立つように、アクティブ スーパーバイザ エンジンからのステート情報を冗長スーパーバイザ エンジンと同期させるように、IS-IS プロトコルを設定できます。Cisco NSF は BGP、OSPF、IS-IS、および Enhanced Interior Gateway Routing Protocol（EIGRP）プロトコルをサポートします。

（注）　NSF 動作の場合、ルーティング プロトコルがルーティング情報を再構築している間、ルーティング プロトコルは CEF に依存してパケット転送を継続します。

BGP の動作

NSF 対応ルータが BGP ピアと BGP セッションを開始するときに、OPEN メッセージをピアに送信します。メッセージには、NSF 対応装置に「グレースフル」リスタート機能があることを示すステートメントが含まれています。グレースフル リスタートとは、スイッチオーバー後に BGP ルーティング ピアでルーティング フラップが発生しないようにするための仕組みです。BGP ピアがこの機能を受信すると、メッセージを送信している装置が NSF 対応であることを認識します。NSF 対応ルータと BGP ピアは、セッション確立時に OPEN メッセージでグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を交換しない場合、このセッションでグレースフル リスタートは行われません。

スーパーバイザ エンジンのスイッチオーバー中に BGP セッションが切断された場合、NSF 認識 BGP ピアは、NSF 対応ルータに関連したすべてのルートを失効とマーキングします。ただし、所定の時間内は、引き続きこれらのルートを転送の決定に使用します。この機能により、新しくアクティブになったスーパーバイザ エンジンが BGP ピアとのルーティング情報のコンバージェンスを待機している間にパケットが消失することを防げます。

スーパーバイザ エンジンのスイッチオーバーが発生したあと、NSF 対応ルータは BGP ピアとのセッションを再構築します。新しいセッションの再構築中に、再起動したときに NSF 対応ルータを識別する新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピア間で交換されています。この交換が完了すると、NSF 対応装置はルーティング情報を使用して RIB と FIB を新しい転送情報で更新します。NSF 認識装置は、ネットワーク情報を使用して失効したルートを BGP テーブルから削除し、これで BGP プロトコルが完全に収束します。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応装置との BGP セッションは確立します。この機能により、NSF 非認識（つまり NSF 機能のない）BGP ピアとのインターオペラビリティが可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタート機能は使用できません。

（注）　NSF での BGP サポートでは、近接ネットワーキング装置が NSF を認識できなければなりません。つまり、装置はグレースフル リスタート機能に対応している必要があり、セッション確立中に OPEN メッセージでその機能をアドバタイズする必要があります。NSF 対応ルータが特定の BGP ネイバにグレースフル リスタート機能がないことを検出すると、NSF 対応セッションをそのネイバと確立しません。グレースフル リスタート機能のある他のすべてのネイバは、この NSF 対応ネットワーキング装置と NSF 対応セッションを継続します。

OSPF の動作

OSPF NSF 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行した場合、リンク ステート データベースを OSPF ネイバと再同期するために、次の作業を実行する必要があります。

- ネイバ関係をリセットせずにネットワーク上の使用可能な OSPF ネイバを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します。

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは OSPF NSF 信号を近接 NSF 認識装置に送信します。近接ネットワーキング装置は、この信号をこのルータとの近接関係がリセットされるべきでないことを示すインジケータとして認識します。NSF 対応ルータがネットワーク上の他のルータから信号を受信すると、近接リストを再構築できます。

近接関係が再確立されたあと、NSF 対応ルータはすべての NSF 認識ネイバとのデータベースの再同期を開始します。この時点で、ルーティング情報は OSPF ネイバ間で交換されています。この交換が完了すると、NSF 対応装置は、ルーティング情報を使用して失効した経路を削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで OSPF プロトコルが完全に収束されます。

（注）　OSPF NSF では、すべての近接ネットワーキング装置が NSF を認識できなければなりません。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバを検出すると、そのセグメントの NSF 機能がディセーブルになります。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

IS-IS の動作

IS-IS 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行した場合、リンク ステート データベースを IS-IS ネイバと再同期するために、次の作業を実行する必要があります。

- ネイバ関係をリセットせずにネットワーク上の使用可能な IS-IS ネイバを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します。

NSF 設定する場合、IS-IS NSF 機能には次の 2 つのオプションがあります。

- Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）IS-IS
- Cisco IS-IS

あるネットワーク セグメントの近接ルータがルータの再起動に関する IETF インターネット ドラフトをサポートするソフトウェア バージョンを実行している場合、再起動する IETF NSF ルータを支援します。IETF を使用すると、近接ルータはスイッチオーバー後のルーティング情報の再構築に役立つ隣接およびリンク ステート情報を提供します。IETF IS-IS 設定のメリットは、標準案に基づくピア装置間の動作にあります。

（注）　ネットワーキング装置で IETF を設定するものの近接ルータが IETF と互換性がない場合、スイッチオーバー後に NSF が打ち切られます。

あるネットワーク セグメントの近接ルータが NSF を認識しない場合、Cisco 設定オプションを使用する必要があります。Cisco IS-IS 設定は、プロトコル隣接およびリンク ステート情報をアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに転送します。Cisco 設定のメリットは、NSF 認識ネイバに依存していないことです。

IETF IS-IS 設定

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは IETF IS-IS 設定を使用して、IS-IS NSF 再起動要求を隣接 NSF 認識装置に送信します。近接ネットワーキング装置は、この再起動要求をこのルータとの近接関係がリセットされるべきでないが、再起動ルータとの間でデータベースの再同期を開始すべきであることを示すインジケータとして認識します。再起動ルータがネットワーク上のルータから再起動要求応答を受信すると、近接リストを再構築できます。

この交換が完了すると、NSF 対応装置はリンク ステート情報を使用して失効したルートを削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで IS-IS が完全に収束されます。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間以内に発生します。IS-IS は、それに数秒プラスしてルーティング テーブルを再確立し、ネットワークと再同期します。この時点で、IS-IS は 2 回目の NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。IS-IS NSF 動作では、IS-IS NSF がもう一度再起動を試行する前に接続が確実に安定するように特定の期間待機します。この機能により、IS-IS が失効した情報でバックツーバック NSF 再起動を試行しないようにします。

Cisco IS-IS 設定

Cisco 設定オプションを使用することで、冗長スーパーバイザ エンジンに対して、すべての隣接および Label Switched Path（LSP; ラベル スイッチド パス）情報が保存されるか、*チェックポイントに設定*されます。スイッチオーバーのあと、新しくアクティブになったスーパーバイザ エンジンはチェックポイント データを使用して隣接を維持し、ルーティング テーブルを迅速に再構築できます。

（注） スイッチオーバーのあと、Cisco IS-IS NSF には完全なネイバ ルータとの隣接関係および LSP 情報があります。ただし、スイッチオーバーの前に隣接であったすべてのインターフェイスがオンラインになるまで待機する必要があります。割り当てられたインターフェイス用の待機時間内にインターフェイスがオンラインにならない場合、近接装置から学習したルートを、ルーティング テーブルの再計算で考慮しないようにします。IS-IS NSF には、何らかの理由で時間内にオンラインにならないインターフェイスに対して、待機時間を延長するコマンドがあります。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間以内に発生します。IS-IS は、それに数秒プラスしてルーティング テーブルを再確立し、ネットワークと再同期します。この時点で、IS-IS は 2 回目の NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。この同期が完了したあと、IS-IS 隣接および LSP データに冗長スーパーバイザ エンジンへのチェックポイントが設定されます。ただし、新しい NSF 再起動は、この期間が経過しないと IS-IS で試行されません。この機能により、IS-IS がバックツーバック NSF 再起動を試行しないようにします。

EIGRP の動作

EIGRP NSF 対応ルータが最初に NSF 再起動から復帰したときには、ネイバはなくトポロジ テーブルは空です。ルータはインターフェイスを立ち上げネイバを再取得し、トポロジとルーティング テーブルを再構築する必要があるときに、冗長（現在アクティブな）スーパーバイザ エンジンから通知を受けます。ルータとピアの再起動では、再起動したルータへ向かうデータ トラフィックを中断せずにこれらの作業を実行する必要があります。EIGRP ピア ルータは、再起動するルータから学習したルートを維持し、NSF 再起動プロセスを通じてトラフィックを転送し続けます。

ネイバによって隣接がリセットされないように、再起動ルータは EIGRP パケット ヘッダーに再起動を示すための新しい再起動（RS）ビットを使用します。RS ビットは、NSF 再起動中に hello パケットと初期 INIT 更新パケットに設定されます。hello パケットの RS ビットにより、ネイバに迅速に NSF 再起動を通知できます。RS ビットを検出しない場合、ネイバは INIT 更新を受信するか hello 保持タイマーの期間が満了することによって、隣接リセットを検出するだけです。RS ビットがないと、ネイバは NSF を使用して隣接リセットが処理されたか、通常のスタートアップを使用して処理されたかを認識しません。

hello パケットまたは INIT パケットを受信することでネイバが再起動表示を受信すると、ピア リスト内のピアが再起動したことを認識し、再起動しているルータとの隣接を維持します。次にネイバは、再起動しているルータに対して、最初の更新パケットに RS ビットを設定してトポロジ テーブルを送信します。この RS ビットは、NSF を認識可能でルータの再起動を支援していることを示します。ネイバが NSF 再起動ネイバでない場合は、hello パケットに RS ビットを設定しません。

（注） ルータが NSF を認識できていても、コールド スタートから立ち上がっているために NSF 再起動ネイバの支援に参加してない場合もあります。

少なくとも 1 つのピア ルータが NSF を認識している場合、再起動ルータは更新を受信しデータベースを再構築します。次に再起動ルータは、RIB を通知できるように収束されているかどうかを検出する必要があります。各 NSF 認識ルータは、テーブルの内容が終わりであることを示すために、最後の更新パケットに End of Table（EOT; テーブルの終わり）マーカを送信する必要があります。EOT マーカを受信すると、再起動ルータは収束していることがわかります。ここで再起動ルータが更新を送信し始めることができます。

NSF 認識ピアは、再起動ルータから EOT 表示を受信したときにいつ再起動ルータが収束したかを認識します。次にピアは、再起動ネイバを送信元としてルートを検索するために、トポロジ テーブルをスキャンします。ピアは、ルートのタイムスタンプと再起動イベント タイムスタンプを比較して、ルートがまだ使用可能かどうかを判断します。次に、ピアはアクティブになり、再起動されたルータで使用できなくなったルートの代替パスを検索します。

再起動ルータがすべての EOT 表示をネイバから受信した場合、または NSF 収束タイマーが満了した場合、EIGRP は RIB にコンバージェンスを通知します。EIGRP は RIB コンバージェンス信号を待機し、待機しているすべての NSF 認識ピアに対してトポロジ テーブルをフラッディングします。

NSF の利点と制約事項

Cisco NSF には次のような利点があります。

- ネットワークの可用性の向上

  NSF は、ユーザのセッション情報がスイッチオーバー後も維持されるように、ネットワーク トラフィックとアプリケーションのステート情報を転送し続けます。

- 全体的なネットワークの安定

  ネットワークの安定性は、ネットワーク内のルータが故障してルーティング テーブルを消失したときに生成されるルート フラップ数を減らすことで改善できます。

- 近接ルータがリンク フラップを検出しない

  スイッチオーバー全体にわたってインターフェイスはアップのままなので、近接ルータはリンク フラップを検出しません（リンクがダウンせずアップに戻ります）。

- ルーティング フラップの回避

  SSO がスイッチオーバー時にネットワーク トラフィックを転送し続けるので、ルーティング フラップが回避されます。

- ユーザ セッションが失われない

  スイッチオーバー前に確立したユーザ セッションは維持されます。

Cisco NSF with SSO には次のような制約事項があります。

- NSF の動作では、装置に SSO を設定しておく必要があります。
- NSF with SSO は、IP バージョン 4 トラフィックおよびプロトコルだけをサポートします。
- Hot Standby Routing Protocol（HSRP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間でステート情報が維持されません。HSRP と SSO は共存できますが、いずれも別々に機能します。HSRP に依存しているトラフィックは、スーパーバイザのスイッチオーバー時に HSRP スタンバイに切り替わる場合があります。
- Gateway Load Balancing Protocol（GLBP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間でステート情報が維持されません。GLBP と SSO は共存できますが、いずれも別々に機能します。GLBP に依存しているトラフィックは、スーパーバイザのスイッチオーバー時に GLBP スタンバイに切り替わる場合があります。
- Virtual Redundancy Routing Protocol（VRRP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間でステート情報が維持されません。VRRP と SSO は共存できますが、いずれも別々に機能します。VRRP に依存しているトラフィックは、スーパーバイザのスイッチオーバー時に VRRP スタンバイに切り替わる場合があります。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は、Cisco NSF with SSO ではサポートされていません。ただし、MPLS と NSF with SSO は共存できます。NSF with SSO が MPLS と同じシャーシに構成されている場合、MPLS プロトコルのフェールオーバー パフォーマンスは少なくとも RRP+ と同等ですが、サポートされている NSF with SSO プロトコルには NSF with SSO の利点が加わります。
- BGP NSF に参加しているすべての近接装置は、NSF 対応で、BGP のグレースフル リスタート用に設定されている必要があります。
- 仮想リンクの OSPF NSF はサポートされていません。

- 同じネットワーク セグメントにあるすべての OSPF ネットワーキング装置は、NSF を認識する必要があります（NSF ソフトウェア イメージを実行している必要があります）。
- IETF IS-IS の場合、すべての近接装置は NSF 認識ソフトウェア イメージを実行している必要があります。
- IPv4 マルチキャスト NSF with SSO は、PFC3 でだけサポートされています。
- 元となるユニキャスト プロトコルはマルチキャスト NSF with SSO を使用するために NSF を認識する必要があります。
- Bidirectional Forwarding Detection（BFD）は SSO を認識せず、NSF with SSO でサポートされません。

スーパーバイザ エンジンの設定の同期化

ここでは、スーパーバイザ エンジンの設定の同期化について説明します。

- 「スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項」（P.7-10）
- 「冗長構成の注意事項および制約事項」（P.7-10）

（注）　Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項

ここでは、スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項について説明します。

- 「冗長構成の注意事項および制約事項」（P.7-10）
- 「ハードウェア設定時の注意事項および制約事項」（P.7-11）
- 「コンフィギュレーション モードに関する制約事項」（P.7-12）

冗長構成の注意事項および制約事項

次の注意事項と制約事項は、すべての冗長モードに適用されます。

- Release 12.2(18)SXD よりも前のリリースでは、冗長スーパーバイザ エンジンがスタンバイ モードにある場合、冗長スーパーバイザ エンジンの 2 つのギガビット イーサネット インターフェイスは常にアクティブです。
- Supervisor Engine 720 の Release 12.2(18)SXE 以降のリリースでは、インストールされているすべてのスイッチング モジュールに DFC がある場合、**fabric switching-mode allow dcef-only** コマンドを入力して両方のスーパーバイザ エンジンでイーサネット ポートをディセーブルにします。これにより、すべてのモジュールが dCEF モードで動作することが保証され、冗長スーパーバイザ エンジンへのスイッチオーバーが簡略化されます。
- Supervisor Engine 2 の Release12.2(18)SXD1 以降のリリースでは、インストールされているすべてのスイッチング モジュールに DFC がある場合、**fabric switching-mode allow dcef-only** コマンドを入力して冗長スーパーバイザ エンジンでイーサネット ポートをディセーブルにします。これにより、すべてのモジュールが dCEF モードで動作することが保証されます。

- スーパーバイザ エンジンを冗長構成にしても、スーパーバイザ エンジンのミラーリングやロードバランシングは行われません。スーパーバイザ エンジンのうちの 1 台だけがアクティブになります。
- SNMP を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。
- スーパーバイザ エンジンのスイッチオーバーは、障害のあるスーパーバイザ エンジンがコア ダンプを完了したあとに行われます。コア ダンプには最大で 15 分間かかります。スイッチオーバー時間を短縮するには、スーパーバイザ エンジンでコア ダンプをディセーブルにします。
- Supervisor Engine 720 の Release 12.2(18)SXF 以降のリリースでは、ファブリック同期化のエラーが発生した場合、デフォルト動作である冗長スーパーバイザ エンジンへのスイッチオーバーが行われます。場合によっては、冗長スーパーバイザ エンジンへのスイッチオーバーの方が、ファブリック同期化エラーの原因となったモジュールの電源切断よりも中断が長くなります。スイッチオーバーをディセーブルにして、ファブリック同期化エラーが発生したモジュールの電源を切断するには、**no fabric error-recovery fabric-switchover** コマンドを入力します。

ハードウェア設定時の注意事項および制約事項

冗長運用を行うには、次の注意事項および制約事項に従う必要があります。

- スーパーバイザ エンジンおよび MSFC で実行する Cisco IOS は、スーパーバイザ エンジンおよび MSFC ルータが同一である冗長構成をサポートします。スーパーバイザ エンジンおよび MSFC ルータが同一でない場合、片方が最初に起動されてアクティブになり、もう一方がリセット状態で保留されます。
- 各スーパーバイザ エンジンが単独でスイッチを稼動させるためのリソースを備えているスーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ装置を含む）が重複している必要があります。
- スーパーバイザ エンジンごとに個別のコンソール接続を行ってください。コンソール ポートに Y 字ケーブルを接続しないでください。
- 両方のスーパーバイザ エンジン内のシステム イメージが同じである必要があります（「冗長スーパーバイザ エンジンへのファイルのコピー」（P.7-21）を参照）。

（注）　新たに取り付けられた冗長スーパーバイザ エンジン上で Catalyst OS（オペレーティング システム）がインストールされている場合は、アクティブなスーパーバイザ エンジンを取り外して、冗長スーパーバイザ エンジンだけが搭載されている状態でスイッチを起動します。最新のリリース ノートの手順に従って、Catalyst OS から冗長スーパーバイザ エンジンを変換してください。

- startup-config のコンフィギュレーション レジスタが自動起動用に設定されている必要があります。

（注）　ネットワークからの起動はサポートされていません。

コンフィギュレーション モードに関する制約事項

スタートアップ同期プロセス中は、設定に関して次の制約事項が適用されます。

- スタートアップ（一括）同期中は、設定を変更できません。このプロセス中に設定を変更しようとすると、次のメッセージが生成されます。

  ```
  Config mode locked out till standby initializes
  ```

- スーパーバイザ エンジンのスイッチオーバー時に設定を変更した場合、その変更内容は失われます。

NSF 設定作業

次に、NFS 機能の設定作業について説明します。

SSO の設定

NSF をサポートしているプロトコルで NSF を使用するには SSO を設定する必要があります。SSO を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-red)# mode sso`	SSO を設定します。このコマンドを入力すると、冗長スーパーバイザ エンジンがリロードされ、SSO モードでの処理が開始されます。
ステップ 3	`Router# show running-config`	SSO がイネーブルになっていることを確認します。
ステップ 4	`Router# show redundancy states`	動作中の冗長モードを表示します。

（注）　**sso** キーワードは、Release 12.2(17b)SXA 以降でサポートされます。

次に、システムを SSO 用に設定して、冗長ステートを表示する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# end
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 29
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0
Router#
```

マルチキャスト MLS NSF with SSO の設定

（注）　このセクションのコマンドはオプションで、設定をカスタマイズするのに使用できます。ほとんどのユーザは、デフォルト設定で十分です。

マルチキャスト MLS NSF with SSO は、SSO が冗長モードとして選択されている場合にデフォルトでオンです。マルチキャスト NSF with SSO パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# mls ip multicast sso convergence-time` *time*	プロトコルのコンバージェンス用に待機する最大時間を指定します。有効な範囲は、0 ～ 3600 秒です。
ステップ 3	`Router(config)# mls ip multicast sso leak` *interval*	パケット リーク インターバルを指定します。有効な範囲は、0 ～ 3600 秒です。PIM sparse（疎）モードおよび PIM dense（密）モードの場合、これは既存の PIM sparse モードおよび PIM dense モード マルチキャスト転送エントリのパケット リーキングが完了したあとの期間です。
ステップ 4	`Router(config)# mls ip multicast sso leak` *percentage*	マルチキャスト フローの割合を指定します。有効な範囲は、1 ～ 100 % です。この値は、パケット リーキングに対してフラグ付けされている既存の PIM sparse（疎）モードおよび PIM dense（密）モード マルチキャスト フローの合計数の割合を示します。

マルチキャスト NSF with SSO の確認

マルチキャスト NSF with SSO 設定を確認するには、**show mls ip multicast sso** コマンドを入力します。

```
router# show mls ip multicast sso
Multicast SSO is enabled
Multicast HA Parameters
-------------------------------------------------+------+
protocol convergence timeout                     120 secs
flow leak percent                                10
flow leak interval                               60 secs
```

CEF NSF の設定

ネットワーキング装置が SSO モードで動作している間、CEF NSF 機能はデフォルトで動作します。設定作業は不要です。

CEF NSF の確認

CEF が NSF に対応していることを確認するには、**show cef state** コマンドを入力します。

```
router# show cef state

CEF Status [RP]
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:      yes
Default CEF switching:     yes
Default dCEF switching:    yes
Update HWIDB counters:     no
Drop multicast packets:    no
.
.
.
CEF NSF capable:           yes
IPC delayed func on SSO:   no
RRP state:
I am standby RRP:          no
My logical slot:           0
RF PeerComm:               no
```

BGP NSF の設定

（注）　BGP NSF に参加しているすべてのピア装置に BGP のグレースフル リスタートを設定する必要があります。

NSF の BGP を設定するには、次の作業を行います（各 BGP NSF ピア装置でこの手順を繰り返します）。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router bgp as-number`	BGP ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# bgp graceful-restart`	BGP のグレースフル リスタート機能をイネーブルにして、BGP の NSF を開始します。 BGP セッションが確立されたあとにこのコマンドを入力した場合、BGP ネイバとグレースフル リスタート機能を交換するためにセッションを再起動する必要があります。 再起動ルータとすべてのピアでこのコマンドを使用します。

BGP NSF の確認

BGP の NSF を確認するには、グレースフル リスタート機能が SSO 対応ネットワーキング装置とその近接装置に設定されているかを確認する必要があります。これを確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、「bgp graceful-restart」が SSO 対応ルータの BGP 設定にあることを確認します。

```
Router# show running-config

.
.
.
router bgp 120
.
.
.
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
.
.
.
```

ステップ 2　各 BGP ネイバでステップ 1 を繰り返します。

ステップ 3　SSO 装置と近接装置で、グレースフル リスタート機能が受信されアドバイタイズされたものとして表示されているかを確認し、グレースフル リスタート機能のあるアドレス ファミリーを確認します。アドレス ファミリーがリストされていない場合、BGP NSF も発生しません。

```
router# show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Address famiiy IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

OSPF NSF の設定

（注）　OSPF NSF に参加しているすべてのピア装置は OSPF NSF 対応でなければならず、NSF ソフトウェア イメージを装置にインストールすれば自動的に対応するようになります。

OSPF NSF 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	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# nsf`	OSPF の NSF 動作をイネーブルにします。

OSPF NSF の確認

OSPF の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。OSPF NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応装置の OSPF 設定に表示されることを確認します。

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
.
.
```

ステップ 2　**show ip ospf** コマンドを入力して NSF が装置でイネーブルであることを確認します。

```
router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

IS-IS NSF の動作

IS-IS NSF 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	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router isis` [*tag*]	IS-IS ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。

	コマンド	目的
ステップ 3	`Router(config-router)# nsf [cisco | ietf]`	IS-IS の NSF 動作をイネーブルにします。 **ietf** キーワードを入力して、ネットワーキング装置の隣接装置が IETF ドラフト ベースの再起動性をサポートしていることを保証している同種ネットワークで IS-IS をイネーブルにします。 **cisco** キーワードを入力して、NSF 認識ネットワーキング装置との隣接装置がない異種ネットワークで IS-IS を実行します。
ステップ 4	`Router(config-router)# nsf interval [minutes]`	（任意）NSF 再起動試行間の最小時間を指定します。*連続する* NSF 再起動のデフォルトの時間間隔は、5 分です。
ステップ 5	`Router(config-router)# nsf t3 {manual [seconds] | adjacency}`	（任意）IS-IS 自身のリンク ステート情報の生成が過負荷になり、その情報がネイバにフラッディングする前に、IS-IS が IS-IS データベースの同期を待機する時間を指定します。 IETF 動作を選択した場合だけ、**t3** キーワードが適用されます。**adjacency** を指定した場合、再起動しているルータは近接装置から待機時間を取得します。
ステップ 6	`Router(config-router)# nsf interface wait seconds`	（任意）再起動が完了する前に、IS-IS 隣接とのインターフェイスがすべて立ち上がるまで、IS-IS NSF の再起動を待機する長さを指定します。デフォルト値は 10 秒です。

IS-IS NSF の確認

IS-IS の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。IS-IS NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応装置の IS-IS 設定にあることを確認します。Cisco IS-IS または IETF IS-IS 設定のいずれかが表示されます。次の表示は、装置で IS-IS NSF のシスコ実装を使用していることを示しています。

```
Router# show running-config
<...Output Truncated...>
router isis
nsf cisco
<...Output Truncated...>
```

ステップ 2　NSF 設定が **cisco** に設定されている場合、**show isis nsf** コマンドを使用して NSF が装置でイネーブルであることを確認します。シスコ設定を使用すると、表示出力はアクティブ RP と冗長 RP で異なります。次の表示は、アクティブ RP 上の Cisco 設定の出力例です。この例で、「NSF restart enabled」があることを確認してください。

```
router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

次の表示は、スタンバイ RP 上のシスコ設定の出力例です。この例で、「NSF restart enabled」があることを確認してください。

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

ステップ 3　NSF 設定が **ietf** に設定されている場合、**show isis nsf** コマンドを使用して NSF が装置でイネーブルであることを確認します。次の表示は、ネットワーキング装置上の IETF IS-IS 設定の出力例です。

```
router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

EIGRP NSF の設定

EIGRP NSF 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	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router eigrp` *as-number*	EIGRP ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# nsf`	EIGRP NSF をイネーブルにします。 再起動ルータとすべてのピアでこのコマンドを使用します。

EIGRP NSF の確認

EIGRP の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。EIGRP NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応装置の EIGRP 設定に表示されることを確認します。

```
Router# show running-config
.
.
.
router eigrp 100
 auto-summary
 nsf
.
.
.
```

ステップ 2　**show ip protocols** コマンドを入力して NSF が装置でイネーブルであることを確認します。

```
Router# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
```

```
Distance: internal 90 external 170
```

スーパーバイザ エンジンの設定の同期化

通常の動作時には、2 つのスーパーバイザ エンジン間で startup-config および config-register 設定がデフォルトで同期化されます。スイッチオーバー時には、新しいアクティブ スーパーバイザ エンジンが現在の設定を使用します。

冗長スーパーバイザ エンジンへのファイルのコピー

次のコマンドを使用して、冗長スーパーバイザ エンジン上の **disk0:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavedisk0:target_filename
```

次のコマンドを使用して、冗長スーパーバイザ エンジン上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavesup-bootflash:target_filename
```

次のコマンドを使用して、冗長 MSFC 上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavebootflash:target_filename
```

CHAPTER 8

Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定

この章では、Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）を使用してスーパーバイザ エンジンの冗長構成を設定する方法について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- すべてのリリースで RPR および RPR+ をサポートしています。
- Release 12.2(18)SXE 以降のリリースの場合、RPR および RPR+ は IPv6 マルチキャスト トラフィックをサポートしています。
- Release 12.2(18)SXD 以降のリリースでは、Nonstop Forwarding（NSF; ノンストップ フォワーディング）with Stateful Switchover（SSO; ステートフル スイッチオーバー）をすべてのスーパーバイザ エンジンでサポートしていま（第 7 章「NSF with SSO スーパーバイザ エンジンの冗長構成の設定」を参照）。

この章で説明する内容は、次のとおりです。

RPR および RPR+ の概要

ここでは、RPR および RPR+ を使用したスーパーバイザ エンジンの冗長構成の概要について説明します。

スーパーバイザ エンジンの冗長構成の概要

Catalyst 6500 シリーズ スイッチは、プライマリ スーパーバイザ エンジンが故障した場合に冗長スーパーバイザ エンジンに処理を引き継ぐことにより、耐障害性を強化することができます。
Catalyst 6500 シリーズ スイッチは、次の冗長モードをサポートします。

- RPR - 2 分以上のスイッチオーバー時間をサポートします。
- Route Processor Redundancy plus（RPR+）- 30 秒以上のスイッチオーバー時間をサポートします。

次のイベントが発生すると、スイッチオーバーが行われます。

- アクティブ スーパーバイザ エンジンでのハードウェア障害
- スーパーバイザ エンジン間のクロック同期損失
- 手動スイッチオーバー

RPR の動作

RPR は次の機能をサポートします。

- 自動スタートアップおよびアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジン間の bootvar の同期化
- スーパーバイザ エンジンのアクティブ ステータスまたは冗長ステータスを検出および決定するハードウェア信号
- アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへ、60 秒間隔でクロック同期化を実行
- 冗長スーパーバイザ エンジンは、起動してもすべてのサブシステムが稼動するわけではなく、アクティブ スーパーバイザ エンジンが故障した場合に、完全に動作可能になります。
- 故障した装置の代わりに動作可能なスーパーバイザ エンジンが、冗長スーパーバイザ エンジンになります。
- Fast Software Upgrade（FSU）のサポート（「Fast Software Upgrade の実行」（P.8-9）を参照）。

スイッチの電源投入時に、2 つのスーパーバイザ エンジン間で RPR が稼動します。最初に起動したスーパーバイザ エンジンが RPR アクティブ スーパーバイザ エンジンになります。Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）および Policy Feature Card（PFC; ポリシー フィーチャ カード）は完全に動作可能になります。冗長スーパーバイザ エンジン上の MSFC および PFC はリセットされますが、動作可能にはなりません。

スイッチオーバーが行われると、冗長スーパーバイザ エンジンが完全に動作可能になり、次の動作が行われます。

- すべてのスイッチ モジュールの電源が再びオンになります。
- MSFC 上の残りのサブシステム（レイヤ 2 およびレイヤ 3 プロトコルを含む）が起動されます。
- Access Control List（ACL; アクセス制御リスト）がスーパーバイザ エンジンのハードウェアに再度プログラミングされます。

（注）　スイッチオーバー時には、一部のアドレス ステートが失われ、ダイナミックに再確認したあとで復元されるので、トラフィックが一時中断されます。

RPR+ の動作

RPR+ モードを使用すると、冗長スーパーバイザ エンジンは完全に初期化および設定され、スイッチオーバー時間が短縮されます。冗長スーパーバイザ エンジンがオンライン状態になると、アクティブなスーパーバイザ エンジンは冗長スーパーバイザ エンジンのイメージ バージョンをチェックします。冗長スーパーバイザ エンジン上のイメージがアクティブなスーパーバイザ エンジン上のイメージと一致しない場合は、RPR 冗長モードが使用されます。

RPR+ を使用すると、冗長スーパーバイザ エンジンが完全に初期化および設定されるので、アクティブなスーパーバイザ エンジンが故障した場合、または手動によるスイッチオーバーが実行された場合に、スイッチオーバー時間が短縮されます。

スイッチの電源投入時に、2 つのスーパーバイザ エンジン間で RPR+ が稼動します。最初に起動したスーパーバイザ エンジンがアクティブ スーパーバイザ エンジンになります。マルチレイヤ スイッチ フィーチャ カード（MSFC）および ポリシー フィーチャ カード（PFC）は完全に動作可能になります。冗長スーパーバイザ エンジン上の MSFC および PFC はリセットされますが、動作可能にはなりません。

RPR+ は、RPR に次の利点を追加して強化したものです。

- スイッチオーバー時間の短縮

  設定に応じて、スイッチオーバー時間が 30 秒以上になります。

- 搭載されたモジュールはリロードされない

  スタートアップ コンフィギュレーションと実行コンフィギュレーションの両方が、アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへ絶えず同期化されるため、搭載されたモジュールはスイッチオーバー中にリロードされません。

- 冗長スーパーバイザ エンジンの Online Insertion and Removal（OIR; ホットスワップ）

  RPR+ を使用すると、メンテナンスするときに冗長スーパーバイザ エンジンの OIR を実行できます。冗長スーパーバイザ エンジンを取り付けると、アクティブなスーパーバイザ エンジンが冗長スーパーバイザ エンジンの存在を検出し、冗長スーパーバイザ エンジンを完全に初期化されたステートに移行させ始めます。

- OIR イベントの同期化
- **redundancy force-switchover** コマンドによる手動でのスイッチオーバーの開始

スーパーバイザ エンジンの設定の同期化

ここでは、スーパーバイザ エンジンの設定の同期化について説明します。

- 「RPR スーパーバイザ エンジンの設定の同期化」（P.8-4）
- 「RPR+ スーパーバイザ エンジンの設定の同期化」（P.8-4）

（注）　SNMP を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こし、RPR+ により冗長スーパーバイザ エンジンおよび MSFC をリロードします。

RPR スーパーバイザ エンジンの設定の同期化

RPR モードの動作時には、2 つのスーパーバイザ エンジン間で startup-config ファイルおよび config-register コンフィギュレーションがデフォルトで同期化されます。スイッチオーバー時には、新しいアクティブ スーパーバイザ エンジンが現在の設定を使用します。

RPR+ スーパーバイザ エンジンの設定の同期化

RPR+ モードを使用している場合、次の動作が設定の同期化を引き起こします。

- 冗長スーパーバイザ エンジンを最初にオンラインにすると、アクティブなスーパーバイザ エンジンから冗長スーパーバイザ エンジンへ、startup-config ファイルがコピーされます。この同期化により、冗長スーパーバイザ エンジン上にある既存のスタートアップ コンフィギュレーション ファイルが上書きされます。
- 通常の動作中に設定が変更されると、冗長運用によりアクティブなスーパーバイザ エンジンから冗長スーパーバイザ エンジンへの差分同期が実行されます。冗長運用により、アクティブなスーパーバイザ エンジンから冗長スーパーバイザ エンジンへ、ユーザが入力した Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドが行単位で差分同期化されます。

冗長スーパーバイザ エンジンが完全に初期化されている場合でも、コンフィギュレーション ファイルが変更されたときに変更の差分を受け取れるように、アクティブなスーパーバイザ エンジンとの相互通信だけは行います。冗長スーパーバイザ エンジンでは CLI コマンドを入力できません。

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項

ここでは、スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項について説明します。

- 「冗長構成の注意事項および制約事項」（P.8-5）
- 「RPR+ に関する注意事項および制約事項」（P.8-5）
- 「ハードウェア設定時の注意事項および制約事項」（P.8-6）
- 「コンフィギュレーション モードに関する制約事項」（P.8-7）

冗長構成の注意事項および制約事項

RPR および RPR+ 冗長モードには、次の注意事項および制約事項が適用されます。

- 冗長スーパーバイザ エンジン 720 上の 2 つのギガビット イーサネット インターフェイスは常にアクティブです。
- スーパーバイザ エンジンを冗長構成にしても、スーパーバイザ エンジンのミラーリングやロードバランシングは行われません。スーパーバイザ エンジンのうちの 1 台だけがアクティブになります。
- SNMP を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こし、RPR+ により冗長スーパーバイザ エンジンおよび MSFC をリロードします。
- スーパーバイザ エンジンのスイッチオーバーは、障害のあるスーパーバイザ エンジンがコア ダンプを完了したあとに行われます。コア ダンプには最大で 15 分間かかります。スイッチオーバー時間を短縮するには、スーパーバイザ エンジンでコア ダンプをディセーブルにします。

RPR+ に関する注意事項および制約事項

RPR+ には、次の注意事項および制約事項が適用されます。

- 冗長スーパーバイザ エンジンが処理を引き継いでスイッチが回復するまで、ネットワーク サービスは中断されます。
- Forwarding Information Base（FIB; 転送情報ベース）テーブルはスイッチオーバー時に消去されます。その結果、ルート テーブルの再コンバージェンスが行われるまで、ルーティング対象トラフィックは中断されます。
- スタティック IP ルートはコンフィギュレーション ファイル内のエントリから設定されるため、スイッチオーバー中も維持されます。
- アクティブなスーパーバイザ エンジン上で維持されるダイナミックなステート情報は、冗長スーパーバイザ エンジンに同期化されないため、スイッチオーバー時に失われます。

  次に、スイッチオーバー時に失われるダイナミックなステート情報の例を示します。

  - フレーム リレー Switched Virtual Circuit（SVC; 相手先選択接続）

  （注） フレーム リレーでスイッチングされる Data Link Connection Identifier（DLCI）設定はコンフィギュレーション ファイル内に保存されているため、フレーム リレーでスイッチングされる DLCI 情報はスイッチオーバー中も維持されます。

  - 中断されたすべての PPP（ポイントツーポイント プロトコル）セッション
  - すべての Asynchronous Transfer Mode（ATM; 非同期転送モード）SVC 情報
  - 中断されたすべての TCP、およびその他のコネクション型レイヤ 3 およびレイヤ 4 セッション
  - BGP セッション
  - Automatic Protection System（APS; 自動保護システム）ステート情報
- 両方のスーパーバイザ エンジンで同じバージョンの Cisco IOS ソフトウェアが稼動している必要があります。両方のスーパーバイザ エンジンで同じバージョンの Cisco IOS ソフトウェアが稼動していない場合は、冗長スーパーバイザ エンジンが RPR モードでオンライン状態になります。

- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンを搭載したスイッチに、**vtp file** *file_name* コマンドを入力しないでください。
- 冗長スーパーバイザ エンジンを取り付ける前に、デフォルト設定に戻すには **no vtp file** コマンドを入力します。
- スーパーバイザ エンジンの冗長構成では、VLAN データベース モードで入力された設定をサポートしていません。RPR+ 冗長構成には、グローバル コンフィギュレーション モードを使用します（第 14 章「仮想 LAN（VLAN）の設定」を参照）。

ハードウェア設定時の注意事項および制約事項

冗長運用を行うには、次の注意事項および制約事項に従う必要があります。

- スーパーバイザ エンジンおよび MSFC で実行する Cisco IOS は、スーパーバイザ エンジンおよび MSFC ルータが同一である冗長構成をサポートします。スーパーバイザ エンジンおよび MSFC ルータが同一でない場合、片方が最初に起動されてアクティブになり、もう一方がリセット状態で保留されます。
- 各スーパーバイザ エンジンが単独でスイッチを稼動させるためのリソースを備えているスーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ装置を含む）が重複している必要があります。
- スーパーバイザ エンジンごとに個別のコンソール接続を行ってください。コンソール ポートに Y 字ケーブルを接続しないでください。
- 両方のスーパーバイザ エンジン内のシステム イメージが同じである必要があります（「MSFC へのファイルのコピー」（P.8-11）を参照）。

（注）　新たに取り付けられた冗長スーパーバイザ エンジン上で Catalyst OS（オペレーティング システム）がインストールされている場合は、アクティブなスーパーバイザ エンジンを取り外して、冗長スーパーバイザ エンジンだけが搭載されている状態でスイッチを起動します。最新のリリース ノートの手順に従って、Catalyst OS から冗長スーパーバイザ エンジンを変換してください。

- startup-config のコンフィギュレーション レジスタが自動起動用に設定されている必要があります（「ブート フィールドの変更」（P.3-24）を参照）。

（注）　ネットワークからの起動はサポートされていません。

Release 12.2(17b)SXA よりも前のリリースでこれらの要件が満たされると、スイッチで RPR+ モードがデフォルトで機能します。

コンフィギュレーション モードに関する制約事項

スタートアップ同期プロセス中は、設定に関して次の制約事項が適用されます。

- スタートアップ（一括）同期中は、設定を変更できません。このプロセス中に設定を変更しようとすると、次のメッセージが生成されます。

  ```
  Config mode locked out till standby initializes
  ```

- スーパーバイザ エンジンのスイッチオーバー時に設定を変更した場合、その変更内容は失われます。

スーパーバイザ エンジンの冗長構成の設定

ここでは、スーパーバイザ エンジンの冗長構成を設定する手順について説明します。

- 「冗長運用の設定」（P.8-7）
- 「スーパーバイザ エンジンの設定の同期化」（P.8-8）
- 「冗長ステートの表示」（P.8-8）

冗長運用の設定

冗長運用を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-red)# mode { rpr | rpr-plus}`	RPR または RPR+ を設定します。このコマンドを入力すると、冗長スーパーバイザ エンジンがリロードされ、RPR または RPR+ モードでの処理が開始されます。
ステップ 3	`Router# show running-config`	RPR または RPR+ がイネーブルになっていることを確認します。
ステップ 4	`Router# show redundancy states`	動作中の冗長モードを表示します。

次に、システムを RPR+ 用に設定して、冗長ステートを表示する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode rpr-plus
Router(config-red)# end
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy Plus
Redundancy Mode (Configured)  = Route Processor Redundancy Plus
     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode

   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0

Router#
```

スーパーバイザ エンジンの設定の同期化

通常の動作時には、2 つのスーパーバイザ エンジン間で startup-config および config-register 設定がデフォルトで同期化されます。スイッチオーバー時には、新しいアクティブ スーパーバイザ エンジンが現在の設定を使用します。

（注）　デフォルトの auto-sync 設定は変更しないでください。

冗長ステートの表示

冗長ステートを表示するには、次の作業を行います。

コマンド	目的
`Router# show redundancy states`	冗長ステートを表示します。

次に、冗長ステートを表示する例を示します。

```
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy Plus
Redundancy Mode (Configured)  = Route Processor Redundancy Plus
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 18
           RF debug mask = 0x0

Router#
```

Fast Software Upgrade の実行

RPR でサポートされている Fast Software Upgrade（FSU）手順を使用すると、システムをリロードしなくても、スーパーバイザ エンジン上の Cisco IOS イメージをアップグレードできます。

（注）　EHSA から RPR へのアップグレードを初めて実行する場合は、両方のスーパーバイザ エンジンをリロードする必要があります。EHSA から FSU への移行はサポートされていません。

FSU を実行するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router# **copy** *source_device*:*source_filename* {**disk0 | disk1**}:*target_filename*	新しい Cisco IOS イメージをアクティブ スーパーバイザ エンジン上の **disk0:** 装置または **disk1:** 装置にコピーします。
	または	
	Router# **copy** *source_device*:*source_filename* **sup-bootflash:***target_filename*	新しい Cisco IOS イメージをアクティブ スーパーバイザ エンジン上の **bootflash:** 装置にコピーします。
	または	
	Router# **copy** *source_device*:*source_filename* {**slavedisk0 | slavedisk1**}:*target_filename*	新しい Cisco IOS イメージを冗長スーパーバイザ エンジン上の **disk0:** 装置または **disk1:** 装置にコピーします。
	または	
	Router# **copy** *source_device*:*source_filename* **slavesup-bootflash:***target_filename*	新しい Cisco IOS イメージを冗長スーパーバイザ エンジン上の **bootflash:** 装置にコピーします。
ステップ 2	Router# **config terminal** Router(config)# **config-register 0x2102** Router(config)# **boot system flash** *device*:*file_name*	新しいイメージを起動するように、スーパーバイザ エンジンを設定します。
ステップ 3	Router# **copy running-config start-config**	設定を保存します。
ステップ 4	Router# **hw-module** {*module num*} **reset**	冗長スーパーバイザ エンジンをリロードして、再びオンライン状態に戻します（新しいバージョンの Cisco IOS ソフトウェアを実行します）。 **（注）** 冗長スーパーバイザ エンジンをリロードする前に、すべての設定の同期変更が完了するまで、十分に待機してください。
ステップ 5	Router# **redundancy force-switchover**	冗長スーパーバイザ エンジンへのスイッチオーバーを手動で実行します。冗長スーパーバイザ エンジンが新しいアクティブ スーパーバイザ エンジンになり、新しい Cisco IOS イメージが稼動します。モジュールがリロードされ、モジュール ソフトウェアが新しいアクティブ スーパーバイザ エンジンからダウンロードされます。 それまでアクティブだったスーパーバイザ エンジンが新しいイメージで再起動され、冗長スーパーバイザ エンジンになります。 **（注）** EHSA から RPR への FSU 処理を実行するには、ステップ 5 で **reload** コマンドを実行します。

次に、FSU の実行例を示します。

```
Router# config terminal
Router(config)# config-register 0x2102
Router(config)# boot system flash disk0:image_name
Router# copy running-config start-config
Router# hw-module reset
Router# redundancy force-switchover
Router#
```

MSFC へのファイルのコピー

次のコマンドを使用して、アクティブ MSFC 上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename bootflash:target_filename
```

次のコマンドを使用して、冗長 MSFC 上の **bootflash:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavebootflash:target_filename
```

CHAPTER 9

インターフェイスの設定

この章では、Catalyst 6500 シリーズ スイッチにインターフェイスを設定する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。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

インターフェイス設定の概要

ソフトウェアの多くの機能は、インターフェイス単位で有効になります。**interface** コマンドを入力する場合、次の情報を指定する必要があります。

- インターフェイス タイプ
  - イーサネット（**ethernet** キーワードを使用）
  - ファスト イーサネット（**fastethernet** キーワードを使用）
  - ギガビット イーサネット（**gigabitethernet** キーワードを使用）
  - 10 ギガビット イーサネット（**tengigabitethernet** キーワードを使用）

（注）　WAN インターフェイスについては、WAN モジュールのコンフィギュレーション ノートを参照してください。

- スロット番号 - モジュールの搭載先スロットです。Catalyst 6500 シリーズ スイッチの各スロットには、上から下へ、1 から始まる通し番号が付けられています。
- ポート番号 - モジュールの物理的なポート番号です。Catalyst 6500 シリーズ スイッチのポート番号は、常に 1 から始まります。通し番号は、スイッチを背面から見たときに左から右へと大きくなっていくように付けられています。

各ポートは、物理的な位置によって識別できます。また、**show** コマンドを使用して、特定のポートまたはすべてのポートに関する情報を表示することもできます。

interface コマンドの使用

（注）　ここに記載されているコマンドは、物理ポートと論理インターフェイスの両方を設定するために使用します。

次の手順は、すべてのインターフェイス設定作業に当てはまります。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の設定作業を開始します。インターフェイス コマンドを使用するには、次の作業を行います。

ステップ 1　イネーブル EXEC プロンプトで **configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

ステップ 2　グローバル コンフィギュレーション モードで **interfaces** コマンドを入力します。インターフェイス タイプ、およびコネクタ（インターフェイス カード）の番号を指定します。

次の例では、ファスト イーサネット、スロット 5、インターフェイス 1 を選択しています。

```
Router(config)# interfaces fastethernet 5/1
Router(config-if)#
```

ステップ 3　インストールされているインターフェイスの全リストを表示するには、**show interfaces** EXEC コマンドを入力します。次の出力例のように、装置がサポートするインターフェイスごとにレポートが表示されます。

```
Router# show interfaces fastethernet 5/48
FastEthernet5/48 is up, line protocol is up
  Hardware is C6k 100Mb 802.3, address is 0050.f0ac.3083 (bia 0050.f0ac.3083)
  Internet address is 172.20.52.18/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
```

```
  5 minute output rate 1000 bits/sec, 1 packets/sec
     4834677 packets input, 329545368 bytes, 0 no buffer
     Received 4796465 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     51926 packets output, 15070051 bytes, 0 underruns
     0 output errors, 2 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

ステップ 4　**show hardware** EXEC コマンドを入力して、システム ソフトウェアおよびハードウェアのリストを表示します。

```
Router# show hardware
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPLOY)
Synced to mainline version: 12.1(5c)
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 28-Mar-01 17:52 by hqluong
Image text-base: 0x30008980, data-base: 0x315D0000

ROM: System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
BOOTFLASH: c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPL)

Router uptime is 2 hours, 55 minutes
System returned to ROM by power-on (SP by power-on)
Running default software

cisco Catalyst 6000 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Virtual Ethernet/IEEE 802.3  interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2

Router#
```

ステップ 5　イネーブル EXEC プロンプトで **interface** キーワード、インターフェイス タイプ、およびスロット番号/ポート番号を入力して、ファスト イーサネット ポート 5/5 の設定を開始する例を次に示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/5
Router(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は、スペースは不要です。上記の例では、*fastethernet 5/5* または *fastethernet5/5* のどちらを入力してもかまいません。

ステップ 6　**interface** コマンドに続いて、個々の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上で実行されるプロトコルおよびアプリケーションが決まります。別の **interface** コマンドを入力するか、または **Ctrl+Z** を押してインターフェイス コンフィギュレーション モードを終了し、イネーブル EXEC モードに戻るまで、入力したコマンドが収集され、対応する **interface** コマンドに適用されます。

ステップ 7　インターフェイスを設定したあと、「インターフェイスのモニタおよびメンテナンス」（P.9-18）に記載されている **show** EXEC コマンドを使用して、インターフェイスのステータスを確認します。

インターフェイスの範囲設定

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、入力したすべてのコマンド パラメータが、その範囲内の全インターフェイスに適用されます。

同じ設定を持つインターフェイスの範囲を設定するには、次の作業を行います。

コマンド	目的
Router(config)# [**no**] **interface range** {{**vlan** *vlan_ID - vlan_ID* [, **vlan** *vlan_ID - vlan_ID*]} | {*type*[1] *slot/port - port* [, *type*[1] *slot/port - port*]} | {*macro_name* [, *macro_name*]}}	設定するインターフェイスの範囲を選択します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

インターフェイスの範囲を設定する際、次の情報に注意してください。

- マクロの詳細については、「インターフェイス レンジ マクロの定義および使用」（P.9-6）を参照してください。
- カンマで区切って、範囲を 5 つまで入力できます。
- カンマの前後にスペースは必要ありません。
- Release12.2(18)SXE よりも前のリリースでは、**interface range** コマンドを使用する場合にインターフェイス番号とダッシュの間にスペースを入れる必要があります。たとえば、**interface range fastethernet 1 - 5** は有効な構文ですが、**interface range fastethernet 1-5** は無効です。
- Release12.2(18)SXE 以降のリリースでは、**interface range** コマンドを使用する場合にインターフェイス番号とダッシュの間にスペースを入れる必要がありません。
- Release12.2(18)SXD よりも前のリリースでは、**no interface range** コマンドは VLAN インターフェイスをサポートしません。
- Release12.2(18)SXD 以降のリリースでは、**no interface range** コマンドは VLAN インターフェイスをサポートします。
- Release12.2(18)SXD よりも前のリリースでは、VLAN インターフェイスの場合、**interface range** コマンドはレイヤ 2 VLAN が **interface vlan** コマンドで作成された VLAN インターフェイスのみをサポートします（**show running-configuration** コマンドが設定済みの VLAN インターフェイスを表示します）。**interface range** コマンドは、**show running-configuration** コマンドで表示されない VLAN インターフェイスをサポートしません。
- Release12.2(18)SXD 以降のリリースでは、レイヤ 2 VLAN が **interface vlan** コマンドで作成されていない VLAN インターフェイスを **interface range** コマンドでサポートします。

（注）　リンク ステート メッセージ（[LINK-3-UPDOWN] および [LINEPROTO-5-UPDOWN]）は、デフォルトではディセーブルに設定されています。このメッセージをイネーブルにするには、各インターフェイスに対して **logging event link status** コマンドを使用します。

次に、ファスト イーサネット ポート 5/1 ～ 5/5 を再びイネーブルにする例を示します。

```
Router(config)# interface range fastethernet 5/1 - 5
Router(config-if)# no shutdown
Router(config-if)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Router(config-if)#
```

次に、カンマを使用して、タイプの異なるインターフェイス ストリングを追加して範囲を指定し、ファスト イーサネット ポート 5/1 ～ 5/5 と、ギガビット イーサネット ポート 1/1 および 1/2 を再びイネーブルにする例を示します。

```
Router(config-if)# interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Router(config-if)# no shutdown
Router(config-if)#
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to
 up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state to
 up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Router(config-if)#
```

インターフェイス レンジ コンフィギュレーション モードで、複数のコンフィギュレーション コマンドを入力する場合、各コマンドは入力するたびに実行されます（インターフェイス レンジ コンフィギュレーション モードの終了後にまとめて実行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 コンフィギュレーション モードを終了すると、一部のコマンドが範囲内の全インターフェイスに実行されない場合があります。コマンド プロンプトが再表示されたのを確認してから、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 マクロの定義および使用

インターフェイス レンジ マクロを定義して、設定するインターフェイスの範囲を自動的に選択することができます。**interface range macro** コマンド ストリングで **macro** キーワードを使用するには、事前にマクロを定義しておく必要があります。

インターフェイス レンジ マクロを定義するには、次の作業を行います。

コマンド	目的
Router(config)# **define interface-range** *macro_name* {**vlan** *vlan_ID - vlan_ID*} | {*type*[1] *slot/port - port*} [, {*type*[1] *slot/port - port*}]	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。
Router(config)# **no define interface-range** *macro_name*	マクロを削除します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/1 ～ 5/4 を選択するように、インターフェイス レンジ マクロ enet_list を定義する例を示します。

```
Router(config)# define interface-range enet_list fastethernet 5/1 - 4
```

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するには、次の作業を行います。

コマンド	目的
Router# **show running-config**	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。

次に、定義済みのインターフェイス レンジ マクロ enet_list を表示する例を示します。

```
Router# show running-config | include define
define interface-range enet_list FastEthernet5/1 - 4
Router#
```

interface range コマンドでインターフェイス レンジ マクロを使用するには、次の作業を行います。

コマンド	目的
Router(config)# **interface range macro** *macro_name*	定義したインターフェイス レンジ マクロに保存された値を使用して、設定するインターフェイスの範囲を選択します。

次に、インターフェイス レンジ マクロ enet_list を使用して、インターフェイス レンジ コンフィギュレーション モードに切り替える例を示します。

```
Router(config)# interface range macro enet_list
Router(config-if)#
```

オプションのインターフェイス機能の設定

ここではオプションのインターフェイス機能について説明します。

イーサネット 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

ここでは、イーサネット ポート速度およびデュプレックス モードを設定する手順について説明します。

速度およびデュプレックス モード設定時の注意事項

通常、イーサネット ポート速度およびデュプレックス モード パラメータは auto に設定し、Catalyst 6500 シリーズ スイッチが、ポート間で速度およびデュプレックス モードをネゴシエーションできるようにします。ポート速度およびデュプレックス モードを手動で設定する場合には、次の点について考慮してください。

- イーサネット ポート速度を auto に設定すると、スイッチは自動的にデュプレックス モードを auto に設定します。
- **no speed** コマンドを入力すると、スイッチは自動的に、速度およびデュプレックスの両方を auto に設定します。
- イーサネット ポート速度を auto 以外の値（10 Mbps、100 Mbps、1000Mbps など）に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。
- イーサネット ポート速度を 10 Mbps または 100 Mbps のいずれかに手動で設定すると、スイッチがポートのデュプレックス モードを設定するように求めるプロンプトを表示します。

（注） Catalyst 6500 シリーズ スイッチは、接続先ポートが auto 以外の値に設定されている場合、イーサネット ポート速度およびデュプレックス モードを自動的にネゴシエーションできません。

注意 イーサネット ポート速度およびデュプレックス モードの設定を変更すると、インターフェイスがシャットダウンされてから再びイネーブルになる場合があります。

イーサネット インターフェイス速度の設定

（注）　10/100 Mbps または 10/100/1000 Mbps イーサネット ポート上でイーサネット ポート速度を **auto** に設定すると、速度およびデュプレックスが両方とも自動ネゴシエーションされます。

10/100 Mbps または 10/100/1000 Mbps イーサネット ポートのポート速度を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface fastethernet` *slot/port*	設定するイーサネット ポートを選択します。
ステップ 2	`Router(config-if)# speed {10 | 100 | 1000 | {auto [10 100 [1000]]}}`	イーサネット インターフェイス速度を設定します。
	`Router(config-if)# no speed`	デフォルト設定に戻します（speed auto）。

Release12.2(17a)SX 以降のリリースでは、**auto** キーワードのあとの **10 100 1000** キーワードをサポートします。Release12.2(17a)SX 以降のリリースで 10/100/1000 Mbps イーサネット ポートのポート速度を設定する場合は、次の点に注意してください。

- ネゴシエーション速度を 10 Mbps または 100 Mbps に制限するには、**auto 10 100** キーワードを入力します。
- **auto 10 100 1000** キーワードには、**auto** キーワードと同じ効果があります。

次に、ファスト イーサネット ポート 5/4 の速度を 100 Mbps に設定する例を示します。

```
Router(config)# interface fastethernet 5/4
Router(config-if)# speed 100
```

インターフェイスのデュプレックス モードの設定

（注）
- 10 ギガビット イーサネットおよびギガビット イーサネットは全二重通信専用です。ギガビット イーサネット用に設定された 10 ギガビット イーサネット ポート、ギガビット イーサネット ポート、または 10/100/1000 Mbps ポート上では、デュプレックス モードを変更できません。
- 10/100 Mbps または 10/100/1000 Mbps イーサネット ポート上でポート速度を auto に設定すると、速度およびデュプレックスが両方とも自動ネゴシエーションされます。自動ネゴシエーション ポートのデュプレックス モードは変更できません。

イーサネット ポートまたはファスト イーサネット ポートのデュプレックス モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface fastethernet` *slot/port*	設定するイーサネット ポートを選択します。
ステップ 2	`Router(config-if)# duplex [auto | full | half]`	イーサネット ポートのデュプレックス モードを設定します。
	`Router(config-if)# no duplex`	デフォルト設定に戻します（duplex auto）。

次に、ファスト イーサネット ポート 5/4 のデュプレックス モードを full に設定する例を示します。

```
Router(config)# interface fastethernet 5/4
Router(config-if)# duplex full
```

ギガビット イーサネット ポート上のリンク ネゴシエーションの設定

（注）　リンク ネゴシエーションでは、ポート速度のネゴシエーションは行われません。

ギガビット イーサネット ポートでは、リンク ネゴシエーションによってフロー制御パラメータ、リモート障害情報、およびデュプレックス情報が交換されます。リンク ネゴシエーションはデフォルトでイネーブルです。

リンクの両端のポートは同じ設定にする必要があります。リンクの両端で設定が矛盾している場合（一方のポートでリンク ネゴシエーションがイネーブルで、他方のポートではディセーブルの場合）、リンクはアクティブになりません。

表 9-1 に、設定可能な 4 種類のリンク ネゴシエーションと各設定ごとのリンク ステータスを示します。

表 9-1　　リンク ネゴシエーションの設定およびリンク ステータス

リンク ネゴシエーションのステート		リンク ステータス	
ローカル ポート	**リモート ポート**	**ローカル ポート**	**リモート ポート**
オフ	オフ	アップ	アップ
オン	オン	アップ	アップ
オフ	オン	アップ	ダウン
オン	オフ	ダウン	アップ

特定のポート上でリンク ネゴシエーションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface gigabitethernet` *slot/port*	設定するポートを選択します。
ステップ 2	`Router(config-if)# speed nonegotiate` `Router(config-if)# no speed nonegotiate`	リンク ネゴシエーションをディセーブルにします。 デフォルトの設定（リンク ネゴシエーションがイネーブル）に戻します。

次に、ギガビット イーサネット ポート 5/4 上でリンク ネゴシエーションをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 5/4
Router(config-if)# no speed nonegotiate
```

速度およびデュプレックス モードの設定の表示

ポート速度およびデュプレックス モードの設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show interfaces** *type*[1] *slot/port*	速度およびデュプレックス モードの設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/4 の速度およびデュプレックス モードを表示する例を示します。

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
  Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:33, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1238 packets input, 273598 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1380 packets output, 514382 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

ジャンボ フレームのサポートの設定

ここではジャンボ フレームのサポートについて説明します。

- 「ジャンボ フレームのサポートの概要」（P.9-11）
- 「MTU サイズの設定」（P.9-13）

注意　次のスイッチング モジュールは、8,092 バイトの最大入力フレーム サイズをサポートします。

- 100 Mbps で稼動している場合の WS-X6516-GE-TX
- WS-X6148-RJ-45、WS-X6148-RJ-45V および WS-X6148-RJ21、WS-X6148-RJ21V
- WS-X6248-RJ-45 および WS-X6248-TEL
- WS-X6248A-RJ-45 および WS-X6248A-TEL
- WS-X6348-RJ-45、WS-X6348-RJ45V および WS-X6348-RJ-21、WX-X6348-RJ21V

ジャンボ フレームのサポートが設定されていると、これらのモジュールは、8092 バイトより大きい入力フレームを廃棄します。

（注）　WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6148-GE-TX、WS-X6148V-GE-TX では、ジャンボ フレームをサポートしません。

ジャンボ フレームのサポートの概要

ここではジャンボ フレームのサポートについて説明します。

ジャンボ フレームのサポートの概要

ジャンボ フレームは、デフォルトのイーサネット サイズよりも大きなフレームです。ポートや VLAN インターフェイスにデフォルト値より大きい Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを設定し、グローバル LAN ポート MTU サイズを設定することにより、ジャンボ フレームのサポートをイネーブルにします。

（注）
- ジャンボ フレームのサポートは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上のソフトウェアのルーテッド トラフィックをフラグメント化します。
- ジャンボ フレームのサポートは、ブリッジド トラフィックをフラグメント化しません。

入力 10 Mbps、10/100 Mbps、100 Mbps イーサネットおよび 10 ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ジャンボ フレームのサポートは、デフォルト値以外の MTU サイズが設定された入力 10 Mbps、10/100 Mbps、100 Mbps イーサネットおよび 10 ギガビット イーサネット LAN ポートで、入力トラフィック サイズとグローバルな LAN ポート MTU サイズを比較します。ポートでは、サイズが大きいトラフィックが廃棄されます。グローバルな LAN ポートの MTU サイズを設定することができます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）を参照）。

入力ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ギガビット イーサネット LAN ポートにデフォルト値以外の MTU サイズを設定すると、パケット サイズが 64 バイトより大きい場合に、フレームを許可します。デフォルト値以外の MTU サイズが設定されている場合、ギガビット イーサネット LAN ポートはサイズが大きい入力フレームを調べません。

PFC でのルーテッド トラフィック サイズの確認

ルーティングする必要があるトラフィックに対して、Policy Feature Card（PFC; ポリシー フィーチャ カード）のジャンボ フレームのサポートは設定された MTU サイズとトラフィック サイズを比較し、そのトラフィックに対応できる MTU サイズが設定されたインターフェイス間のジャンボ トラフィックに、レイヤ 3 スイッチングが提供されます。MTU サイズが十分な大きさに設定されていないインターフェイス間では、[do not fragment bit] が設定されていない場合、PFC はトラフィックを MSFC に送信して、フラグメント化およびソフトウェアでのルーティングを行います。[do not fragment bit] が設定されていれば、PFC はトラフィックを廃棄します。

出力 10 Mbps、10/100 Mbps、100 Mbps イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

10 Mbps、10/100 Mbps、100 Mbps イーサネット LAN ポートにデフォルト値以外の MTU サイズを設定すると、パケット サイズが 64 バイトより大きいフレームが送信されます。デフォルト値以外の MTU サイズが設定されている場合、10 Mbps、10/100 Mbps、100 Mbps イーサネット LAN ポートはサイズが大きい出力フレームを調べません。

出力ギガビット イーサネットおよび 10 ギガビット イーサネット ポートでのブリッジドおよびルーテッド トラフィック サイズのチェック

ジャンボ フレームのサポートは、デフォルト値以外の MTU サイズが設定された出力ギガビット イーサネットおよび 10 ギガビット イーサネット LAN ポートで、出力トラフィック サイズとグローバルな出力 LAN ポートの MTU サイズを比較します。ポートでは、サイズが大きいトラフィックが廃棄されます。グローバルな LAN ポートの MTU サイズを設定することができます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）を参照）。

イーサネット ポート

ここでは、イーサネット ポートに対する、デフォルト値以外の MTU サイズの設定について説明します。

イーサネット ポートの概要

デフォルト値以外の MTU サイズを 10 Mbps、10/100 Mbps、または 100 Mbps イーサネット ポートに設定すると、出力パケットはグローバルな LAN ポートの MTU サイズに制限され、64 バイトより大きいサイズの出力トラフィックが許可されます。

ギガビット イーサネット ポートでデフォルト値以外の MTU サイズを設定すると、64 バイトより大きいすべてのサイズの入力パケットが許可され、出力トラフィックはグローバルな LAN ポートの MTU サイズに制限されます。

デフォルト値以外の MTU サイズを 10 ギガビット イーサネット ポートに設定すると、入出力パケットはグローバルな LAN ポートの MTU サイズに制限されます。

イーサネット ポートにデフォルト値以外の MTU サイズを設定すると、ルーテッド トラフィックは設定された MTU サイズに制限されます。

いずれのイーサネット ポートでも MTU サイズを設定できます。

レイヤ 3 イーサネット ポート

レイヤ 3 ポートでは、レイヤ 3 イーサネット ポートごとにグローバルな LAN ポート MTU サイズとは異なる MTU サイズを設定できます。

（注）　デフォルト値以外の MTU サイズが設定されているレイヤ 3 イーサネット LAN ポートを経由するトラフィックは、グローバルな LAN ポートの MTU サイズにも影響を受けます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）を参照）。

レイヤ 2 イーサネット ポート

レイヤ 2 ポートでは、グローバルな LAN ポート MTU サイズと一致する MTU サイズのみを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）を参照）

VLAN インターフェイス

レイヤ 3 VLAN インターフェイスごとに異なる MTU サイズを設定できます。VLAN インターフェイスにデフォルト値以外の MTU サイズを設定すると、トラフィックはデフォルト値以外の MTU サイズに制限されます。ジャンボ フレームをサポートするように VLAN インターフェイスに MTU サイズを設定できます。

MTU サイズの設定

ここでは、MTU サイズを設定する手順について説明します。

- 「MTU サイズの設定」（P.9-13）
- 「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）

MTU サイズの設定

MTU サイズを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {{type[1] slot/port} | {port-channel port_channel_number} slot/port}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mtu mtu_size` `Router(config-if)# no mtu`	MTU サイズを設定します。 デフォルトの MTU サイズ（1,500 バイト）に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show running-config interface [{gigabitethernet | tengigabitethernet} slot/port]`	実行コンフィギュレーションを表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、または **ge-wan**

MTU サイズを設定する際、次の情報に注意してください。

- VLAN インターフェイスとレイヤ 3 イーサネット ポートについては、サポートされている MTU 値は 64 ～ 9,216 バイトです。
- レイヤ 2 イーサネット ポートでは、グローバルな出力 LAN ポートの MTU サイズのみ設定することができます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.9-14）を参照）。

次に、ギガビット イーサネット ポート 1/2 上で MTU サイズを設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# mtu 9216
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show interface gigabitethernet 1/2
GigabitEthernet1/2 is administratively down, line protocol is down
  Hardware is C6k 1000Mb 802.3, address is 0030.9629.9f88 (bia 0030.9629.9f88)
  MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
<...Output Truncated...>
Router#
```

グローバルな出力 LAN ポート MTU サイズの設定

グローバルな出力 LAN ポート MTU サイズを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# system jumbomtu mtu_size`	グローバルな出力 LAN ポートの MTU サイズを設定します。
	`Router(config)# no system jumbomtu`	デフォルトのグローバルな出力 LAN ポートの MTU サイズ（9,216 バイト）に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

IEEE 802.3x フロー制御の設定

Catalyst 6500 シリーズ スイッチ上のギガビット イーサネット ポートおよび 10 ギガビット イーサネット ポートは、指定時間の間、ポートへのフレーム送信を停止するためにフロー制御を使用します。他のイーサネット ポートは、フロー制御要求に応答するためにフロー制御を使用します。

ギガビット イーサネット ポートまたは 10 ギガビット イーサネット ポートの受信バッファがいっぱいになると、指定時間の間、フレーム送信処理を遅らせるようにリモート ポートに要求する IEEE802.3x ポーズ フレームが送信されます。すべてのイーサネット ポート（10Gbps、1Gbps、100Mbps、および 10Mbps）は、他の装置から IEEE802.3x ポーズ フレームを受信し、これに応答することができます。

イーサネット ポート上でフロー制御を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# flowcontrol {receive | send} {desired | off | on}`	ポーズ フレームを送信またはポーズ フレームに応答するように、ポートを設定します。
	`Router(config-if)# no flowcontrol {receive | send}`	デフォルトのフロー制御設定に戻します。
ステップ 3	`Router# show interfaces [type[1] slot/port] flowcontrol`	すべてのポートのフロー制御設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

フロー制御を設定する際、次の情報に注意してください。

- WS-X6502-10GE 10 ギガビット イーサネット ポートのポーズフレームへの応答方法は設定できません。WS-X6502-10GE 10 ギガビット イーサネット ポートは、ポーズ フレームに応答するように永続的に設定されています。
- ポーズフレームへの応答方法を設定する場合、次の情報を参照してください。
  - ギガビット イーサネット ポートのリモート ポートの設定が不明な場合は、**receive desired** キーワードを使用して、受信したポーズ フレームに応答するようにギガビット イーサネット ポートを設定できます。（ギガビット イーサネット ポートでのみサポート）
  - **receive on** キーワードを使用すると、受信したポーズ フレームに応答するようにポートが設定されます。
  - **receive off** キーワードを使用すると、受信したポーズ フレームを無視するようにポートが設定されます。

- ポーズ フレームの送信をポートに設定する場合は、次の情報に注意してください。
  - ギガビット イーサネット リモート ポートの設定が不明な場合は、**send desired** キーワードを使用して、ポーズ フレームに送信するようにギガビット イーサネット ポートを設定できます。（ギガビット イーサネット ポートでのみサポート）
  - **send on** キーワードを使用すると、ポーズ フレームを送信するようにポートが設定されます。
  - **send off** キーワードを使用すると、ポーズ フレームを送信しないようにポートが設定されます。

次に、フロー制御の受信を有効にし、フロー制御設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# flowcontrol receive on
Router(config-if)# end
Router# show interfaces flowcontrol

Interface Send         Receive
Gi1/1     Desired      OFF
Gi1/2     Desired      ON
Fa5/1     Not capable  OFF
<output truncated>
```

ポート デバウンス タイマーの設定

ポート デバウンス タイマーはリンク変更の通知を遅らせ、ネットワークの再設定によるトラフィック損失を減らすことができます。通知を遅延させることにより、ポートがダウンした場合に通常必要となる STP トポロジの変更をトリガーすることなく、迅速にポート ステータスを変更およびリカバリできるようになります。ポート デバウンス タイマーは、各 LAN ポートに、個別に設定することができます。

注意　ポート デバウンス タイマーをイネーブルにすると、リンクダウンの検出が遅れることになり、デバウンス期間中のトラフィック損失につながります。この状況は、一部のレイヤ 2 とレイヤ 3 プロトコルのコンバージェンスと再コンバージェンスに影響する可能性があります。

ポート上でデバウンス タイマーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するポートを選択します。
ステップ 2	`Router(config-if)# link debounce [time` *debounce_time*`]`	デバウンス タイマーを設定します。
	`Router(config-if)# no link debounce`	デフォルト設定に戻します。
ステップ 3	`Router# show interfaces debounce`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ポートのデバウンス タイマーを設定する際、次の情報に注意してください。

- **time** キーワードは、光ファイバ ギガビット イーサネット ポートでのみサポートされています。
- 銅製メディアを通じて 1000 Mbps で動作しているポートで、ポート デバウンス タイマー値を 100 ミリ秒単位で 5,000 ミリ秒まで増やすことができます。
- Release 12.2(17a)SX より以前のリリースでは、WS-X6502-10GE のみをサポートします。

- Release12.2(18)SXD より以前のリリースでは、10 Gbps ポートは光ファイバ メディアを使用していることを前提にしています。
- Release12.2(18)SXD 以降のリリースでは、10 Gbps 銅製メディアを認識します。
- Release12.2(18)SXD よりも前のリリースでは、メディアのみの変更を検知しません。
- Release12.2(18)SXD 以降のリリースでは、メディアのみの変更を検知します。

表 9-2 は、リンク変更の通知前に発生する時間遅延を一覧表示します。

表 9-2　デフォルト ポート デバウンス タイマー遅延時間

ポート タイプ	デバウンス タイマーがディセーブルの場合	デバウンス タイマーがイネーブルの場合
10 Mbps または 100 Mbps で動作するポート	300 ミリ秒	3,100 ミリ秒
銅製メディアを通じて 1000 Mbps または 10 Gbps で動作するポート	300 ミリ秒	3,100 ミリ秒
光ファイバ メディアを通じて 1000 Mbps または 10 Gbps で動作するポート	10 ミリ秒[1]	100 ミリ秒
WS-X6502-10GE 10 Gbps ポート	1,000 ミリ秒	3,100 ミリ秒

1. Release 12.2(18)SXF13 以降のリリースでは 10 ミリ秒。

（注） どの 10 ギガビット イーサネット ポートでも、デバウンス タイマー ディセーブルは 10 ミリ秒、デバウンス タイマー イネーブルは 1 秒です。

次に、ファスト イーサネット ポート 5/12 のポート デバウンス タイマーをイネーブルにする例を示します。

```
Router(config)# interface fastethernet 5/12
Router(config-if)# link debounce
Router(config-if)# end
```

次に、ポート デバウンス タイマーの設定を表示する例を示します。

```
Router# show interfaces debounce | include enable
Fa5/12  enable          3100
```

インターフェイスに関する説明の追加

インターフェイスの機能をわかりやすくするため、インターフェイスに関する説明を追加することができます。説明は、**show configuration**、**show running-config**、および **show interfaces** コマンドの出力に表示されます。

インターフェイスに説明を追加するには、次の作業を行います。

コマンド	目的
`Router(config-if)# description` *string*	インターフェイスに説明を追加します。
`Router(config-if)# no description`	インターフェイスから説明を削除します。

次に、ファスト イーサネット ポート 5/5 に関する説明を追加する例を示します。

```
Router(config)# interface fastethernet 5/5
Router(config-if)# description Channel-group to "Marketing"
```

OIR の概要

Catalyst 6500 シリーズ スイッチでは Online Insertion and Removal（OIR; ホットスワップ）機能がサポートされており、システムをオンラインにしたままモジュールの取り外しおよび交換を行うことができます。モジュールを取り外す前にシャットダウンし、取り付けたあとで再起動しても、他のソフトウェアまたはインターフェイスはシャットダウンされません。

（注） 取り外しおよび取り付けを行うモジュールは、一度に 1 つだけにしてください。モジュールの取り外しおよび取り付け後に、LED を確認してから次の作業を始めます。モジュールの LED については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

モジュールの取り外しおよび取り付けを行うと、Catalyst 6500 シリーズ スイッチはモジュールのトラフィック処理を停止し、設定の変更がないかどうかシステムを走査します。各インターフェイス タイプがシステム コンフィギュレーションと照らし合わせてチェックされます。そのあと、システムは新しいモジュールに関して診断を実行します。モジュールの取り付けおよび取り外し中に、通常の動作が中断されることはありません。

スイッチがオンラインにできるのは、設定が同一の交換モジュールだけです。同一モジュールでの OIR をサポートするために、モジュールを取り外すときにモジュール設定が running-config ファイルから削除されません。

交換モジュールと取り外したモジュールが異なる場合は、交換モジュールを設定してからでないと、スイッチはこのモジュールをオンラインにしません。

レイヤ 2 MAC（メディア アクセス制御）アドレスは Electrically Erasable Programmable Read-Only Memory（EEPROM; 電気的消去再書き込み可能 ROM）上に保存され、システムがスイッチング テーブルおよびデータ構造を更新しなくても、モジュールをオンラインで交換できます。レイヤ 2 MAC アドレスは、インストールされているモジュールのタイプとは関係なく、スーパーバイザ エンジンを交換しない限り変更されません。スーパーバイザ エンジンを交換すると、*すべての* ポートのレイヤ 2 MAC アドレスが、新しいスーパーバイザ エンジン上のアドレス アロケータで指定されるアドレスに変更されます。

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、インターフェイスをモニタおよびメンテナンスするために行う作業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

インターフェイスに関する情報（ソフトウェア/ハードウェアのバージョン、インターフェイス統計情報など）を表示するためのコマンドが準備されています。これらのコマンドは、EXEC プロンプトで入力します。次の表に、インターフェイスをモニタするためのコマンドをいくつか紹介します（**show** コマンドの全リストを表示するには、EXEC プロンプトで **show ?** コマンドを入力します）。これらのコマンドについての詳細は、『*Cisco IOS Interface Command Reference*』を参照してください。

インターフェイスに関する情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ibc**	現在の内部ステータス情報を表示します。
Router# **show eobc**	現在の内部帯域外情報を表示します。
Router# **show interfaces** [*type slot/port*]	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、ステータスおよび設定を表示します。
Router# **show running-config**	現在の実行コンフィギュレーションを表示します。
Router# **show rif**	現在の Routing Information Field（RIF）キャッシュの内容を表示します。
Router# **show protocols** [*type slot/port*]	設定されている任意のプロトコルについて、グローバル（システム全体）およびインターフェイス固有のステータスを表示します。
Router# **show version**	ハードウェア設定、ソフトウェア バージョン、コンフィギュレーション ファイルの名前と送信元、およびブート イメージを表示します。

次に、ファスト イーサネット ポート 5/5 のステータスを表示する例を示します。

```
Router# show protocols fastethernet 5/5
FastEthernet5/5 is up, line protocol is up
Router#
```

インターフェイスのカウンタのクリア

show interfaces コマンドで表示されるインターフェイス カウンタをクリアするには、次の作業を行います。

コマンド	目的
Router# **clear counters** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *channel_ID*}}	インターフェイス カウンタをクリアします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/5 のカウンタをクリアしてリセットする例を示します。

```
Router# clear counters fastethernet 5/5
Clear "show interface" counters on this interface [confirm] y
Router#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface FastEthernet5/5
```

clear counters コマンドを実行すると、オプションの引数を使用して特定のインターフェイスを指定しない限り、現在のすべてのインターフェイス カウンタがクリアされます。

（注）　**clear counters** コマンドでは、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して取得したカウンタはクリアされず、**show interfaces** EXEC コマンドで表示されるカウンタだけがクリアされます。

インターフェイスのリセット

インターフェイスをリセットするには、次の作業を行います。

コマンド	目的
Router# **clear interface** *type*[1] *slot/port*	インターフェイスをリセットします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/5 をリセットする例を示します。

```
Router# clear interface fastethernet 5/5
Router#
```

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、指定したインターフェイス上の全機能がディセーブルになり、そのインターフェイスはすべてのモニタ コマンド出力で使用不能として表示されます。この情報は、あらゆるダイナミック 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。そのインターフェイスは、あらゆるルーティング アップデートに含まれなくなります。

インターフェイスをシャットダウンしたあとで再起動するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *channel_ID*}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **shutdown**	インターフェイスをシャットダウンします。
ステップ 3	Router(config-if)# **no shutdown**	インターフェイスを再びイネーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/5 をシャットダウンする例を示します。

```
Router(config)# interface fastethernet 5/5
Router(config-if)# shutdown
Router(config-if)#
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface FastEthernet5/5, changed state to
administratively down
```

次に、ファスト イーサネット ポート 5/5 を再びイネーブルにする例を示します。

```
Router(config-if)# no shutdown
Router(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
```

インターフェイスがディセーブルになったかどうかを確認するには、**show interfaces** EXEC コマンドを使用します。シャットダウンされたインターフェイスは、**show interfaces** コマンドの出力では [administratively down] と表示されます。

TDR を使用したケーブル ステータスの確認

Time Domain Reflectometer（TDR; タイム ドメイン反射率計）を使用して銅線ケーブルのステータスを確認できます。TDR は、まず信号ケーブルに送信し、反射して戻ってきた信号を読み取ることでケーブルの不良を検出します。信号の全部または一部が、ケーブルの不良箇所またはケーブルの終端から反射して戻ってきます。

リンクを確立できない場合に、TDR を使用してケーブルが不良かどうかを判断します。これは、既存スイッチの交換、ギガビット イーサネットへのアップグレード、または新しいケーブルを導入する際に特に重要になります。

TDR テストの開始前にインターフェイスを起動しておく必要があります。ポートがダウンしている場合、**test cable-diagnostics tdr** コマンドを正常に入力できず、次のようなメッセージが表示されます。

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

（注）

- TDR は、最大 115 メートルまでのケーブルをテストできます。
- TDR をサポートするモジュールの詳細については、『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

TDR テストを開始または停止するには、次の作業を行います。

コマンド	目的
test cable-diagnostics tdr interface {*interface interface-number*}	TDR テストを開始または停止します。

次に、TDR ケーブル診断を実行する例を示します。

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
Router #
```

CHAPTER 10

レイヤ 2 スイッチング用 LAN ポートの設定

この章では、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、Catalyst 6500 シリーズ スイッチ上でレイヤ 2 スイッチング用のイーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット LAN ポートを設定する手順について説明します。この章の設定作業は、LAN スイッチング モジュール上の LAN ポート、およびスーパーバイザ エンジン上の LAN ポートに適用されます。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- レイヤ 3 インターフェイスの設定手順については、第 22 章「レイヤ 3 インターフェイスの設定」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。

レイヤ 2 スイッチングの機能概要

ここでは、Catalyst 6500 シリーズ スイッチにおけるレイヤ 2 スイッチングの機能について説明します。

レイヤ 2 イーサネット スイッチングの概要

ここではレイヤ 2 イーサネット スイッチングについて説明します。

レイヤ 2 イーサネット スイッチングの概要

Catalyst 6500 シリーズ スイッチは、レイヤ 2 イーサネット セグメント間の同時パラレル接続をサポートしています。イーサネット セグメント間のスイッチド コネクションが維持されるのは、パケットの伝送時間の長さだけです。次のパケットには、別のセグメント間に新しい接続が確立されます。

Catalyst 6500 シリーズ スイッチは、広帯域の装置および大量のユーザに起因する輻輳問題を解決するために、装置（サーバなど）ごとに専用の 10 Mbps、100 Mbps、または 1000 Mbps 衝突ドメインを割り当てます。各 LAN ポートは、それぞれ別のイーサネット衝突ドメインに接続されているので、スイッチング環境が適切に設定されていれば、サーバは全帯域幅にアクセスできます。

衝突はイーサネット ネットワークにおける重大な障害になっていますが、有効な解決策の 1 つは全二重通信です。通常、イーサネットは半二重モードで動作します。つまり、各ステーションは送信または受信のどちらか一方しか実行できません。全二重モードでは、2 つのステーション間で同時に送受信を行うことができます。パケットは両方向で同時に流れることができる場合、有効なイーサネット帯域幅が 2 倍になります。

セグメント間のフレーム スイッチング

Catalyst 6500 シリーズ スイッチ上の各 LAN ポートは、1 台のワークステーションまたはサーバに接続することも、ハブを介して複数のワークステーションまたはサーバをネットワークに接続することもできます。

標準的なイーサネット ハブでは、すべてのポートがハブ内の共通のバックプレーンに接続され、ハブに接続されたすべての装置が、ネットワークの帯域幅を共用します。2 つのステーション間で、相当量の帯域幅を使用するセッションを確立した場合には、そのハブに接続された他のすべてのステーションで、ネットワークのパフォーマンスが低下します。

このようなパフォーマンス低下を軽減するために、スイッチは各 LAN ポートをそれぞれ独立したセグメントとして扱います。異なる LAN ポートに接続されているステーションが相互に通信する必要がある場合、スイッチは、一方の LAN ポートから他方の LAN ポートにワイヤ速度でフレームを転送して、各セッションが全帯域幅を利用できるようにします。

LAN ポート間のフレーム スイッチングを効率的に行うために、スイッチはアドレス テーブルを維持します。フレームがスイッチに着信すると、スイッチは送信元ネットワーク装置の MAC アドレスと、フレームを受信した LAN ポートを関連付けます。

アドレス テーブルの作成

Catalyst 6500 シリーズ スイッチは、受信したフレームの送信元アドレスを使用して、アドレス テーブルを作成します。アドレス テーブルに宛先アドレスが登録されていないフレームをスイッチが受信すると、そのフレームを受信したポート以外の、同一 VLAN のすべての LAN ポートに、フレームをフラッディングします。宛先ステーションから応答があると、スイッチは関連する送信元アドレスおよびポート ID をアドレス テーブルに追加します。スイッチは以後、LAN ポートすべてに後続フレームをフラッディングせずに、1 つの LAN ポートだけに転送します。

アドレス テーブルには、エントリのフラッディングを伴わずに 32,000 以上のアドレス エントリを保管できます。スイッチは設定変更可能なエージング タイマーによって定められたエージング メカニズムを使用するので、アドレスが所定の秒数だけ非アクティブ状態になると、アドレス テーブルから削除されます。

VLAN トランクの概要

ここでは、Catalyst 6500 シリーズ スイッチ上での VLAN トランクについて説明します。

- 「トランキングの概要」（P.10-3）
- 「カプセル化タイプ」（P.10-4）

トランキングの概要

（注）　VLAN の詳細については、第 14 章「仮想 LAN（VLAN）の設定」を参照してください。

トランクとはスイッチとその他のネットワーキング装置間のポイントツーポイント リンクです。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

次の 2 種類のトランキング カプセル化方式が、すべてのイーサネット ポートで使用可能です。

- Inter-Switch Link（ISL; スイッチ間リンク）- ISL はシスコ独自のトランキング カプセル化方式です。

  （注）　次のスイッチング モジュールは ISL カプセル化をサポートしていません。

  - WS-X6502-10GE
  - WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6548-GE-45AF
  - WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6148-GE-45AF

- 802.1Q - 802.1Q は、業界標準のトランキング カプセル化方式です。

1 つのイーサネット ポートまたは EtherChannel に対してトランクを設定できます。EtherChannel の詳細については、第 12 章「EtherChannel の設定」を参照してください。

イーサネット トランク ポートは、数種類のトランキング モードをサポートしています（表 10-2（P.10-5）を参照）。さらに、トランクでの ISL または 802.1Q カプセル化の使用、またはカプセル化タイプの自動ネゴシエーションを指定することもできます。

（注）　カプセル化タイプをネゴシエーションするように LAN ポートを設定できます。カプセル化タイプをネゴシエーションするように WAN インターフェイスを設定することはできません。

Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）は LAN ポート上のトランク自動ネゴシエーションを管理します。DTP は、1 つの VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）ドメイン内で ISL トランクと 802.1Q トランク両方の自動ネゴシエーションをサポートします。

トランキングを自動ネゴシエーションするには、LAN ポートが同じ VTP ドメインに存在する必要があります。異なるドメイン内の LAN ポートを強制的にトランクするには、**trunk** キーワードまたは **nonegotiate** キーワードを使用します。VTP ドメインの詳細については、第 13 章「VLAN トランキング プロトコル（VTP）の設定」を参照してください。

カプセル化タイプ

表 10-1 に、イーサネット トランクのカプセル化タイプを示します。

表 10-1　イーサネット トランクのカプセル化タイプ

カプセル化	機能
switchport trunk encapsulation isl	トランク リンクに ISL カプセル化を指定します。 （注）　ISL カプセル化をサポートしていないモジュールもあります（「トランキングの概要」（P.10-3）を参照）。
switchport trunk encapsulation dot1q	トランク リンクに 802.1Q カプセル化を指定します。
switchport trunk encapsulation negotiate	LAN ポートが近接 LAN ポートとネゴシエーションを行い、近接 LAN ポートの設定および機能に応じて、ISL トランク（優先）または 802.1Q トランクになるように指定します。

リンクが ISL トランクまたは 802.1Q トランクのどちらになるかは、接続された 2 つの LAN ポートのトランキング モード、トランク カプセル化タイプ、およびハードウェア機能によって決まります。

レイヤ 2 LAN ポート モード

表 10-2 に、レイヤ 2 LAN ポート モードを示し、LAN ポートにおける各モードの機能について説明します。

表 10-2　レイヤ 2 LAN ポート モード

モード	機能
switchport mode access	LAN ポートは永続的な非トランキング モードになり、リンクを非トランク リンクに変換するようにネゴシエーションを行います。近接 LAN ポートが変更に同意しなくても、LAN ポートは非トランク ポートになります。
switchport mode dynamic desirable	リンクからトランク リンクへの変換を LAN ポートにアクティブに試行させます。近接 LAN ポートが **trunk**、**desirable**、または **auto** モードに設定されていれば、LAN ポートはトランク ポートになります。このモードは、すべての LAN ポートのデフォルト モードです。
switchport mode dynamic auto	LAN ポートにリンクからトランク リンクへの変換を試行させます。近接 LAN ポートが **trunk** または **desirable** モードに設定されていれば、LAN ポートはトランク ポートになります。
switchport mode trunk	LAN ポートは永続的なトランキング モードになり、リンクをトランク リンクに変換するようにネゴシエーションを行います。近接ポートが変更に同意しなくても、LAN ポートはトランク ポートになります。
switchport nonegotiate	LAN ポートを永続的なトランキング モードにしますが、LAN ポートが DTP フレームを生成するのを防ぎます。トランク リンクを確立するには、近接ポートを手動でトランク ポートとして設定する必要があります。

（注） DTP は PPP（ポイントツーポイント プロトコル）です。ただし、インターネットワーキング装置によっては、DTP フレームが正しく転送されないことがあります。この問題を避けるために、これらのリンク上でトランキングを行わない場合は、DTP をサポートしない装置に接続されている LAN ポートが、**access** キーワードを使用して設定されていることを確認してください。DTP をサポートしない装置へのトランキングをイネーブルにするには、**nonegotiate** キーワードを使用して、LAN ポートをトランクにし、DTP フレームが生成されないようにします。

レイヤ 2 LAN インターフェイスのデフォルト設定

表 10-3 に、レイヤ 2 LAN ポートのデフォルト設定を示します。

表 10-3　レイヤ 2 LAN インターフェイスのデフォルト設定

機能	デフォルト
インターフェイス モード： • **switchport** コマンドの入力前 • **switchport** コマンドの入力後	 レイヤ 3（未設定） **switchport mode dynamic desirable**
トランク カプセル化	**switchport trunk encapsulation negotiate**
VLAN 許容範囲	VLAN 1 ～ 4094（予約済み VLAN を除く）（表 14-1（P.14-2）を参照）
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルト アクセス VLAN	VLAN 1
ネイティブ VLAN（802.1Q トランク用）	VLAN 1
Spanning Tree Protocol（STP; スパンニング ツリー プロトコル）	すべての VLAN でイネーブル
STP ポート プライオリティ	128
STP ポート コスト	• 10 Mbps イーサネット LAN ポートでは 100 • 10/100 Mbps ファスト イーサネット LAN ポートでは 19 • 100 Mbps ファスト イーサネット LAN ポートでは 19 • 1,000 Mbps ギガビット イーサネット LAN ポートでは 4 • 10,000 Mbps 10 ギガビット イーサネット LAN ポートでは 2

レイヤ 2 LAN インターフェイス設定時の注意事項および制約事項

レイヤ 2 LAN ポートを設定する際に、以下の注意事項と制約事項に従ってください。

- 次のスイッチング モジュールは、ISL カプセル化をサポートしません。
  - WS-X6502-10GE
  - WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6548-GE-45AF
  - WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6148-GE-45AF
- 次に示す設定時の注意事項および制約事項は、802.1Q トランクを使用するときに適用され、ネットワークのトランキングの構築方法が多少制限されます。802.1Q トランクを使用するときは、これらの制約事項に注意してください。
  - 802.1Q トランクを介してシスコ製スイッチを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と他端のネイティブ VLAN が異なると、スパニング ツリー ループの原因になります。
  - 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、802.1Q トランクの 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。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ことを推奨します。この設定ができない場合は、ネットワークのすべての VLAN 上でスパニング ツリーをディセーブルにしてください。スパニング ツリーをディセーブルにする場合には、事前にネットワークに物理的なループが存在しないことを確認してください。
  - 802.1Q トランクを介して 2 台のシスコ製スイッチを接続すると、トランク上で許容される VLAN ごとにスパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態で、予約済み IEEE 802.1d スパニング ツリー マルチキャスト MAC（メディア アクセス制御）アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
  - 他社製の 802.1Q スイッチでは、すべての VLAN に対してスパニング ツリー トポロジを定義する単一のインスタンスしか維持されません。802.1Q トランクを介してシスコ製スイッチを他社製のスイッチに接続すると、他社製のスイッチの MST とシスコのスイッチのネイティブ VLAN スパニング ツリーが組み合わされて、Common Spanning Tree（CST）と呼ばれる単一のスパニング ツリー トポロジが形成されます。
  - シスコ製スイッチは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を送信します。したがって、他社製のスイッチではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッディングされます。他社製の 802.1Q クラウドに接続された他のシスコのスイッチは、フラッディングされたこれらの BPDU を受信します。このようにして、シスコのスイッチは、他社製の 802.1Q スイッチ クラウドにわたって、VLAN 別のスパニング ツリー トポロジを維持できます。シスコのスイッチを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのスイッチ間の単一のブロードキャスト セグメントとして処理されます。
  - シスコのスイッチを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。

– 他社製の特定の 802.1Q クラウドに複数のシスコのスイッチを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。ISL トランクまたはアクセス ポートを介して、シスコのスイッチを他社製の 802.1Q クラウドに接続することはできません。このように接続すると、スイッチで ISL トランク ポートまたアクセス ポートはスパニング ツリーのポート ステートが「一貫しない」状態になり、ポートを介してトラフィックが送信されなくなります。

レイヤ 2 スイッチング用の LAN インターフェイスの設定

ここでは、Catalyst 6500 シリーズ スイッチにおけるレイヤ 2 スイッチングの設定手順について説明します。

（注）　インターフェイスをデフォルト設定に戻すには、**default interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* コマンドを使用します。

レイヤ 2 スイッチング用の LAN ポートの設定

レイヤ 2 スイッチング用の LAN ポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# shutdown`	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。
ステップ 3	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 （注）　LAN ポートをレイヤ 2 ポートとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。
	`Router(config-if)# no switchport`	レイヤ 2 LAN ポートの設定を消去します。
ステップ 4	`Router(config-if)# no shutdown`	インターフェイスをアクティブにします（インターフェイスをシャットダウンしている場合に限り必要）。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show running-config interface` [*type*[1] *slot/port*]	インターフェイスの実行コンフィギュレーションを表示します。
ステップ 7	`Router# show interfaces` [*type*[1] *slot/port*] **switchport**	インターフェイスのスイッチ ポートの設定を表示します。
ステップ 8	`Router# show interfaces` [*type*[1] *slot/port*] **trunk**	インターフェイスのトランクの設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

switchport コマンドを入力したあとのデフォルト モードは、**switchport mode dynamic desirable** です。近接ポートがトランキングをサポートし、かつトランキングを許可するように設定されている場合、**switchport** コマンドを入力すると、リンクはレイヤ 2 トランクになります。LAN トランク ポートは、デフォルトでカプセル化についてネゴシエーションします。近接ポートが ISL および 802.1Q カプセル化をサポートし、かつ両方のポートがカプセル化タイプについてネゴシエーションするように設定されていれば、トランクは ISL カプセル化を使用します（10 ギガビット イーサネット ポートは ISL カプセル化をサポートしません）。

（注）　**switchport** コマンドを使用して、レイヤ 3 用に設定されていたポートをレイヤ 2 用に設定すると、レイヤ 3 用の設定は実行コンフィギュレーション内からはなくなりますが、メモリ内には保持され、ポートがレイヤ 3 に戻されたときにはいつでもメモリ内の設定が適用されます。レイヤ 2 用に設定されていたポートをレイヤ 3 用に設定した場合も、レイヤ 2 用の設定は実行コンフィギュレーション内からはなくなりますが、メモリ内には保持され、ポートがレイヤ 2 に戻されたときにはいつでもメモリ内の設定が適用されます。メモリ内および実行コンフィギュレーション内の設定をポートのデフォルト設定に戻すには、**default interface** コマンドを使用します。**switchport** コマンドを使用してポートのロールを変更している間に問題が発生するのを回避するために、**switchport** コマンドを適用する場合は、その前にインターフェイスをシャットダウンしてください。

トランクとしてのレイヤ 2 スイッチング ポートの設定

ここでは、レイヤ 2 スイッチング ポートをトランクとして設定する手順について説明します。

ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定

（注）
- ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。
- キーワードを指定せずに **switchport** コマンドを入力した場合（前のセクションの ステップ 3）、デフォルト モードは **switchport mode dynamic desirable** と **switchport trunk encapsulation negotiate** です。

レイヤ 2 スイッチング ポートを ISL または 802.1Q トランクとして設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}`	（任意）カプセル化を設定して、レイヤ 2 スイッチング ポートを ISL または 802.1Q トランクとして設定します。
`Router(config-if)# no switchport trunk encapsulation`	デフォルトのトランク カプセル化モード（**negotiate**）に戻します。

レイヤ 2 スイッチング ポートを ISL または 802.1Q トランクとして設定する際、次の作業情報に注意してください。

- **switchport mode trunk** コマンド（「DTP を使用しないようにするためのレイヤ 2 トランクの設定」（P.10-11）を参照）は、**switchport trunk encapsulation negotiate** コマンドとは互換性がありません。
- **switchport mode trunk** コマンドを使用できるようにするには、ISL または 802.1Q としてカプセル化を設定する必要があります。
- 次のスイッチング モジュールは、ISL カプセル化をサポートしません。
  - WS-X6502-10GE
  - WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6548-GE-45AF
  - WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6148-GE-45AF

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

DTP を使用するためのレイヤ 2 トランクの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

DTP を使用するようにレイヤ 2 トランクを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport mode dynamic {auto | desirable}`	（任意）DTP を使用するようにトランクを設定します。
`Router(config-if)# no switchport mode`	デフォルトのトランク トランキング モード（**switchport mode dynamic desirable**）に戻します。

DTP を使用するようにレイヤ 2 トランクを設定する際、次の情報に注意してください。

- インターフェイスがレイヤ 2 アクセス ポートの場合、またはトランキング モードを指定する場合に限り必須です。
- トランキング モードの詳細については、表 10-2（P.10-5）を参照してください。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

DTP を使用しないようにするためのレイヤ 2 トランクの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

DTP を使用しないようにレイヤ 2 トランクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# switchport mode trunk`	（任意）無条件にポートをトランクに設定します。
	`Router(config-if)# no switchport mode`	デフォルトのトランク トランキング モード（**switchport mode dynamic desirable**）に戻します。
ステップ 2	`Router(config-if)# switchport nonegotiate`	（任意）DTP を使用しないようにトランクを設定します。
	`Router(config-if)# no switchport nonegotiate`	ポート上で DTP をイネーブルにします。

DTP を使用しないようにレイヤ 2 トランクを設定する際、次の情報に注意してください。

- **switchport mode trunk** コマンドを入力する前に、カプセル化を設定する必要があります（「ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-10）を参照）。
- **switchport nonegotiate** コマンドを使用できるようにするには、**switchport mode trunk** コマンドを入力する必要があります。
- **switchport mode dynamic trunk** コマンドを入力します。トランキング モードの詳細については、表 10-2（P.10-5）を参照してください。

- **switchport nonegotiate** コマンドを入力する前にカプセル化を設定し（「ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-10）を参照）、**switchport mode trunk** コマンドを使用して無条件にポートをトランクに設定する必要があります（「DTP を使用するためのレイヤ 2 トランクの設定」（P.10-11）を参照）。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

アクセス VLAN の設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

アクセス VLAN を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# 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アクセス VLAN を設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
`Router(config-if)# no switchport access vlan`	デフォルト値に戻します（VLAN 1）。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

802.1Q ネイティブ VLAN の設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

802.1Q ネイティブ VLAN を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk native vlan vlan_ID`	（任意）802.1Q ネイティブ VLAN を設定します。
`Router(config-if)# no switchport trunk native vlan`	デフォルト値に戻します（VLAN 1）。

ネイティブ VLAN を設定する際、次の情報に注意してください。

- *vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
- アクセス VLAN がネイティブ VLAN として自動的に使用されることはありません。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

トランク上で許容される VLAN のリストの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

トランク上で許容される VLAN のリストを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]]`	（任意）トランク上で許容される VLAN のリストを設定します。
`Router(config-if)# no switchport trunk allowed vlan`	デフォルト値に戻します（すべての VLAN を許容）。

トランク上で許容される VLAN のリストを設定する際、次の情報に注意してください。

- *vlan* パラメータは、1 ～ 4094 の範囲の単一の VLAN 番号、または 2 つの VLAN 番号（小さい番号が先、ダッシュで区切る）で指定する VLAN 範囲です。カンマで区切った *vlan* パラメータの間、またはダッシュ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。
- VLAN 1 を削除できます。トランクから VLAN 1 を削除した場合も、トランク インターフェイスは VLAN 1 の Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）、VTP、Port Aggregation Protocol（PAgP）、DTP などの管理トラフィックを引き続き送受信します。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

プルーニング適格 VLAN のリストの設定

（注）　ここに記載された作業を実行する前に、「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-8）の手順を実行します。

レイヤ 2 トランクでプルーニング適格 VLAN のリストを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport trunk pruning vlan {none |{{add | except | remove} vlan[,vlan[,vlan[,...]]]}}`	（任意）トランクでプルーニング適格 VLAN のリストを設定します（「VTP プルーニングの概要」（P.13-4）を参照）。
`Router(config-if)# no switchport trunk pruning vlan`	デフォルト値に戻します（すべての VLAN がプルーニング適格）。

トランク上で許容されるプルーニング適格 VLAN のリストを設定する際、次の情報に注意してください。

- *vlan* パラメータは、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く。表 14-1（P.14-2）を参照）、または 2 つの VLAN 番号（小さい番号が先、ダッシュで区切る）で指定する VLAN 範囲です。カンマで区切った *vlan* パラメータの間、またはダッシュ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、プルーニングが許容される VLAN のリストには、すべての VLAN が含まれます。
- VTP 透過モードのネットワーク装置は、VTP Join メッセージを送信しません。VTP 透過モードのネットワーク装置にトランク接続されている Catalyst 6500 シリーズ スイッチでは、透過モード ネットワーク装置によって使用される VLAN、またはプルーニング不適格として透過モード ネットワーク装置全体に伝送する必要がある VLAN を設定します。

（注）　ここに記載された作業を実行したあとで、「トランクの設定の完了」（P.10-14）の手順を実行します。

トランクの設定の完了

レイヤ 2 トランクの設定を完了するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# no shutdown`	インターフェイスをアクティブにします（インターフェイスをシャットダウンしている場合に限り必要）。
ステップ 2	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

レイヤ 2 トランクの設定の確認

レイヤ 2 トランクの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show running-config interface` *type*[1] *slot/port*	インターフェイスの実行コンフィギュレーションを表示します。
ステップ 2	`Router# show interfaces` [*type*[1] *slot/port*] `switchport`	インターフェイスのスイッチ ポートの設定を表示します。
ステップ 3	`Router# show interfaces` [*type*[1] *slot/port*] `trunk`	インターフェイスのトランクの設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

設定および確認の例

次に、ファスト イーサネット ポート 5/8 を 802.1Q トランクとして設定する例を示します。この例では、近接ポートが 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。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/8
Router(config-if)# shutdown
Router(config-if)# switchport
Router(config-if)# switchport mode dynamic desirable
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

次に、設定を確認する例を示します。

```
Router# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 no ip address
 switchport
 switchport trunk encapsulation dot1q
end

Router# show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL

Router# show interfaces fastethernet 5/8 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa5/8     desirable    n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa5/8 1-1005

Port      Vlans allowed and active in management domain
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Router#
```

レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定

（注） 存在しない VLAN に LAN ポートを割り当てると、VLAN データベースにその VLAN を作成するまで、LAN ポートはシャットダウンされます（「イーサネット VLAN の作成または変更」（P.14-11）を参照）。

LAN ポートをレイヤ 2 アクセス ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# shutdown`	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。
ステップ 3	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 **（注）** LAN ポートをレイヤ 2 ポートとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。
ステップ 4	`Router(config-if)# no switchport`	レイヤ 2 LAN ポートの設定を消去します。
ステップ 5	`Router(config-if)# switchport mode access`	LAN ポートをレイヤ 2 アクセス ポートとして設定します。
	`Router(config-if)# no switchport mode`	デフォルトのスイッチポート モード（**switchport mode dynamic desirable**）に戻します。
ステップ 6	`Router(config-if)# switchport access vlan` *vlan_ID*	LAN ポートを VLAN に入れます。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config-if)# no switchport access vlan`	デフォルトのアクセス VLAN に戻します（VLAN 1）。
ステップ 7	`Router(config-if)# no shutdown`	インターフェイスをアクティブにします （インターフェイスをシャットダウンしている場合に限り必要）。
ステップ 8	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 9	`Router# show running-config interface` [*type*[1] *slot/port*]	インターフェイスの実行コンフィギュレーションを表示します。
ステップ 10	`Router# show interfaces` [*type*[1] *slot/port*] **switchport**	インターフェイスのスイッチ ポートの設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/6 を VLAN 200 のアクセス ポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/6
Router(config-if)# shutdown
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 200
Router(config-if)# no shutdown
Router(config-if)# end
Router# exit
```

次に、設定を確認する例を示します。

```
Router# show running-config interface fastethernet 5/6
Building configuration...
!
Current configuration:
interface FastEthernet5/6
 no ip address
 switchport access vlan 200
 switchport mode access
end

Router# show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Enabled
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL

Router#
```

カスタム IEEE 802.1Q EtherType フィールド値の設定

Release 12.2(17a)SX 以降のリリースでは、802.1Q タグ付きまたは 802.1p タグ付きフレームの標準 0x8100 EtherType フィールド値を使用しないネットワーク装置をサポートするように、ポートでカスタム EtherType フィールド値を設定できます。

EtherType フィールドのカスタム値を設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# switchport dot1q ethertype` *value*	ポートの 802.1Q EtherType フィールド値を設定します。
`Router(config-if)# no switchport dot1q ethertype`	デフォルトの 802.1Q EtherType フィールド値（0x8100）に戻します。

カスタム EtherType フィールド値を設定する場合、次の情報に注意してください。

- カスタム EtherType フィールド値を使用するには、ネットワーク上のトラフィック パス内のネットワーク装置すべてがカスタム EtherType フィールド値をサポートする必要があります。
- トランク ポート、アクセス ポート、トンネル ポート上のカスタム EtherType フィールド値を設定できます。
- EtherChannel のメンバ ポート上のカスタム EtherType フィールド値を設定できます。
- ポート チャネル インターフェイス上のカスタム EtherType フィールド値は設定できません。
- ポートごとに、EtherType フィールド値を 1 つだけサポートします。カスタム EtherType フィールド値で設定されたポートでは、他の EtherType フィールド値を持つフレームはタグ付きフレームとして認識されません。たとえば、カスタム EtherType フィールド値で設定されたトランク ポートでは、802.1Q タグ付きフレームの標準 0x8100 EtherType フィールド値は認識されず、このフレームが属する VLAN にフレームを配置することができません。

注意　カスタム EtherType フィールド値で設定されたポートは、他の EtherType フィールド値を持つフレームをタグなしのフレームと見なします。カスタム EtherType フィールド値を持つトランク ポートは、他の EtherType フィールド値を持つフレームをネイティブ VLAN に配置します。カスタム EtherType フィールド値を持つアクセス ポートまたはトンネル ポートは、他の EtherType フィールド値を持つフレームをアクセス VLAN に配置します。カスタム EtherType フィールド値を正しく設定しないと、フレームは間違った VLAN に配置される場合があります。

- カスタム IEEE 802.1Q EtherType フィールド値をサポートするモジュールのリストについては、『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

次に、EtherType フィールド値を 0x1234 に設定する例を示します。

```
Router (config-if)# switchport dot1q ethertype 1234
Router (config-if)#
```

CHAPTER 11

Flex Link の設定

この章では、Catalyst 6500 シリーズ スイッチに Flex Link を設定する手順について説明します。Flex Link は Release12.2(18)SXF 以降のリリースでサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

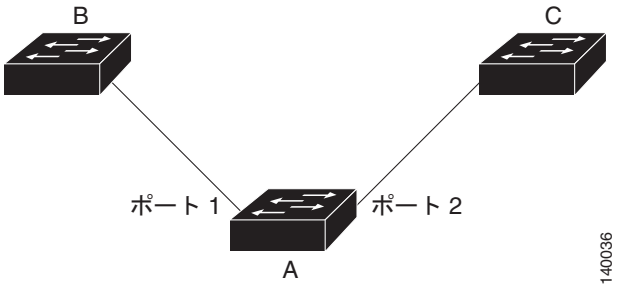
Flex Link の概要

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インターフェイス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。一般的にカスタマーが Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）を実行したくないサービス プロバイダー ネットワークまたは企業ネットワーク内に設定されます。また、Flex Link は、STP の代わりとなるリンク レベルの冗長性を提供します。STP は、Flex Link インターフェイスで自動的にディセーブルになります。

Flex Link 機能を設定するには、1 つのレイヤ 2 インターフェイスをプライマリとするリンクのスタンバイ リンクとして設定します。インターフェイスのペアに Flex Link を設定すると、1 つのインターフェイスのみがリンク アップ ステートになって、トラフィックを転送します。プライマリ リンクがシャットダウンすると、スタンバイ リンクがトラフィックの転送を開始します。非アクティブなリンクが再びアップすると、これがスタンバイ モードになります。

図 11-1 では、アップリンク スイッチ B および C に、スイッチ A のポート 1 およびポート 2 が接続されています。これらは Flex Link として設定されているため、1 つのインターフェイスのみがトラフィックを転送し、もう一方はスタンバイ モードになっています。ポート 1 がアクティブ リンクの場合、ポート 1 とスイッチ B との間でトラフィックの転送が開始され、ポート 2（バックアップ リンク）とスイッチ C との間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、ポート 2 がアップになり、スイッチ C へのトラフィックの転送を開始します。ポート 1 が再びアップになったときには、これはスタンバイ モードになり、トラフィックの転送は行いません。ポート 2 が引き続きトラフィックを転送します。

図 11-1　Flex Link の設定例



プライマリ（転送）リンクがダウンすると、トラップがこれを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 リンクがダウンすると、トラップはユーザに通知します。

Flex Link は レイヤ 2 ポートとポート チャネルでのみサポートされ、VLAN やレイヤ 3 ポートではサポートされません。

Flex Link の設定

ここでは、次の設定情報について説明します。

Flex Link のデフォルト設定

Flex Link にはデフォルト設定がありません。

Flex Link 設定時の注意事項および制約事項

Flex Link を設定する際に、以下の注意事項と制約事項に従ってください。

- アクティブ リンクに設定できる 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異なるインターフェイスでなければなりません。
- インターフェイスは 1 つの Flex Link ペアにのみ属します。1 つのインターフェイスがバックアップ リンクになることができるのは、1 つのアクティブ リンクに対してのみです。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。
- どのリンクも EhterChannel に属しているポートになることはできません。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 チャネルと物理インターフェイスを Flex Link として設定できます。この場合、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をアクティブ リンクとします。
- 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）である必要はありません。ただし、スタンバイ リンクがアクティブになった場合にループが発生したり処理が変更されたりしないように、両方の Flex Link を同様の特性で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になります。STP がスイッチでディセーブルの場合、ネットワーク トポロジでレイヤ 2 ループが存在していないことを確認してください。

- Flex Link ポートやリンクが接続するポートに STP 機能（PortFast、BPDU ガードなど）を設定しないでください。
- 設定された MAC アドレスは、アクティブなポート上とバックアップ ポート上とで異なっていなければなりません。現在の CLI では、2 つのポート上で同じアドレスを設定することはできません。このため、ユーザは Flex Links のフェールオーバー後にこれらのアドレスを再設定しなければなりません。
- Flex Links ポートでのポート セキュリティが、Flex Links のスイッチオーバー中に誤った違反を発生させ、それがポートのセキュリティ シャットダウンまたはアクション制限につながる場合があります。このため、Flex Links ポートではポート セキュリティを設定*しない*ことをお勧めします。

Flex Link の設定

Flex Link 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	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(conf)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	レイヤ 2 インターフェイスを指定します。
ステップ 3	`Router(conf-if)# switchport backup interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	Flex Link ペアの一部としてインターフェイスを設定します。
ステップ 4	`Router(conf-if)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show interface [{`*type*[1] *slot/port*`} | {port-channel` *number*`}] switchport backup`	設定を確認します。
ステップ 6	`Router# copy running-config startup config`	（任意）エントリをスイッチのスタートアップ コンフィギュレーション ファイルに保存します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、バックアップ インターフェイスを持つインターフェイスを設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(conf)# interface fastethernet1/1
Router(conf-if)# switchport backup interface fastethernet1/2
Router(conf-if)# exit
Router# show interface switchport backup
Router Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------------------------
FastEthernet1/1         FastEthernet1/2       Active Up/Backup Standby
FastEthernet1/3         FastEthernet2/4       Active Up/Backup Standby
Port-channel1           GigabitEthernet7/1    Active Up/Backup Standby
```

Flex Link のモニタ

表 11-1 に、Flex Link 設定をモニタするためのイネーブル EXEC コマンドを示します。

表 11-1　Flex Link のモニタ コマンド

コマンド	目的
show interface [{*type*[1] *slot/port*} | {**port-channel** *number*}] **switchport backup**	インターフェイスに設定されている Flex Link バックアップ インターフェイスを表示するか、スイッチに設定されているすべての Flex Link、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ステート（アップまたはスタンバイ モード）を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

CHAPTER 12

EtherChannel の設定

この章では、Catalyst 6500 シリーズ スイッチのレイヤ 2 またはレイヤ 3 LAN ポートに EtherChannel を設定する方法について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

EtherChannel の機能概要

ここでは、EtherChannel の機能について説明します。

EtherChannel 機能の概要

EtherChannel は、個々のイーサネット リンクを 1 つの論理リンクにバンドルすることによって、最大 8 つの物理リンクを合計した帯域幅を提供します。

Release12.2(18)SXE 以降のリリースでは、Catalyst 6500 シリーズ スイッチは最大 128 個の EtherChannel をサポートします。Release12.2(18)SXE よりも前のリリースでは、Catalyst 6500 シリーズ スイッチは最大 64 個の EtherChannel をサポートします。

Catalyst 6500 シリーズ スイッチの任意のモジュール上の（設定に互換性のある）LAN ポートを 8 つまで使用して、1 つの EtherChannel を形成できます。各 EtherChannel の LAN ポートは、すべて同じ速度で、レイヤ 2 ポートまたはレイヤ 3 LAN ポートのどちらか一方として設定されている必要があります。

（注）　Catalyst 6500 シリーズ スイッチに接続するネットワーク装置によって、1 つの EtherChannel にバンドルできるポート数が制限される場合があります。

EtherChannel 内のセグメントで障害が発生すると、障害リンク上でそれまで伝送されていたトラフィックがその EtherChannel 内の残りのセグメントに切り替えられます。障害が発生した場合、EtherChannel 機能はスイッチ、EtherChannel、および障害リンクを識別するトラップを送信します。EtherChannel の 1 つのセグメントに着信したブロードキャストおよびマルチキャスト パケットが、EtherChannel の別のセグメントに戻されることはありません。

EtherChannel の設定方法

ここでは、EtherChannel を設定する手順について説明します。

EtherChannel の設定の概要

EtherChannel を形成するには、EtherChannel を手動で設定するか、Port Aggregation Control Protocol（PAgP）または Link Aggregation Control Protocol（LACP）を使用します。EtherChannel プロトコルを使用すると、接続先のネットワーク装置とダイナミックにネゴシエーションを行うことにより、同様な特性を持つポートが EtherChannel を形成できます。PAgP はシスコ システムズ独自のプロトコルであり、LACP は IEEE 802.3ad で定義されたプロトコルです。

PAgP および LACP はお互いに相互運用しません。PAgP を使用するように設定されたポートは、LACP を使用するように設定されたポートと EtherChannel を形成できません。LACP を使用するように設定されたポートは、PAgP を使用するように設定されたポートと EtherChannel を形成できません。手動で設定されたポートとも相互作用できません。

表 12-1 に、ユーザ側で設定変更可能な EtherChannel モードを示します。

表 12-1　EtherChannel のモード

モード	説明
on	LAN ポートを無条件かつ強制的にチャネル化するモード。**on** モードでは、**on** モードの LAN ポート グループが、**on** モードの別の LAN ポート グループに接続されている場合にのみ、使用可能な EtherChannel が存在します。**on** モードで設定されたポートはネゴシエーションを行わないため、ポート間にネゴシエーション トラフィックは発生しません。EtherChannel プロトコルでは、**on** モードを設定できません。片方の端で **on** モードを使用している場合は、他方の端でもそうしなければなりません。
auto	PAgP モード。LAN ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した PAgP パケットには応答しますが、PAgP ネゴシエーションは開始しません （デフォルト）。
desirable	PAgP モード。LAN 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。ポートは PAgP パケットを送信して、他の LAN ポートとのネゴシエーションを開始します。
passive	LACP モード。ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した LACP パケットには応答しますが、LACP ネゴシエーションは開始しません （デフォルト）。
active	LACP モード。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。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。

EtherChannel の手動設定

手動設定された EtherChannel ポートは、EtherChannel プロトコル パケットを交換しません。手動設定された EtherChannel が形成されるのは、すべてのポートを EtherChannel 互換で設定した場合だけです。

PAgP による EtherChannel 設定

PAgP を使用すると、LAN 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。PAgP パケットが交換されるのは、**auto** モードおよび **desirable** モードのポート間に限られます。

このプロトコルは、LAN ポート グループの機能をダイナミックに学習し、他の LAN ポートに通知します。PAgP は、正確に一致しているイーサネット リンクを識別すると、これらのリンクを 1 つの EtherChannel としてまとめます。作成された EtherChannel は、単一ブリッジ ポートとしてスパニング ツリーに追加されます。

auto モードおよび **desirable** モードでは、PAgP は LAN ポート間でネゴシエーションを行い、ポート速度、トランキング ステートなどの一定の基準に従って EtherChannel を形成できるかどうかを判別します。レイヤ 2 EtherChannel は VLAN 番号も使用します。

LAN ポート間で PAgP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。次に、例を示します。

- **desirable** モードの LAN ポートは、**desirable** モードの別の LAN ポートと EtherChannel を形成できます。
- **desirable** モードの LAN ポートは、**auto** モードの別の LAN ポートと EtherChannel を形成できます。
- **auto** モードの LAN ポートは、どちらのポートもネゴシエーションを開始しないので、**auto** モードの別の LAN ポートとは EtherChannel を形成できません。

IEEE 802.3ad LACP による EtherChannel の設定

LACP では、LAN ポート間で LACP パケットを交換することによる、EtherChannel の自動作成をサポートしています。LACP パケットが交換されるのは、**passive** モードおよび **active** モードのポート間に限られます。

このプロトコルは、LAN ポート グループの機能をダイナミックに学習し、他の LAN ポートに通知します。LACP は、正確に一致しているイーサネット リンクを識別すると、これらのリンクを 1 つの EtherChannel としてまとめます。作成された EtherChannel は、単一ブリッジ ポートとしてスパニング ツリーに追加されます。

passive モードおよび **active** モードでは、LACP は LAN ポート間でネゴシエーションを行い、ポート速度、トランキング ステートなどの一定の基準に従って EtherChannel を形成できるかどうかを判別します。レイヤ 2 EtherChannel は VLAN 番号も使用します。

LAN ポート間で LACP モードが異なっていても、モードが矛盾しない限り EtherChannel を形成できます。次に、例を示します。

- **active** モードの LAN ポートは、**active** モードの別の LAN ポートと EtherChannel を形成できます。
- **active** モードの LAN ポートは、**passive** モードの別の LAN ポートと EtherChannel を形成できます。
- **passive** モードの LAN ポートは、どちらのポートもネゴシエーションを開始しないので、**passive** モードの別の LAN ポートとは EtherChannel を形成できません。

LACP では次のパラメータを使用します。

- LACP システム プライオリティ - LACP が稼動しているスイッチごとに LACP システム プライオリティを設定する必要があります。システム プライオリティは自動設定、または Command-Line Interface（CLI; コマンドライン インターフェイス）から設定することができます（「LACP のシステム プライオリティおよびシステム ID の設定」（P.12-11）を参照）。LACP はシステム ID を形成するために、システム プライオリティとスイッチの MAC（メディア アクセス制御）アドレスを使用します。また、他のシステムとのネゴシエーション中にもこれらを使用します。

  （注）　LACP のシステム ID は、LACP システム プライオリティ値とスイッチの MAC アドレスを組み合わせたものです。

- LACP ポート プライオリティ - LACP を使用するように設定されたポートごとに、LACP ポート プライオリティを設定する必要があります。ポート プライオリティは自動設定、または CLI から設定することができます（「チャネル グループの設定」（P.12-8）を参照）。LACP はポート プライオリティとポート番号を使用してポート ID を形成します。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポート プライオリティを使用して、スタンバイ モードにする必要があるポートを決定します。
- LACP 管理キー - LACP は、LACP を使用するように設定されたポートごとに、チャネル グループ ID 番号と同じ管理キー値を自動的に設定します。管理キーは、他のポートと集約されるポートの機能を定義します。他のポートと集約されるポート機能は、次の要因によって決まります。
  - データ レート、デュプレックス機能、ポイントツーポイント型や共有型メディアなどのポートの物理特性
  - ユーザが作成した設定に関する制限事項

LACP を使用するように設定されたポート上で、LACP は EtherChannel 内の互換性のあるポートの最大数を、ハードウェアで許容されている最大数（8 ポート）以下の値で設定しようとします。互換性のあるすべてのポートを LACP が集約できない場合（たとえば、リモート システムのハードウェア制限が厳しい場合）、チャネルにアクティブに追加できないすべてのポートはホット スタンバイ ステートになり、チャネル ポートのいずれかに障害が発生した場合のみ使用されます。さらに 8 個のスタンバイ ポートを設定できます（EtherChannel には合計 16 個のポートが関連付けられます）。

ポートチャネル インターフェイスの概要

各 EtherChannel には、番号付きのポートチャネル インターフェイスが 1 つずつあります。リリース 12.2(18)SXE 以降のリリースでは、1 ～ 256 の範囲内の番号を使用して、最大 128 のポートチャネル インターフェイスを設定できます。リリース 12.2(18)SXE よりも前のリリースでは、1 ～ 256 の範囲内の番号を使用して、最大 64 のポートチャネル インターフェイスを設定できます。

ポートチャネル インターフェイスに適用する設定は、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 LAN ポートに作用します。

EtherChannel を設定すると、ポートチャネル インターフェイスに適用した設定は、EtherChannel に作用します。一方、LAN ポートに適用した設定は、適用先の LAN ポートだけに作用します。EtherChannel の全ポートのパラメータを変更する場合は、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）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のコンフィギュレーション コマンドをポート チャネル インターフェイスに適用します。

ロード バランシングの概要

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変換することによって、EtherChannel 内のリンク間でトラフィックの負荷を分散させます。

EtherChannel のロード バランシングには、MAC アドレスまたは IP アドレスを使用できます。EtherChannel のロード バランシングにはレイヤ 4 ポート番号も使用できます。EtherChannel のロード バランシングには、送信元と宛先のいずれか、または送信元と宛先の両方のアドレス、またはポートを使用できます。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。EtherChannel のロード バランシングには Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）レイヤ 2 ポート情報も使用できます。

使用する設定で最多の種類のロード バランシング条件を提供するオプションを使用してください。たとえば、EtherChannel 上のトラフィックが 1 つの MAC アドレスにのみ送信され、かつ EtherChannel ロード バランシングの基準として宛先 MAC アドレスを使用している場合、EtherChannel は常に EtherChannel 内の同じリンクを選択します。IP アドレスの送信元アドレスを使用すると、ロード バランシングが向上することがあります。

EtherChannel 機能の設定時の注意事項および制約事項

EtherChannel インターフェイスを正しく設定しないと、ネットワーク ループなど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ることがあります。設定に関する問題を回避するために、次の注意事項および制約事項に従ってください。

- この章で説明するコマンドは、スーパーバイザ エンジンおよび冗長スーパーバイザ エンジンのポートも含めて、Catalyst 6500 シリーズ スイッチのすべての LAN ポートに対して使用できます。
- Release 12.2(17b)SXA 以降のリリースでは、WS-X6548-GE-TX および WS-X6548V-GE-TX スイッチング モジュールは、EtherChannel 単位で 1Gbps を超えるトラフィックをサポートします。
- Release 12.2(17a)SX および Release 12.2(17a)SX1 では、WS-X6548-GE-TX および WS-X6548V-GE-TX ファブリック対応スイッチング モジュールは、EtherChannel 単位で 1Gbps を超えるトラフィックをサポートしません。
- WS-X6148-GE-TX および WS-X6148V-GE-TX スイッチング モジュールは、EtherChannel 単位で 1Gbps を超えるトラフィックをサポートしません。
- EtherChannel への Inter-Switch Link（ISL; スイッチ間リンク）トランキングをサポートしていないメンバ ポートを追加すると、Cisco IOS ソフトウェアは、EtherChannel を ISL トランクとして設定しないように、自動的に **switchport trunk encapsulation dot1q** コマンドをポート チャネル インターフェイスに追加します。EtherChannel がトランクでない場合、**switchport trunk encapsulation dot1q** コマンドが非アクティブになります。
- 冗長スーパーバイザ エンジン上のポートも含めて、すべてのモジュール上のすべてのイーサネット LAN ポートが、EtherChannel（最大 8 つの LAN ポート）をサポートします。これらの LAN ポートは、物理的に隣接している LAN ポートでなくても、また同じモジュール上の LAN ポートでなくてもかまいません。
- 同じ EtherChannel プロトコルを使用するように EtherChannel 内のすべての LAN ポートを設定します。1 つの EtherChannel 内で 2 つの EtherChannel プロトコルを実行することはできません。
- EtherChannel 内のすべての LAN ポートが、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てください。
- LACP は半二重をサポートしません。LACP EtherChannel 内の半二重ポートは中断ステートになります。
- EtherChannel 内のすべての LAN ポートに対して **no shutdown** コマンドを入力します。EtherChannel 内の LAN ポートを 1 つシャットダウンすると、リンク障害として扱われ、そのポートのトラフィックが EtherChannel 内の残りのポートの 1 つに転送されます。
- LAN ポートの 1 つが Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートである場合には、EtherChannel は形成されません。
- レイヤ 3 EtherChannel の場合は、チャネル内の LAN ポートに対してではなく、ポート チャネル論理インターフェイスに対してレイヤ 3 アドレスを割り当ててください。
- レイヤ 2 EtherChannel の場合
  - EtherChannel 内のすべての LAN 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。
  - トランキング LAN 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 モードが同じであることを確認してください。EtherChannel 内の LAN ポートをそれぞれ異なるトランク モードに設定すると、予期しない結果が生じ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 LAN ポートで同じ許容範囲の VLAN をサポートします。VLAN の許容範囲が異なる場合、LAN ポートは EtherChannel を形成しません。

  - STP ポート パス コストが異なる LAN ポートは、設定に互換性がある限り、EtherChannel を形成できます。異なる STP ポート パス コストを設定しても、LAN ポートが EtherChannel を形成できなくなるわけではありません。
  - プロトコル フィルタリングの設定が LAN ポートで異なっている場合には、EtherChannel を形成できません。
- EtherChannel の設定後は、ポート チャネル インターフェイスに適用した設定が EtherChannel に作用します。LAN ポートに適用した設定は、設定を適用した LAN ポートだけに作用します。
- Quality of Service（QoS; サービス品質）がイネーブルであれば、**no mls qos channel-consistency** ポートチャネル インターフェイス コマンドを入力し、完全優先キューのあるポートと完全優先キューのないポートを持つ EtherChannel をサポートします。

注意　PAgP モードまたは LACP モードと手動モードを混在させたり、EtherChannel が設定されていないポートと手動モードを混在させたりすると、重大なトラフィック問題が発生する場合があります。たとえば、**on** モードで設定されているポートが **desirable** モードで設定されている他のポートに接続されたり、EtherChannel 用に設定されていないポートに接続されたりすると、ブリッジ ループができて、ブロードキャスト ストームが発生します。片方の端で **on** モードを使用している場合は、他方の端でもそうしなければなりません。

EtherChannel の設定

ここでは、EtherChannel を設定する手順について説明します。

- 「レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定」（P.12-7）
- 「チャネル グループの設定」（P.12-8）
- 「EtherChannel ロード バランシングの設定」（P.12-11）
- 「EtherChannel Min-Links 機能の設定」（P.12-12）

（注）　LAN ポートが正しく設定されていることを確認してください（「EtherChannel 機能の設定時の注意事項および制約事項」（P.12-6）を参照）。

レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定

（注）

- レイヤ 2 EtherChannel を設定する場合は、手動で作成したポート チャネル論理インターフェイスにレイヤ 2 LAN ポートを追加できません。レイヤ 2 EtherChannel を設定している場合は、ここに記載されている手順を実行しないでください（「チャネル グループの設定」（P.12-8）を参照）。
- レイヤ 3 EtherChannel を設定する場合は、ここに記載されたポート チャネル論理インターフェイスを手動で作成し、レイヤ 3 LAN ポートをチャネル グループに追加する必要があります（「チャネル グループの設定」（P.12-8）を参照）。
- レイヤ 3 LAN ポートから EtherChannel に IP アドレスを移動するには、レイヤ 3 LAN ポートから IP アドレスを削除したあとで、その IP アドレスをポート チャネル論理インターフェイス上で設定する必要があります。

レイヤ 3 EtherChannel 用のポートチャネル インターフェイスを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface port-channel group_number`	ポートチャネル インターフェイスを作成します。
	`Router(config)# no interface port-channel group_number`	ポートチャネル インターフェイスを削除します。
ステップ 2	`Router(config-if)# ip address ip_address mask`	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show running-config interface port-channel group_number`	設定を確認します。

Release12.2(18)SXE 以降のリリースでは、*group_number* は 1 ～ 256 で、最大 128 個のポート チャネル インターフェイスを作成できます。Release12.2(18)SXE よりも前のリリースでは、*group_number* は 1 ～ 256 で、最大 64 個のポート チャネル インターフェイスを作成できます。

次に、ポート チャネル インターフェイス 1 を作成する例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(config-if)# end
```

次に、ポート チャネル インターフェイス 1 の設定を確認する例を示します。

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration:
!
interface Port-channel1
 ip address 172.32.52.10 255.255.255.0
 no ip directed-broadcast
end
Router#
```

チャネル グループの設定

（注）

- レイヤ 3 EtherChannel を設定する場合は、ポート チャネル論理インターフェイスを手動で作成してから（「レイヤ 3 EtherChannel のポート チャネル論理インターフェイスの設定」（P.12-7）を参照）、ここに記載されているように、レイヤ 3 LAN ポートをチャネル グループに追加する必要があります。
- レイヤ 2 EtherChannel を設定するには、ここに記載されているように、ポート チャネル論理インターフェイスを自動作成する **channel-group** コマンドを使用して、LAN ポートを設定します。手動で作成したポート チャネル インターフェイスにレイヤ 2 LAN ポートを組み込むことはできません。
- Cisco IOS がレイヤ 2 EtherChannel 用のポート チャネル インターフェイスを作成するには、レイヤ 2 LAN ポートが接続され、動作している必要があります。

チャネル グループを設定するには、LAN ポートごとに次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# no ip address`	この LAN ポートに IP アドレスが割り当てられていないことを確認します。
ステップ 3	`Router(config-if)# channel-protocol {lacp | pagp}`	（任意）選択した LAN ポート上で、**channel-group** コマンドの適用範囲を、**channel-protocol** コマンドを使用して設定された EtherChannel プロトコルに制限します。
	`Router(config-if)# no channel-protocol`	制限を解除します。
ステップ 4	`Router(config-if)# channel-group group_number mode {active | auto | desirable | on | passive}`	ポートチャネル内の LAN ポートを設定し、モードを指定します（表 12-1（P.12-3）を参照）。PAgP は、auto および desirable モードのみをサポートします。LACP は、active および passive モードのみをサポートします。
	`Router(config-if)# no channel-group`	チャネル グループから LAN ポートを削除します。
ステップ 5	`Router(config-if)# lacp port-priority priority_value`	（LACP 用で任意）有効な値は、1 ～ 65535 です。数字が大きい方がプライオリティが低くなります。デフォルト値は 32768 です。
	`Router(config-if)# no lacp port-priority`	デフォルト値に戻します。
ステップ 6	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 7	`Router# show running-config interface type[1] slot/port` `Router# show interfaces type[1] slot/port etherchannel`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/6 および 5/7 を、ポートチャネル 2、PAgP、モード **desirable** に設定する例を示します。

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```

（注）　**range** キーワードの詳細については、「インターフェイスの範囲設定」（P.9-4）を参照してください。

次に、ポート チャネル インターフェイス 2 の設定を確認する例を示します。

```
Router# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
end
Router#
```

次に、ファスト イーサネット ポート 5/6 の設定を確認する例を示します。

```
Router# show running-config interface fastethernet 5/6
Building configuration...

Current configuration:
!
interface FastEthernet5/6
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
Router# show interfaces fastethernet 5/6 etherchannel
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                               Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/2     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 04d:18h:57m:19s
```

次に、LAN ポートを設定したあとに、ポート チャネル インターフェイス 2 の設定を確認する例を示します。

```
Router# show etherchannel 12 port-channel
                Port-channels in the group:
                ----------------------

Port-channel: Po12
------------

Age of the Port-channel   = 04d:18h:58m:50s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP

Router#
```

LACP のシステム プライオリティおよびシステム ID の設定

LACP のシステム ID は、LACP システム プライオリティ値とスイッチの MAC アドレスを組み合わせたものです。

LACP のシステム プライオリティおよびシステム ID を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# lacp system-priority` *priority_value*	（LACP 用で任意）有効な値は、1 ～ 65535 です。数字が大きい方がプライオリティが低くなります。デフォルト値は 32768 です。
	`Router(config)# no lacp system-priority`	デフォルト値に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show lacp sys-id`	設定を確認します。

次に、LACP のシステム プライオリティを設定する例を示します。

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

次に、設定を確認する例を示します。

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

システム プライオリティが最初に表示され、次にスイッチの MAC アドレスが表示されます。

EtherChannel ロード バランシングの設定

EtherChannel ロード バランシングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}`	EtherChannel ロード バランシングを設定します。
	`Router(config)# no port-channel load-balance`	デフォルトの EtherChannel ロード バランシングに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show etherchannel load-balance`	設定を確認します。

ロード バランシングのキーワードの意味は、次のとおりです。

- **dst-ip** - 宛先 IP アドレス
- **dst-mac** - 宛先 MAC アドレス
- **dst-port** - 宛先レイヤ 4 ポート
- **mpls** - MPLS パケットのロード バランシング
- **src-dst-ip** - 送信元および宛先 IP アドレス
- **src-dst-mac** - 送信元および宛先 MAC アドレス
- **src-dst-port** - 送信元および宛先レイヤ 4 ポート
- **src-ip** - 送信元 IP アドレス
- **src-mac** - 送信元 MAC アドレス
- **src-port** - 送信元レイヤ 4 ポート

次に、送信元および宛先 IP アドレスを使用するように EtherChannel を設定する例を示します。

```
Router# configure terminal
Router(config)# port-channel load-balance src-dst-ip
Router(config)# end
Router(config)#
```

次に、設定を確認する例を示します。

```
Router# show etherchannel load-balance
Source XOR Destination IP address
Router#
```

EtherChannel Min-Links 機能の設定

（注）　Release12.2(18)SXF 以降のリリースでは、EtherChannel Min-Links 機能をサポートします。

EtherChannel Min-Links 機能は、LACP EtherChannel でサポートされています。この機能を使用すると、リンク アップ ステートであり、かつリンク アップ ステートに移行させるためにポート チャネル インターフェイスの EtherChannel にバンドルされていなければならないメンバ ポートの最小数を設定できます。EtherChannel Min-Links 機能を使用して低帯域幅の LACP EtherChannel をアクティブにしないようにできます。またこの機能により、アクティブなメンバ ポートが少なすぎて必要な最小帯域幅を供給できないような場合に、LACP EtherChannel を非アクティブにすることもできます。

EtherChannel Min-Links 機能を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface port-channel group_number`	LACP ポート チャネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# port-channel min-links number`	リンク アップ ステートになっていて、リンク アップ ステートに移行させるためにポート チャネル インターフェイスの EtherChannel にバンドルされていなければならないメンバ ポートの最小数を設定します。
	`Router(config-if)# no port-channel min-links`	デフォルトの アクティブ メンバ ポート数（1）に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show running-config interface type[1] slot/port` `Router# show interfaces type[1] slot/port etherchannel`	設定を確認します。

（注）　EtherChannel の一端でのみ EtherChannel Min-Links 機能が設定されていて正常に機能していた場合でも、最適な結果を得るためには、同じ数の最小リンクを EtherChannel の両端で設定します。

次に、EtherChannel でアクティブなメンバ ポートが 2 個未満の場合にポート チャネル インターフェイス 1 を非アクティブに設定する例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# port-channel min-links 2
Router(config-if)# end
```

CHAPTER 13

VLAN トランキング プロトコル（VTP）の設定

この章では、Catalyst 6500 シリーズ スイッチ に VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を設定する方法について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

VTP の機能概要

VTP はレイヤ 2 のメッセージング プロトコルであり、VTP ドメインでの Virtual LAN（VLAN; 仮想 LAN）の追加、削除、名前変更などを管理することにより、VLAN 設定の整合性を維持します。VTP ドメイン（別名、VLAN 管理ドメイン）は、同じ VTP ドメイン名を共有し、トランクで相互接続された 1 つ以上のネットワーク装置で構成されます。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などのさまざまな問題によって生じる不正な設定および設定の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 台または複数のネットワーク装置上で中央集約的に設定変更を行い、それらの変更を自動的にネットワーク上の他のネットワーク装置に伝達することができます。

（注） VLAN の詳しい設定手順については、第 14 章「仮想 LAN（VLAN）の設定」を参照してください。

ここでは、VTP の機能について説明します。

VTP ドメインの概要

VTP ドメイン（別名、VLAN 管理ドメイン）は、同じ VTP ドメイン名を共有し、相互接続された 1 つまたは複数のネットワーク装置で構成されます。1 つのネットワーク装置が所属できる VTP ドメインは 1 つだけです。ドメインのグローバル VLAN 設定を変更するには、Command-Line Interface（CLI; コマンドライン インターフェイス）または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用します。

デフォルトでは、Catalyst 6500 シリーズ スイッチは VTP サーバ モードであり、トランク リンクを介してドメインに関するアドバタイズをスイッチが受信するか、またはユーザが管理ドメインを設定しない限り、非管理ドメイン ステートのままです。

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した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。スイッチは、別の管理ドメイン名または古い設定のリビジョン番号が指定されたアドバタイズについては無視します。

スイッチ を VTP 透過として設定した場合、VLAN の作成および変更は可能ですが、その変更が適用されるのは個々のスイッチに限られます。

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ネットワーク装置に伝播されます。VTP アドバタイズはトランク接続すべてに送信されます。

VTP は、一意の名前と内部インデックスの対応によって、複数の LAN タイプに対して VLAN をダイナミック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装置を管理するための作業負担が大幅に軽減されます。

VTP モードの概要

次のいずれかの VTP モードで動作するように Catalyst 6500 シリーズ スイッチを設定できます。

- サーバ - VTP サーバ モードでは、VLAN の作成、変更、および削除を行うことができます。また、VTP ドメイン全体に対して他の設定パラメータ（VTP バージョン、VTP プルーニングなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のネットワーク装置に、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、VLAN 設定を他のネットワーク装置と同期化します。VTP サーバがデフォルトのモードです。
- 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ますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。
- 透過 - VTP 透過ネットワーク装置は、VTP に関与しません。VTP 透過ネットワーク装置は、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同期化することもありません。ただし VTP バージョン 2 では、透過ネットワーク装置は、トランキング LAN ポートから受信した VTP アドバタイズを転送します。

（注）　Catalyst 6500 シリーズ スイッチは、NVRAM（不揮発性 RAM）に設定を書き込むときにスイッチが障害を検出すると、自動的に VTP サーバ モードから VTP クライアント モードに切り替わります。この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。

VTP アドバタイズの概要

VTP ドメインの各ネットワーク装置は、予約されたマルチキャスト アドレスに対して、各トランキング LAN ポートからアドバタイズを定期的に送信します。VTP アドバタイズを受信した近接ネットワーク装置は、必要に応じて各自の VTP および VLAN 設定を更新します。

VTP アドバタイズでは、次のグローバル設定情報が配布されます。

- VLAN ID（Inter-Switch Link（ISL; スイッチ間リンク）および 802.1Q）
- エミュレート LAN 名（Asynchronous Transfer Mode（ATM; 非同期転送モード）LAN Emulation（LANE; LAN エミュレーション）用）
- 802.10 Security Association Identifier（SAID）値（FDDI）
- VTP ドメイン名
- VTP 設定のリビジョン番号
- 各 VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを含めた VLAN 設定
- フレーム形式

VTP バージョン 2 の概要

ネットワークで VTP を使用する場合は、VTP バージョン 1 またはバージョン 2 のどちらを使用するかを決定する必要があります。

（注）　トークンリング環境で VTP を使用している場合は、バージョン 2 を使用する必要があります。

VTP バージョン 2 でサポートされる機能は、次のとおりです。バージョン 1 ではサポートされません。

- トークンリング サポート - VTP バージョン 2 は、トークンリング LAN スイッチングおよび VLAN（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））をサポートします。トークンリング VLAN の詳細については、「VLAN の機能概要」（P.14-1）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。認識不能な TLV は、NVRAM に保存されます。
- バージョン依存型透過モード - VTP バージョン 1 の場合、VTP 透過ネットワーク装置は、VTP メッセージの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ってメッセージを転送します。スーパーバイザ エンジン ソフトウェアでサポートされるドメインは 1 つだけなので、VTP バージョン 2 は、バージョンをチェックせずに VTP メッセージを透過モードで転送します。

- 整合性検査 - VTP バージョン 2 では、CLI または SNMP 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 メッセージのダイジェストが有効であれば、整合性検査を行わずに情報を受け入れます。

VTP プルーニングの概要

VTP プルーニングは、ブロードキャスト パケット、マルチキャスト パケット、未知のパケット、フラッディング ユニキャスト パケットなど、不要なフラッディング トラフィックを削減することにより、ネットワークの帯域幅を拡張します。VTP プルーニングを使用すると、トラフィックがネットワーク装置にアクセス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、使用可能な帯域幅が増えます。VTP 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 プルーニングを有効にするには、管理ドメイン内のすべての装置が VTP プルーニングをサポートする必要があります。VTP プルーニングをサポートしない装置については、トランク上で VLAN を使用できるように手動で設定する必要があります。

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。ネットワーク スイッチ 1 のインターフェイス 1 およびスイッチ 4 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 1 に接続されたホストから、ブロードキャストが送信されます。スイッチ 1 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 3、5、6 も含めて、ネットワーク内の全ネットワーク装置がこのブロードキャストを受信します。

プルーニングの設定は、Catalyst 6500 シリーズ スイッチ上でグローバルに行います（「VTP プルーニングのイネーブル化」（P.13-8）を参照）。レイヤ 2 トランキング LAN ポートにプルーニングを設定します（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-9）を参照）。

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

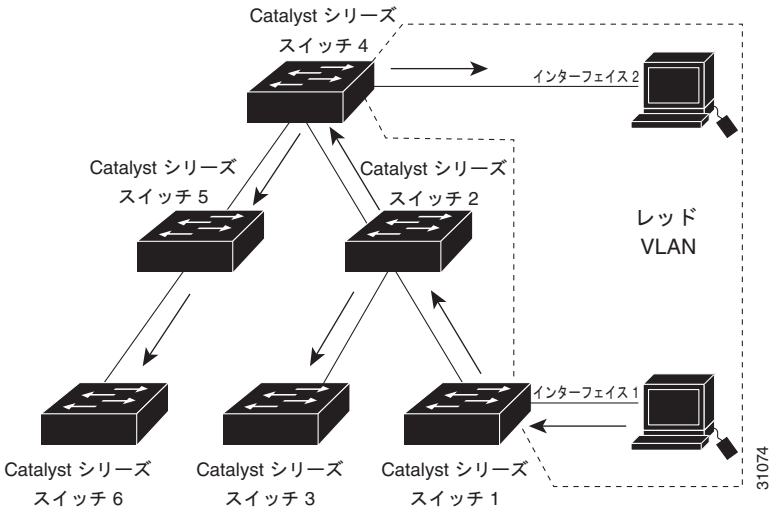
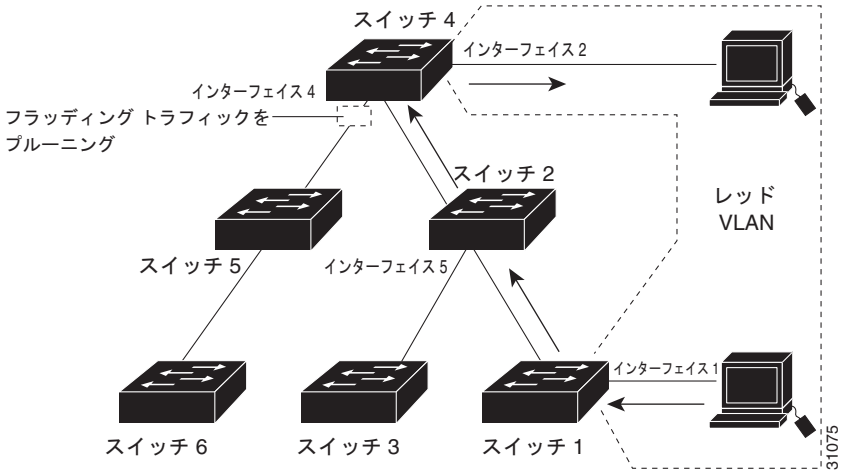


図 13-2 は、VTP プルーニングをイネーブルにした場合の同じスイッチド ネットワークを示しています。Red VLAN のトラフィックは指定されたリンク（スイッチ 2 のポート 5、スイッチ 4 のポート 4）でプルーニングされるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 3、5、6 には転送されません。

図 13-2　VTP プルーニングを使用した場合のフラッディング トラフィック



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。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。デフォルトでは、VLAN 2 ～ 1000 がプルーニング適格です。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 は常にプルーニング不適格です。VLAN 1 からのトラフィックをプルーニングすることはできません。

トランキング LAN ポートに VTP プルーニングを設定するには、**switchport trunk pruning vlan** コマンドを使用します（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-9）を参照）。VTP プルーニングは、LAN ポートがトランキングを実行している場合に動作します。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またはディセーブルのどちらに設定されているか、特定の VLAN が存在するかどうか、および LAN ポート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、設定することができます。

VTP のデフォルト設定

表 13-1 に、VTP のデフォルト設定を示します。

表 13-1　VTP のデフォルト設定

機能	デフォルト値
VTP ドメイン名	ヌル
VTP モード	サーバ
VTP バージョン 2 のイネーブル ステート	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 設定時の注意事項および制約事項

ネットワークに VTP を実装する際、次の注意事項および制約事項に注意してください。

- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンを搭載したスイッチに、**vtp file** *file_name* コマンドを入力しないでください。
- 冗長スーパーバイザ エンジンを取り付ける前に、デフォルト設定に戻すには **no vtp file** コマンドを入力します。
- VTP ドメイン内のすべてのネットワーク装置で、同じ VTP バージョンを実行する必要があります。
- セキュア モードの場合、管理ドメイン内の各ネットワーク装置にパスワードを設定する必要があります。

注意　VTP パスワードを設定した場合、ドメイン内の各ネットワーク装置に管理ドメイン パスワードを割り当てないと、管理ドメインは正常に動作しません。

- VTP バージョン 2 対応のネットワーク装置上で 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 対応ネットワーク装置は、同一 VTP ドメイン内で VTP バージョン 1 が稼動しているネットワーク装置として動作することができます（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ネットワーク装置がバージョン 2 に対応する場合を除いて、ネットワーク装置上で VTP バージョン 2 をイネーブルにしないでください。ネットワーク装置上で VTP 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 対応ネットワーク装置で VTP バージョン 2 がイネーブルになります。
- 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常に動作させるために、VTP バージョン 2 をイネーブルにする必要があります。
- VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン全体で VTP プルーニングがイネーブルまたはディセーブルになります。
- プルーニングの適格性の設定は、スイッチ上のすべてのトランクにグローバルに適用されます。プルーニングの適格性は、各トランクに個別に設定できません。
- 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、その VLAN のプルーニング適格性の影響を受けるのはそのスイッチだけです。VTP ドメイン内のすべてのネットワーク装置に影響するわけではありません。
- VTPv1 および VTPv2 は、拡張範囲 VLAN（VLAN 番号 1006 ～ 4094）の設定情報を伝播しません。各ネットワークデバイスで拡張範囲 VLAN を手動で設定する必要があります。
- VTP が使用する利用可能な DRAM が不十分な場合、VTP のモードは透過に変わります。
- VTP 透過モードのネットワーク装置は、VTP Join メッセージを送信しません。VTP 透過モードのネットワーク装置にトランク接続されている Catalyst 6500 シリーズ スイッチでは、透過モード ネットワーク装置によって使用される VLAN、またはプルーニング不適格としてトランク全体に伝送する必要がある VLAN を設定します。プルーニング適格性の設定については、「プルーニング適格 VLAN のリストの設定」（P.10-13）を参照してください。

VTP の設定

ここでは、VTP の設定手順について説明します。

VTP グローバル パラメータの設定

ここでは、VTP グローバル パラメータの設定について説明します。

（注）　VTP グローバル パラメータは、グローバル コンフィギュレーション モード、または EXEC モードで入力できます。

VTP パスワードの設定

VTP グローバル パラメータを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# vtp password password_string`	VTP ドメインのパスワード（8 ～ 64 文字）を設定します。
`Router(config)# no vtp password`	パスワードを消去します。

次に、グローバル コンフィギュレーション モードで VTP パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```

次に、EXEC モードで VTP パスワードを設定する例を示します。

```
Router# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```

（注）　パスワードは実行コンフィギュレーション ファイルには保存されません。

VTP プルーニングのイネーブル化

管理ドメイン内で VTP プルーニングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vtp pruning`	管理ドメイン内で VTP プルーニングをイネーブルにします。
	`Router(config)# no vtp pruning`	管理ドメイン内で VTP プルーニングをディセーブルにします。
ステップ 2	`Router# show vtp status`	設定を確認します。

次に、管理ドメイン内で VTP プルーニングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp pruning
Pruning switched ON
```

次に、リリースに関係なく、管理ドメイン内で VTP プルーニングをイネーブルにする例を示します。

```
Router# vtp pruning
Pruning switched ON
```

次に、設定を確認する例を示します。

```
Router# show vtp status | include Pruning
VTP Pruning Mode: Enabled
Router#
```

プルーニング適格性の設定については、「プルーニング適格 VLAN のリストの設定」（P.10-13）を参照してください。

VTP バージョン 2 のイネーブル化

VTP バージョン 2 対応のネットワーク装置では、デフォルトで VTP バージョン 2 がディセーブルに設定されています。ネットワーク装置で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべての VTP バージョン 2 対応ネットワーク装置でバージョン 2 がイネーブルになります。

注意　同一 VTP ドメイン内のネットワーク装置に関して、VTP バージョン 1 とバージョン 2 の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ネットワーク装置で、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ネットワーク装置が VTP バージョン 2 をサポートしている場合以外では、VTP バージョン 2 をイネーブルにしないでください。

（注）　トークンリング環境では、トークンリング インターフェイスをサポートする装置上でトークンリング VLAN スイッチングを正常に動作させるために、VTP バージョン 2 をイネーブルにする必要があります。

VTP バージョン 2 をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **vtp version** {**1** | **2**}	VTP バージョン 2 をイネーブルにします。
	Router(config)# **no vtp version**	デフォルト値に戻します（VTP バージョン 1）。
ステップ 2	Router# **show vtp status**	設定を確認します。

次に VTP バージョン 2 をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp version 2
V2 mode enabled.
Router(config)#
```

次に、リリースに関係なく、VTP バージョン 2 をイネーブルにする例を示します。

```
Router# vtp version 2
V2 mode enabled.
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status | include V2
VTP V2 Mode: Enabled
Router#
```

VTP モードの設定

VTP モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **vtp mode** {**client** | **server** | **transparent**}	VTP モードを設定します。
	Router(config)# **no vtp mode**	デフォルトの VTP モードに戻します（サーバ）。
ステップ 2	Router(config)# **vtp domain** *domain_name*	（任意 - サーバ モード用）VTP ドメイン名を定義します（最大 32 文字）。VTP サーバ モードではドメイン名が必要です。スイッチが VTP ドメインにトランク接続されている場合、スイッチはドメイン内の VTP サーバからドメイン名を取得します。 **（注）**　ドメイン名は消去できません。
ステップ 3	Router(config)# **end**	VLAN コンフィギュレーション モードを終了します。
ステップ 4	Router# **show vtp status**	設定を確認します。

（注）　VTP 透過モードでは、VLAN 設定はスタートアップ コンフィギュレーション ファイルに保存されます。

次に、スイッチを VTP サーバとして設定する例を示します。

```
Router# configuration terminal
Router(config)# vtp mode server
Setting device to VTP SERVER mode.
Router(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status
VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 33
VTP Operating Mode              : Server
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Local updater ID is 172.20.52.34 on interface Gi1/1 (first interface found)
Router#
```

次に、スイッチを VTP クライアントとして設定する例を示します。

```
Router# configuration terminal
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)# exit
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status
VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 33
VTP Operating Mode              : Client
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Router#
```

次にスイッチ上で VTP をディセーブルにする例を示します。

```
Router# configuration terminal
Router(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show vtp status
VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 33
VTP Operating Mode              : Transparent
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Router#
```

VTP 統計情報の表示

VTP に関する統計情報（送受信された VTP アドバタイズ、VTP エラーなど）を表示するには、次の作業を行います。

コマンド	目的
`Router# show vtp counters`	VTP の統計情報を表示します。

次に、VTP の統計情報を表示する例を示します。

```
Router# show vtp counters
VTP statistics:
Summary advertisements received    : 7
Subset advertisements received     : 5
Request advertisements received    : 0
Summary advertisements transmitted : 997
Subset advertisements transmitted  : 13
Request advertisements transmitted : 3
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa5/8               43071            42766            5
```

CHAPTER 14

仮想 LAN（VLAN）の設定

この章では、Catalyst 6500 シリーズ スイッチに Virtual LAN（VLAN; 仮想 LAN）を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

VLAN の機能概要

ここでは、VLAN の機能について説明します。

VLAN の概要

VLAN は、物理的な位置にかかわりなく、共通の要件を持つエンド ステーションのグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、物理的に同じ LAN セグメントに置かれていないエンド ステーションでもグループ化することができます。

VLAN は、通常 IP サブネットワークと関連付けます。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 ステーションを同じ VLAN に属させる場合などです。VLAN 相互間のトラフィックは、ルーティングする必要があります。LAN ポートの VLAN メンバシップは、ポートごとに手動で割り当てます。

VLAN の範囲

（注）　4096 個の VLAN を使用するには、拡張システム ID をイネーブルにする必要があります（「ブリッジ ID の概要」（P.20-3）を参照）。

Catalyst 6500 シリーズ スイッチは、Institute of Electrical and Electronic Engineers（IEEE; 米国電気電子学会）802.1Q 規格に準拠した VLAN を 4096 個サポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）を使用している場合、これらの VLAN の一部はネットワーク内の他のスイッチに伝播されます。拡張範囲 VLAN は伝播されないため、ネットワーク装置ごとに手動で設定する必要があります。

表 14-1 に VLAN の範囲を示します。

表 14-1　VLAN の範囲

VLAN	範囲	用途	VTP による伝播
0, 4095	予約済み	システム専用です。これらの VLAN は参照または使用できません。	—
1	標準	シスコ システムズのデフォルトです。使用できますが、削除できません。	あり
2 ～ 1001	標準	イーサネット VLAN に使用します。作成、使用、削除できます。	あり
1002 ～ 1005	標準	FDDI およびトークンリング用のシスコ システムズのデフォルトです。VLAN 1002 ～ 1005 は削除できません。	あり
1006 ～ 4094	拡張	イーサネット VLAN 専用です。	なし

次の情報が VLAN の範囲に適用されます。

- レイヤ 3 LAN ポート、WAN インターフェイスとサブインターフェイス、および一部のソフトウェアの機能は、拡張範囲内の内部 VLAN を使用します。内部使用に割り当てられている拡張範囲 VLAN は使用できません。
- 内部で使用されている VLAN を表示するには、**show vlan internal usage** コマンドを入力します。旧リリースの場合は、**show vlan internal usage** および **show cwan vlans** コマンドを入力します。
- 昇順の内部 VLAN 割り当て（1006 以降の番号）、または降順の内部 VLAN 割り当て（4094 以下の番号）を設定できます。
- 拡張範囲 VLAN を使用するには、拡張システム ID をイネーブルにする必要があります（「ブリッジ ID の概要」（P.20-3）を参照）。

設定可能な VLAN パラメータ

（注）
- イーサネット VLAN 1 はデフォルト値だけを使用します。
- VLAN 名を除き、イーサネット VLAN 1006 ～ 4094 はデフォルト値だけを使用します。
- 1006 ～ 4094 のイーサネット VLAN に対し、VLAN 名を設定できます。

VLAN 2 ～ 1001 では、次のパラメータを設定できます。

- VLAN 名
- VLAN タイプ（イーサネット、Fiber Distributed Data Interface（FDDI）、FDDI Network Entity Title（NET）、Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）、または 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 ステート（アクティブまたは中断）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF 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

トークンリング VLAN の概要

ここでは、VTP バージョン 2 が稼動するネットワーク装置でサポートされる、2 つのトークンリング VLAN タイプについて説明します。

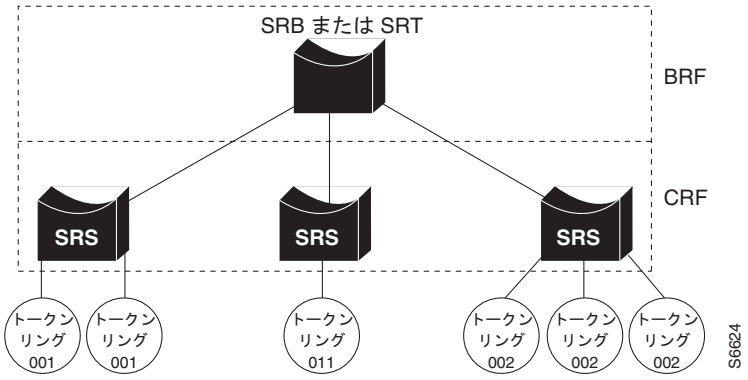
- 「トークンリング TrBRF VLAN」（P.14-4）
- 「トークンリング TrCRF VLAN」（P.14-5）

（注）Catalyst 6500 シリーズ スイッチは、Inter-Switch Link（ISL; スイッチ間リンク）でカプセル化されたトークンリング フレームをサポートしません。Catalyst 6500 シリーズ スイッチが VTP サーバとして設定されている場合は、スイッチからトークンリング VLAN を設定することができます。

トークンリング TrBRF VLAN

トークンリング ブリッジ リレー機能（TrBRF）VLAN は、スイッチド トークンリング ネットワーク環境において、複数のトークンリング コンセントレータ リレー機能（TrCRF）VLAN を相互接続します（図 14-1 を参照）。TrBRF は、トランク リンクを経由して相互接続されたネットワーク装置全体に拡張することができます。TrCRF と TrBRF 間の接続を*論理ポート*といいます。

図 14-1　　相互接続されたトークンリング TrBRF VLAN および TrCRF VLAN



ソース ルーティングでは、Catalyst 6500 シリーズ スイッチは各論理リング間を結ぶ単一のブリッジになります。TrBRF は、IBM または IEEE STP を実行する Source-Route Bridge（SRB; ソースルート ブリッジ）または Source-Route Transparent（SRT; ソースルート トランスペアレント）ブリッジとして動作できます。SRB を使用する場合、異なる論理リングに重複する Media Access Control（MAC; メディア アクセス制御）アドレスを定義できます。

トークンリング ソフトウェアは、TrBRF VLAN および TrCRF VLAN ごとに 1 つずつ STP インスタンスを実行します。TrCRF VLAN の場合、STP により、論理リングのループが排除されます。TrBRF VLAN の場合、STP は外部ブリッジと対話して、ブリッジ トポロジからループを排除します。これはイーサネット VLAN における STP の動作と同様です。

注意　特定の親 TrBRF STP および TrCRF ブリッジ モードを設定すると、TrBRF の論理ポート（TrBRF と TrCRF 間の接続）がブロック ステートになる可能性があります。詳細については、「VLAN 設定時の注意事項および制約事項」（P.14-9）を参照してください。

IBM の System Network Architecture（SNA）トラフィックに対応するために、SRT モードと SRB モードを組み合わせて使用することができます。混在モードでは、TrBRF の判別により、一部のポート（TrCRF に接続された論理ポート）は SRB モードで動作し、他のポートは SRT モードで動作します。

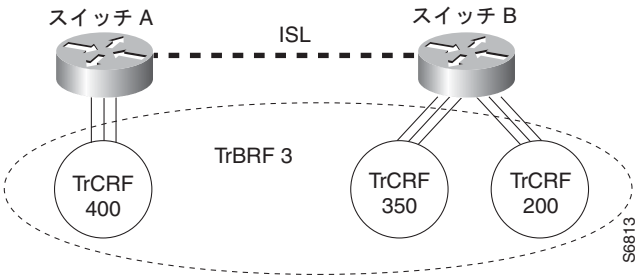
トークンリング TrCRF VLAN

トークンリング コンセントレータ リレー機能（TrCRF）VLAN は、同じ論理リング番号を持つポート グループを定義します。2 種類の TrCRF をネットワークで設定できます。非分散型とバックアップです。

通常、TrCRF は非分散型です。つまり、各 TrCRF が 1 台のネットワーク装置のポートに限定されます。同一ネットワーク装置または異なるネットワーク装置上の複数の非分散型 TrCRF を、1 つの親 TrBRF に対応させることができます（図 14-2 を参照）。親 TrBRF はマルチポート ブリッジとして動作し、非分散型 TrCRF の間でトラフィックを転送します。

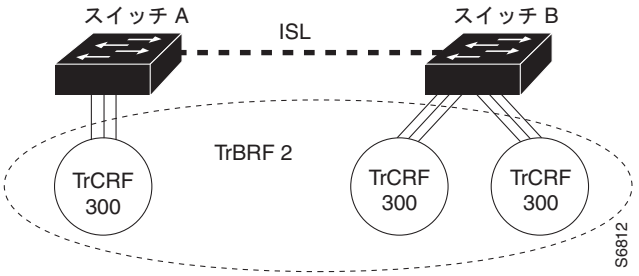
（注）　異なるネットワーク装置上に存在するリング間でデータを渡すには、リングを同じ TrBRF に関連付け、その TrBRF を SRB 用に設定します。

図 14-2　　非分散型 TrCRF



デフォルトの設定では、トークンリング ポートはデフォルトの TrCRF（VLAN 1003、trcrf-default）に対応し、これにはデフォルトの TrBRF（VLAN 1005、trbrf-default）が親として存在します。この設定では、分散型 TrCRF が可能であり（図 14-3 を参照）、ネットワーク装置が ISL トランクを介して接続されていれば、異なるネットワーク装置上のデフォルト TrCRF 間をトラフィックが通過できます。

図 14-3　　分散型 TrCRF



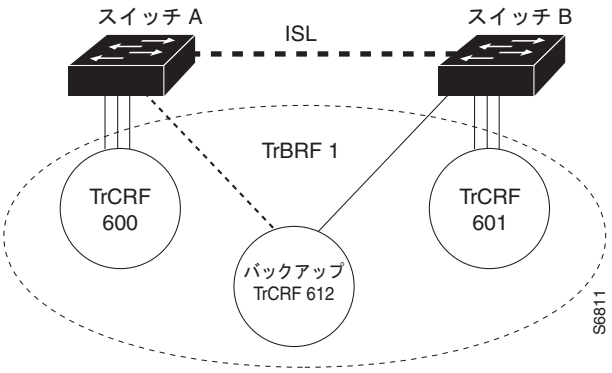
TrCRF 内では、ソースルート スイッチングを使用し、MAC アドレスまたはルート ディスクプリタに基づいてフレーム転送を行います。VLAN 全体を 1 つのリングとして動作させ、フレームを 1 つの TrCRF 内のポート間でスイッチングすることもできます。

各 TrCRF の All-Routes フレームおよび Spanning Tree Explorer フレームに対して、最大ホップ カウントを指定できます。最大ホップ カウントを指定すると、エクスプローラが経由できる最大ホップ数が制限されます。ポートが受信したエクスプローラ フレームが、指定のホップ数を超えて送信されたことが判別されると、ポートはそのフレームを転送しません。TrCRF は、ルート情報フィールドのブリッジ ホップ数によって、エクスプローラが経由したホップ数を判別します。

ネットワーク装置間の ISL 接続に障害が発生した場合、バックアップ TrCRF を使用して非分散型 TrCRF 間のトラフィックに代替ルートを設定できます。1 つの TrBRF に設定できるバックアップ TrCRF は 1 つだけで、バックアップ TrCRF に属すことができるのは、各ネットワーク装置で 1 つのポートに限られます。

ネットワーク装置間の ISL 接続に障害が発生した場合、影響を受ける各ネットワーク装置上のバックアップ TrCRF ポートが自動的にアクティブになり、バックアップ TrCRF を介して非分散型 TrCRF 間のトラフィックが再ルーティングされます。ISL 接続が再確立されると、バックアップ TrCRF の 1 つのポートを除くすべてのポートがディセーブルになります。図 14-4 に、バックアップ TrCRF を示します。

図 14-4　　バックアップ TrCRF



VLAN のデフォルト設定

表 14-2 ～ 14-6 に、VLAN メディア タイプ別のデフォルト設定を示します。

表 14-2　　イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ～ 4094
VLAN 名	default（VLAN 1 の場合） VLAN*vlan_ID*（他のイーサネット VLAN の場合）	—
802.10 SAID	10*vlan_ID*	100001 ～ 104094
Maximum Transmission Unit（MTU; 最大伝送ユニット）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、中断
プルーニング適格性	VLAN 2 ～ 1001 はプルーニング適格です。VLAN 1006 ～ 4094 は、プルーニング不適格です。	—

表 14-3　FDDI VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1002	1 ～ 1005
VLAN 名	fddi-default	—
802.10 SAID	101002	1 ～ 4294967294
MTU サイズ	1500	1500 ～ 18190
リング番号	0	1 ～ 4095
親 VLAN	0	0 ～ 1005
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、中断

表 14-4　トークンリング（TrCRF）VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1003	1 ～ 1005
VLAN 名	token-ring-default	—
802.10 SAID	101003	1 ～ 4294967294
リング番号	0	1 ～ 4095
MTU サイズ	VTPv1 のデフォルトは 1500 VTPv2 のデフォルトは 4472	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、中断
ブリッジ モード	srb	srb、srt
ARE 最大ホップ数	7	0 ～ 13
STE 最大ホップ数	7	0 ～ 13
バックアップ Concentrator Relay Function（CRF; コンセントレータ リレー機能）	ディセーブル	ディセーブル、イネーブル

表 14-5　FDDI-Net VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1004	1 ～ 1005
VLAN 名	fddinet-default	—
802.10 SAID	101004	1 ～ 4294967294
MTU サイズ	1500	1500 ～ 18190
ブリッジ番号	1	0 ～ 15
STP タイプ	ieee	auto、ibm、ieee
VLAN ステート	アクティブ	アクティブ、中断

表 14-6　トークンリング（TrBRF）VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1005	1 ～ 1005
VLAN 名	trnet-default	—
802.10 SAID	101005	1 ～ 4294967294
MTU サイズ	VTPv1 は 1500、VTPv2 は 4472	1500 ～ 18190
ブリッジ番号	1	0 ～ 15
STP タイプ	ibm	auto、ibm、ieee
VLAN ステート	アクティブ	アクティブ、中断

VLAN 設定時の注意事項および制約事項

ネットワークで VLAN を作成および変更する際、次の注意事項および制約事項に注意してください。

- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンを搭載したスイッチに、**vtp file** *file_name* コマンドを入力しないでください。
- 冗長スーパーバイザ エンジンを取り付ける前に、デフォルト設定に戻すには **no vtp file** コマンドを入力します。
- Route Processor Redundancy Plus（RPR+）冗長構成（第 8 章「Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定」を参照）は、VLAN データベース モードで入力された設定をサポートしていません。RPR+ 冗長構成には、グローバル コンフィギュレーション モードを使用します。
- 拡張範囲 VLAN を設定できるのは、グローバル コンフィギュレーション モードの場合だけです。VLAN データベース モードの場合は、拡張範囲 VLAN を設定できません。（「VLAN の設定方法」（P.14-10）を参照）。
- VLAN を作成する前に、Catalyst 6500 シリーズ スイッチを VTP サーバ モードまたは VTP 透過モードにする必要があります。VTP の設定手順については、第 13 章「VLAN トランキング プロトコル（VTP）の設定」を参照してください。
- VLAN の設定は vlan.dat ファイルに保存され、vlan.dat ファイルは不揮発性メモリに保存されます。vlan.dat ファイルを手動で削除すると、VLAN データベースに矛盾が生じる可能性があります。VLAN の設定または VTP の変更には、個々に記載されているコマンド、および『*Cisco IOS Master Command List*, Release 12.2SX』に記載されているコマンドを使用してください。
- 設定を完全にバックアップする場合は、vlan.dat ファイルをバックアップに追加します。
- VLAN データベース モードでは、Cisco IOS の **end** コマンドはサポートされません。
- **Ctrl+Z** を押しても、VLAN データベース モードを終了できません。
- Catalyst 6500 シリーズ 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 トラフィックを転送するのではなく、VTP を介して VLAN 設定を伝播できます。
- Catalyst 6500 シリーズ スイッチが VTP サーバとして設定されている場合は、スイッチから FDDI およびトークンリング VLAN を設定することができます。
- TrBRF を設定してから、TrCRF を設定する必要があります（指定する親 TrBRF VLAN がすでに存在していなければなりません）。
- トークンリング環境では、次のいずれかの条件が成立する場合、TrBRF の論理インターフェイス（TrBRF と TrCRF 間の接続）がブロック ステートになります。
  - TrBRF が IBM STP を実行していると同時に TrCRF が SRT モードにある。
  - TrBRF が IEEE STP を実行していると同時に TrCRF が SRB モードにある。

VLAN の設定

ここでは、VLAN の設定手順について説明します。

（注）　VLAN は、ここで紹介されている以外にも多くのパラメータをサポートしています。詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

VLAN の設定方法

ここでは VLAN の設定方法について説明します。

グローバル コンフィギュレーション モードでの VLAN の設定

スイッチが VTP サーバ モードまたは透過モードの場合は（「VTP の設定」（P.13-7）を参照）、グローバル コンフィギュレーション モードまたは config-vlan コンフィギュレーション モードで VLAN を設定できます。グローバル コンフィギュレーション モードおよび config-vlan コンフィギュレーション モードで VLAN を設定すると、VLAN の設定は vlan.dat ファイルに保存されます。VLAN の設定を表示するには、**show vlan** コマンドを入力します。

スイッチが VLAN 透過モードの場合、VLAN の設定は実行コンフィギュレーション ファイルに保存されます。copy **running-config startup-config** コマンドを使用して、VLAN の設定を startup-config ファイルに保存します。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として保存したあとに、**show running-config** および **show startup-config** コマンドを使用すると、VLAN の設定が表示されます。

（注）
- スイッチの起動時に、startup-config ファイルおよび vlan.dat ファイル内の VTP ドメイン名および VTP モードが異なる場合は、スイッチは vlan.dat ファイル内の設定を使用します。
- 拡張範囲 VLAN を設定できるのは、グローバル コンフィギュレーション モードの場合だけです。VLAN データベース モードの場合は、拡張範囲 VLAN を設定できません。

VLAN データベース モードでの VLAN の設定

（注）
- VLAN データベース モードは、Release 12.2(18)SXD よりも前のリリースでサポートされます。
- VLAN データベース モードの場合は、拡張範囲 VLAN を設定できません。拡張範囲 VLAN を設定できるのは、グローバル コンフィギュレーション モードの場合だけです。RPR+ 冗長構成は、VLAN データベース モードで入力された設定をサポートしていません。RPR+ 冗長構成には、グローバル コンフィギュレーション モードを使用します。

スイッチが VTP サーバ モードまたは透過モードの場合は、VLAN データベース モードで VLAN を設定できます。VLAN データベース モードで VLAN を設定すると、VLAN の設定は vlan.dat ファイルに保存されます。VLAN の設定を表示するには、**show vlan** コマンドを入力します。

ポート メンバシップ モードを定義したり、VLAN のポートを追加および削除するには、インターフェイス コンフィギュレーション コマンド モードを使用します。これらのコマンドの結果は、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** コマンドを使用します。

イーサネット VLAN の作成または変更

ユーザ定義 VLAN には、予約済み VLAN を除く 1 ～ 4094 の一意の ID があります（表 14-1（P.14-2）を参照）。VLAN を作成するには、**vlan** コマンドを入力して、未使用 ID を指定します。既存の VLAN を変更するには、その VLAN に対して **vlan** コマンドを入力します（レイヤ 3 ポートまたはソフトウェア機能が使用している既存 VLAN は変更できません）。

VLAN の作成時に割り当てられるデフォルト パラメータの一覧は、「VLAN のデフォルト設定」（P.14-6）を参照してください。**media** キーワードを使用して VLAN タイプを指定しない場合、VLAN はイーサネット VLAN になります。

VLAN を作成または変更するには、次の作業を行います。

	コマンド	目的

ステップ 1	`Router# configure terminal`
	または
	`Router# vlan database`
		VLAN コンフィギュレーション モードを開始します。

ステップ 2	`Router(config)# vlan` *vlan_ID*`{[-`*vlan_ID*`]|[,`*vlan_ID*`]}`
	`Router(config-vlan)#`
	または
	`Router(vlan)# vlan` *vlan_ID*
	`Router(config)# no vlan` *vlan_ID*
	`Router(config-vlan)#`
	または
	`Router(vlan)# no vlan` *vlan_ID*
		単独のイーサネット VLAN、イーサネット VLAN の範囲、またはカンマで区切った複数のイーサネット VLAN のリストを作成または変更します（スペースは挿入しないでください）。
		
		VLAN を削除します。

ステップ 3	`Router(config-vlan)# end`
	または
	`Router(vlan)# exit`
		VLAN データベースを更新して、イネーブル EXEC モードに戻ります。

ステップ 4	`Router# show vlan [id | name]` *vlan*	VLAN の設定を確認します。

イーサネット VLAN を作成または変更する場合は、次の情報に注意してください。

- RPR+ 冗長構成は、VLAN データベース モードで入力された設定をサポートしていません。RPR+ 冗長構成には、グローバル コンフィギュレーション モードを使用します。
- レイヤ 3 ポートおよび一部のソフトウェア機能を使用するには、1006 以降に割り当てられた内部 VLAN が必要であるため、4094 から始まる拡張範囲 VLAN を設定します。
- 拡張範囲 VLAN を設定できるのは、グローバル コンフィギュレーション モードの場合だけです。VLAN データベース モードの場合は、拡張範囲 VLAN を設定できません。
- レイヤ 3 ポートおよび一部のソフトウェア機能は、拡張範囲 VLAN を使用しています。作成または変更しようとしている VLAN がレイヤ 3 ポートまたはソフトウェア機能によって使用されている場合、スイッチはメッセージを表示し、VLAN 設定を変更しません。

VLAN を削除する場合は、次の情報に注意してください。

- 次の異なるメディア タイプのデフォルト VLAN は削除できません。イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005。
- VLAN を削除すると、その VLAN に割り当てられ、アクセス ポートとして設定されている LAN ポートは、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（非アクティブのまま）関連付けられています。

次に、グローバル コンフィギュレーション モードでイーサネット VLAN を作成し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
```

次に、VLAN データベース モードでイーサネット VLAN を作成する方法を示します。

```
Router# vlan database
Router(vlan)# vlan 3
VLAN 3 added:
    Name: VLAN0003
Router(vlan)# exit
APPLY completed.
Exiting....
```

次に、設定を確認する例を示します。

```
Router# show vlan name VLAN0003
VLAN Name                             Status    Ports
---- -------------------------------- --------- ---------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
Router#
```

VLAN へのレイヤ 2 LAN インターフェイスの割り当て

管理ドメイン内で作成された VLAN は、1 つまたは複数の LAN ポートを VLAN に割り当てない限り、未使用の状態です。

（注）　LAN ポートは必ず、適切なタイプの VLAN に割り当ててください。イーサネット ポートはイーサネットタイプの VLAN に割り当てます。

VLAN に 1 つまたは複数の LAN ポートを割り当てるには、「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.10-8）に記載されている手順を行います。

内部 VLAN 割り当てポリシーの設定

VLAN 割り当ての詳細については、「VLAN の範囲」（P.14-2）を参照してください。

（注）　内部 VLAN 割り当てポリシーは、リロードのあとにだけ適用されます。

内部 VLAN 割り当てポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan internal allocation policy {ascending | descending}`	内部 VLAN 割り当てポリシーを設定します。
	`Router(config)# no vlan internal allocation policy`	デフォルト値（昇順）に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# reload`	新しい内部 VLAN 割り当てポリシーを適用します。 **注意**　すぐに **reload** コマンドを入力する必要はありません。**reload** コマンドは、予定されているメンテナンス ウィンドウが表示されている間に入力します。

内部 VLAN 割り当てポリシーを設定する際、次の情報に注意してください。

- 1006 以降から内部 VLAN を割り当てるには、**ascending** キーワードを入力します。
- 4094 以下に内部 VLAN を割り当てるには、**descending** キーワードを入力します。

次に、内部 VLAN 割り当てポリシーとして、descending を設定する例を示します。

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

VLAN 変換の設定

トランク ポート上では、ある VLAN 番号を他の VLAN 番号に変換することができます。これにより、ある VLAN で受信されたすべてのトラフィックが他の VLAN に転送されます。

ここでは、VLAN 変換について説明します。

（注）
- Release12.2(17b)SXA 以降のリリースで、VLAN 変換がサポートされます。
- スパニング ツリー ループが生じないように、VLAN 変換機能を正しく設定するよう注意してください。

VLAN 変換に関する注意事項および制約事項

VLAN を変換する際に、以下の注意事項と制約事項に従ってください。

- レイヤ 2 トランクではないポートに適用される VLAN 変換は、非アクティブとなります。
- 802.1Q トランク上で、ネイティブ VLAN 入力トラフィックの変換を設定しないでください。802.1Q ネイティブ VLAN トラフィックはタグなしのため、変換の際に認識されません。他の VLAN から 802.1Q トランクのネイティブ VLAN に、トラフィックを変換することはできます。
- トランクの変換先の VLAN を削除しないでください。
- VLAN 変換の設定は、ポート グループ内のすべてのポートに適用されます。VLAN 変換は、ポート グループ内のすべてのポートで、デフォルトでディセーブルに設定されています。必要に応じて、ポートでの VLAN 変換をイネーブルにします。
- 次の表の内容は、次のとおりです。
  - VLAN 変換をサポートするモジュール
  - VLAN 変換の設定が適用されるポート グループ
  - ポート グループがサポートする VLAN 変換数
  - モジュールがサポートするトランク タイプ

（注）Optical Services Module（OSM; オプティカル サービス モジュール）上の LAN ポートは、VLAN 変換をサポートします。OSM 上の LAN ポートは、単一のポート グループにあります。

製品番号	ポート番号	ポートグループ番号	ポートグループ単位のポート範囲	ポートグループ単位の変換数	サポートされる VLAN 変換のトランクタイプ
WS-SUP720-3BXL WS-SUP720-3B WS-SUP720	2	1	1 ～ 2	32	802.1Q
WS-SUP32-10GE	3	2	1、2 ～ 3	16	ISL 802.1Q
WS-SUP32-GE	9	1	1 ～ 9	16	ISL 802.1Q
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2	2	1	1 ～ 2	32	802.1Q
WS-X6704-10GE	4	4	各グループで 1 つのポート	128	ISL 802.1Q
WS-X6502-10GE	1	1	各グループで 1 つのポート	32	802.1Q
WS-X6724-SFP	24	2	1 ～ 12 13 ～ 24	128	ISL 802.1Q
WS-X6816-GBIC	16	2	1 ～ 8 9 ～ 16	32	802.1Q
WS-X6516A-GBIC	16	2	1 ～ 8 9 ～ 16	32	802.1Q
WS-X6516-GBIC	16	2	1 ～ 8 9 ～ 16	32	802.1Q
WS-X6748-GE-TX	48	4	1 ～ 12 13 ～ 24 25 ～ 36 37 ～ 48	128	ISL 802.1Q
WS-X6516-GE-TX	16	2	1 ～ 8 9 ～ 16	32	802.1Q
WS-X6524-100FX-MM	24	1	1 ～ 24	32	ISL 802.1Q
WS-X6548-RJ-45	48	1	1 ～ 48	32	ISL 802.1Q
WS-X6548-RJ-21	48	1	1 ～ 48	32	ISL 802.1Q

（注）　ポートをトランクとして設定するには、「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-9）を参照してください。

トランク ポート上の VLAN 変換の設定

トランク ポート上で VLAN を変換するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するレイヤ 2 トランク ポートを選択します。
ステップ 2	`Router(config-if)# switchport vlan mapping enable`	VLAN 変換をイネーブルにします。
ステップ 3	`Router(config-if)# switchport vlan mapping original_vlan_ID translated_vlan_ID`	VLAN を他の VLAN に変換します。有効な範囲は、1 ～ 4094 です。 ポート上で元の VLAN から変換 VLAN への VLAN マッピングを設定する場合、元の VLAN に到着するトラフィックは、スイッチ ポートの入力で変換 VLAN にマッピングまたは変換されます。さらに、スイッチ ポートから送信される前に、変換 VLAN によって内部的にタグ付けされたトラフィックは、元の VLAN にマッピングされます。VLAN をマッピングするこの方法は双方向マッピングです。
	`Router(config-if)# no switchport vlan mapping {all | original_vlan_ID translated_vlan_ID}`	マッピングを削除します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show interface type[1] slot/port vlan mapping`	VLAN マッピングを確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ギガビット イーサネット ポート 5/2 で VLAN 1649 を VLAN 755 にマッピングする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping 1649 755
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show interface gigabitethernet 5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
------------- ---------------
  1649          755
```

ポート グループ内の他のポートでの VLAN 変換のイネーブル化

ポート グループ内の他のポートで、VLAN 変換をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport vlan mapping enable`	VLAN 変換をイネーブルにします。
	`Router(config-if)# no switchport vlan mapping enable`	VLAN 変換をディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show interface` *type*[1] *slot/port* `vlan mapping`	VLAN マッピングを確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポートで VLAN 変換をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping enable
Router(config-if)# end
Router#
```

802.1Q VLAN から ISL VLAN へのマッピング

ユーザ設定可能な ISL VLAN の有効範囲は、1 ～ 1001 と 1006 ～ 4094 です。IEEE 802.1Q 規格で規定されている VLAN の有効範囲は、1 ～ 4094 です。802.1Q VLAN 番号を ISL VLAN 番号にマッピングできます。

1 ～ 1001 および 1006 ～ 4094 の範囲の 802.1Q VLAN は、対応する ISL VLAN に自動的にマッピングされます。シスコ製のネットワーク装置によって認識および転送されるように、予約済み VLAN 番号に対応する 802.1Q VLAN 番号を ISL VLAN にマッピングしておく必要があります。

802.1Q VLAN を ISL VLAN にマッピングする際、次の制約事項があります。

- Catalyst 6500 シリーズ スイッチ上で、802.1Q から ISL VLAN へのマッピングを 8 つまで設定できます。
- 802.1Q VLAN は、イーサネット タイプの ISL VLAN にしかマッピングできません。
- 802.1Q トランクのネイティブ VLAN をマッピング テーブルに入れないでください。
- 802.1Q VLAN を ISL VLAN にマッピングすると、マッピングした ISL VLAN に対応する 802.1Q VLAN 上のトラフィックはブロックされます。たとえば、802.1Q VLAN 1007 を ISL VLAN 200 にマッピングした場合、802.1Q VLAN 200 上のトラフィックがブロックされます。
- VLAN マッピングは、各 Catalyst 6500 シリーズ スイッチでローカルに適用されます。該当するすべてのネットワーク装置には、必ず同じ VLAN マッピングを設定してください。

802.1Q VLAN を ISL VLAN にマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan mapping dot1q dot1q_vlan_ID isl isl_vlan_ID`	802.1Q VLAN を ISL イーサネット VLAN にマッピングします。*dot1q_vlan_ID* の有効範囲は 1001 ～ 4094 です。*isl_vlan_ID* の有効範囲も同じです。
	`Router(config)# no vlan mapping dot1q {all | dot1q_vlan_ID}`	マッピングを削除します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show vlan`	VLAN マッピングを確認します。

次に、802.1Q VLAN 1003 を ISL VLAN 200 にマッピングする例を示します。

```
Router# configure terminal
Router(config)# vlan mapping dot1q 1003 isl 200
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show vlan
<...output truncated...>
802.1Q Trunk Remapped VLANs:
802.1Q VLAN    ISL VLAN
-----------   -----------
   1003          200
```

VLAN 情報の保存

VLAN データベースは vlan.dat ファイルに保存されます。実行コンフィギュレーション ファイルと startup-config ファイルのバックアップに加えて、vlan.dat ファイルのバックアップを作成する必要があります。既存のスーパーバイザ エンジンを交換する場合、システムを復元するために、startup-config ファイルおよび vlan.dat ファイルをコピーします。vlan.dat ファイルはブートアップ時に読み込まれ、ファイルのアップロード後にスーパーバイザ エンジンをリロードする必要があります。ファイルの場所を表示するには、**dir vlan.dat** コマンドを使用します。（バイナリ）ファイルをコピーするには、**copy vlan.dat tftp** コマンドを使用します。

CHAPTER 15

プライベート VLAN の設定

この章では、Catalyst 6500 シリーズ スイッチにプライベート VLAN を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

プライベート VLAN の機能概要

ここでは、プライベート VLAN の機能について説明します。

プライベート VLAN ドメイン

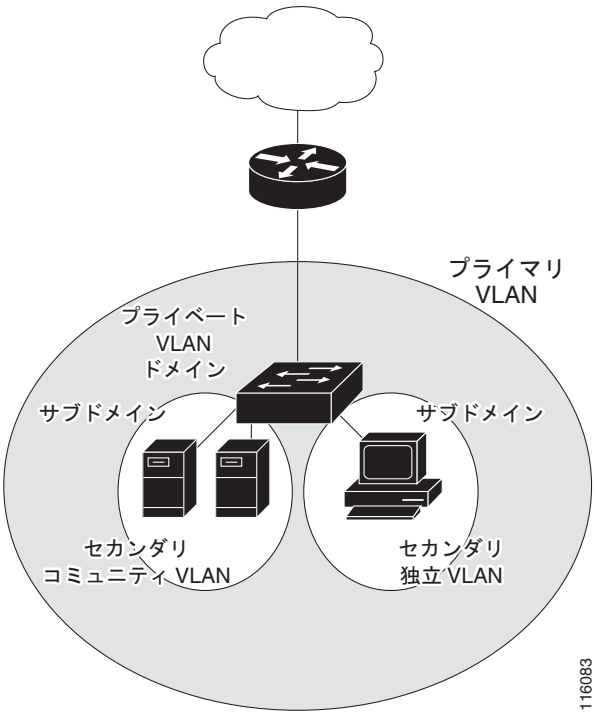
プライベート VLAN 機能では、サービス プロバイダー が VLAN を使用する際に直面する 2 つの問題を対処します。

- スイッチは、最大 4096 の VLAN をサポートします。サービス プロバイダーがカスタマーごとに 1 つの VLAN を割り当てる場合、サポートできるカスタマー数は制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てます。これにより未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が生じます。

プライベート VLAN を使用することにより、スケーラビリティの問題は解決され、サービス プロバイダーにとっては IP アドレスの管理が便利になり、カスタマーにはレイヤ 2 セキュリティが提供されます。

プライベート VLAN 機能により、VLAN のレイヤ 2 ブロードキャスト ドメインはサブドメインに分割されます。サブドメインは、プライマリ VLAN およびセカンダリ VLAN という 1 つの プライベート VLAN ペアです。プライベート VLAN ドメインには、複数のプライベート VLAN ペアが設定可能で、各サブドメインに 1 つのペアとなります。プライベート VLAN ドメイン内のすべての VLAN ペアは、同じプライマリ VLAN を共有します。セカンダリ VLAN ID では、あるサブドメインを他のサブドメインと区別します（図 15-1 を参照）。

図 15-1　　プライベート VLAN ドメイン



プライベート VLAN ドメインには、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN ドメイン内のすべてのポートは、プライマリ VLAN のメンバです。言い換えると、プライマリ VLAN はプライベート VLAN ドメイン全体となります。

セカンダリ VLAN は、同じ プライベート VLAN ドメイン内のポート間をレイヤ 2 で分離します。セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN - 独立 VLAN 内のポートは、レイヤ 2 レベルで相互に通信できません。
- コミュニティ VLAN - コミュニティ VLAN 内のポートは、相互に通信できますが、レイヤ 2 レベルの他のコミュニティ上のポートとは通信できません。

プライベート VLAN ポート

プライベート VLAN ポートには 3 つの種類があります。

- プロミスキャス - プロミスキャス ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられているセカンダリ VLAN に属するコミュニティ ホスト ポートおよび独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立 - 独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。このポートは、プロミスキャス ポート以外の、同じプライベート VLAN ドメイン内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、プロミスキャス ポートからのトラフィックを除き、独立ポート宛てのトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、プロミスキャス ポートにだけ転送されます。
- コミュニティ - コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN 内の他のポートおよびプロミスキャス ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN ドメイン内の独立ポートからレイヤ 2 で分離されています。

（注） トランクは独立ポート、コミュニティ ポート、およびプロミスキャス ポート間でトラフィックを伝達する VLAN をサポートできます。したがって、独立ポートおよびコミュニティ ポートのトラフィックはトランク インターフェイスを介してスイッチに送受信できます。

プライマリ、独立、およびコミュニティ VLAN

プライマリ VLAN および 2 種類のセカンダリ VLAN（独立 VLAN およびコミュニティ VLAN）には、次の特性があります。

- プライマリ VLAN - プライマリ VLAN は、単一方向のトラフィックのダウンストリームをプロミスキャス ポートから（独立およびコミュニティ）ホスト ポートおよび他のプロミスキャス ポートに伝送します。
- 独立 VLAN - プライベート VLAN ドメインの独立 VLAN は、1 つだけです。独立 VLAN は、単一方向のトラフィックのアップストリームをホストからプロミスキャス ポートおよびゲートウェイに伝送するセカンダリ VLAN です。
- コミュニティ VLAN - コミュニティ VLAN は、アップストリーム トラフィックをコミュニティ ポートからプロミスキャス ポート ゲートウェイおよび同じコミュニティ内の他のホスト ポートに伝送するセカンダリ VLAN です。1 つのプライベート VLAN ドメイン内に複数のコミュニティ VLAN を設定できます。

プロミスキャス ポートでは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけを処理できます。レイヤ 3 ゲートウェイは、通常プロミスキャス ポート経由でスイッチに接続されます。プロミスキャス ポートを使用すると、さまざまな装置を「アクセス ポイント」としてプライベート VLAN に接続できます。たとえば、プロミスキャス ポートを使用すると、管理ワークステーションからすべてのプライベート VLAN サーバをモニタ、またはバックアップできます。

スイッチング環境では、個々のエンド ステーションに、または共通グループのエンド ステーションに、個別のプライベート VLAN や、関連する IP サブネットを割り当てることができます。エンド ステーションが、プライベート VLAN の外部と通信するには、デフォルト ゲートウェイだけと通信する必要があります。

プライベート VLAN ポートの独立

プライベート VLAN を使用すると、エンド ステーションへのアクセスを次のように制御できます。

- エンド ステーションに接続された特定のインターフェイスを独立ポートとして設定すると、レイヤ 2 での通信が禁止されます。たとえば、エンド ステーションがサーバの場合は、サーバ間のレイヤ 2 通信が禁止されます。
- デフォルト ゲートウェイおよび選択されたエンド ステーション（たとえば、バックアップ サーバなど）に接続されたインターフェイスをプロミスキャス ポートとして設定すると、すべてのエンド ステーションがデフォルト ゲートウェイにアクセスできます。

複数の装置にわたるようにプライベート VLAN を拡張するには、プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN を、プライベート VLAN をサポートする他の装置にトランキングします。使用するプライベート VLAN の設定のセキュリティを確保して、プライベート VLAN として設定された VLAN が他の目的に使用されないようにするには、プライベート VLAN ポートがない装置を含めて、すべての中間装置でプライベート VLAN を設定します。

プライベート VLAN による IP アドレッシング方式

カスタマーごとに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

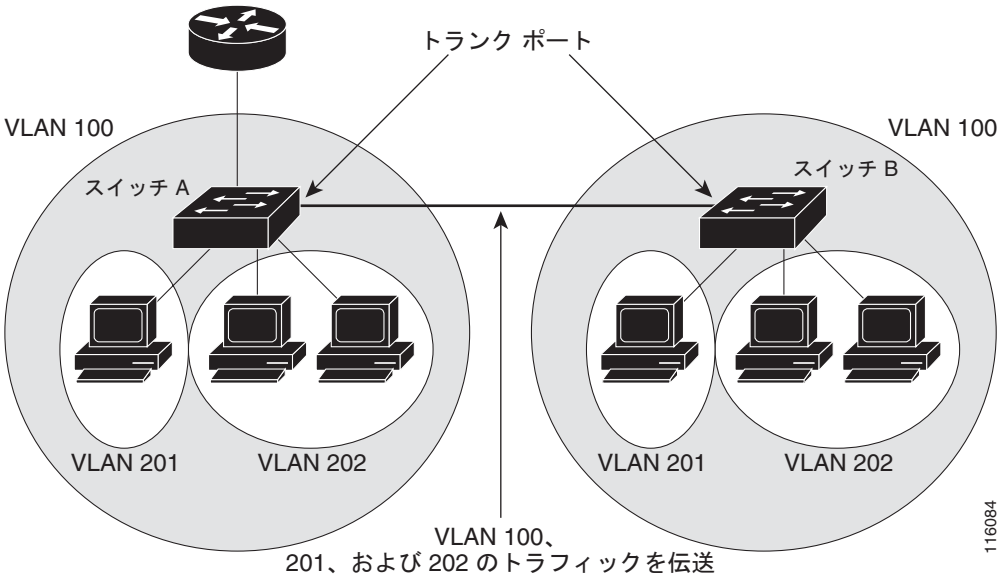
- カスタマー VLAN に アドレス ブロックを割り当てると、未使用の IP アドレスが生じます。
- VLAN 内の装置数が増加した場合、割り当てられるアドレス数はそれに対応できるほど多くはない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減されます。この場合、プライベート VLAN 内のすべてのメンバは、プライマリ VLAN に割り当てられる共通のアドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol（DHCP）サーバが プライマリ VLAN に割り当てられたアドレス ブロックから IP アドレスを割り当てます。同じプライマリ VLAN 内の別のセカンダリ VLAN 内のカスタマー装置に後続の IP アドレスを割り当てられます。新しい装置が追加された場合、DHCP サーバはサブネット アドレスの大きなプールから次に使用可能なアドレスを装置に割り当てます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を近接スイッチに伝送します。トランク ポートは、プライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能では、スイッチ A の独立ポートからのトラフィックは、スイッチ B の独立ポートに到達しません （図 15-2 を参照）。

図 15-2　スイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
VLAN 201 = セカンダリ独立 VLAN
VLAN 202 = セカンダリ コミュニティ VLAN

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、プライベート VLAN をサポートしないため、レイヤ 2 ネットワークのすべてのスイッチではプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリ VLAN とセカンダリ VLAN のアソシエーションを設定しない場合、これらのスイッチ内のレイヤ 2 データベースは結合されません。この状況により、これらのスイッチ上のプライベート VLAN トラフィックが不要にフラッディングする可能性があります。

プライベート VLAN の他の機能との相互作用

ここでは、プライベート VLAN の他の機能との相互作用について説明します。

- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」（P.15-6）
- 「プライベート VLAN およびスイッチ仮想インターフェイス（SVI）」（P.15-6）

「プライベート VLAN 設定時の注意事項および制約事項」（P.15-7）も参照してください。

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

通常の VLAN では、同じ VLAN 内の装置はレイヤ 2 レベルで相互に通信できますが、異なる VLAN のインターフェイスに接続されている装置とは、レイヤ 3 レベルで通信する必要があります。プライベート VLAN では、プロミスキャス ポートはプライマリ VLAN のメンバで、ホスト ポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に関連付けられているため、これらの VLAN のメンバはレイヤ 2 レベルで相互に通信できます。

通常の VLAN では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN のブロードキャスト転送は、ブロードキャストを送信するポートにより異なります。

- 独立ポートは、ブロードキャストをプロミスキャス ポートまたはトランク ポートにだけ送信します。
- コミュニティ ポートは、ブロードキャストをすべてのプロミスキャス ポート、トランク ポート、および同じコミュニティ VLAN 内のポートに送信します。
- プロミスキャス ポートは、ブロードキャストをプライベート VLAN 内のすべてのポート（他のプロミスキャス ポート、トランク ポート、独立ポート、およびコミュニティ ポート）に送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて、単一のコミュニティ VLAN 内でルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN 内のポート間または異なるセカンダリ VLAN 内のポート間で転送されません。

プライベート VLAN およびスイッチ仮想インターフェイス（SVI）

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）は、レイヤ 2 VLAN のレイヤ 3 インターフェイスです。レイヤ 3 装置は、セカンダリ VLAN ではなく、プライマリ VLAN を介してだけプライベート VLAN と通信します。プライマリ VLAN に対してだけ、レイヤ 3 VLAN SVI を設定します。セカンダリ VLAN 用にレイヤ 3 VLAN インターフェイスを設定しないでください。VLAN がセカンダリ VLAN として設定されている場合、セカンダリ VLAN の SVI は非アクティブです。

- アクティブな SVI が設定された VLAN をセカンダリ VLAN として設定しようとする場合、SVI をディセーブルにしなければ設定は許可されません。
- セカンダリ VLAN として設定されている VLAN 上に SVI を作成しようとした場合、セカンダリ VLAN がレイヤ 3 ですでにマッピングされていると、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 でマッピングされていない場合、SVI は作成されますが、自動的にシャット ダウンされます。

プライマリ VLAN がセカンダリ VLAN に関連付けられていて、マッピングされている場合、プライマリ VLAN 上のすべての設定はセカンダリ VLAN の SVI に伝播されます。たとえば、プライマリ VLAN の SVI に IP サブネットを割り当てる場合、このサブネットはプライベート VLAN 全体の IP サブネット アドレスとなります。

プライベート VLAN 設定時の注意事項および制約事項

プライベート VLAN の設定時の注意事項の内容は、次のとおりです。

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN を設定する場合、次の注意事項を考慮してください。

- プライベート VLAN を設定して、VTP を透過モードに設定したあとは、VTP モードをクライアントまたはサーバに変更できません。VTP の詳細については、第 13 章「VLAN トランキング プロトコル（VTP）の設定」を参照してください。
- プライベート VLAN を設定するには、VLAN コンフィギュレーション（config-vlan）モードを使用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 モードの場合は、プライベート VLAN を設定できません。VLAN 設定の詳細については、「VLAN の設定方法」（P.14-10）を参照してください。
- プライベート VLAN を設定後、**copy running-config startup config** イネーブル EXEC コマンドを使用して、VTP 透過モード設定およびプライベート VLAN 設定を startup-config ファイルに保存します。スイッチをリセットした場合は、プライベート VLAN をサポートするため、デフォルトの VTP 透過モードにする必要があります。
- VTP は、プライベート VLAN 設定を伝播しません。プライベート VLAN ポートを使用する装置ごとに、プライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ～ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN（VLAN ID 1006 ～ 4094）は、プライベート VLAN に属することができます。プライベート VLAN にできるのは、イーサネット VLAN に限られます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立またはコミュニティ VLAN には、1 つのプライマリ VLAN だけを関連付けることができます。
- セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）パラメータ（ブリッジ プライオリティなど）はセカンダリ VLAN に伝播されます。ただし、他の装置に STP パラメータを伝播する必要はありません。VLAN が同一の転送データベースを適切に共有できるように、プライマリ、独立、およびコミュニティ VLAN のスパニング ツリー トポロジの一致を確認するには、STP 設定を手動で検証する必要があります。
- スイッチの MAC アドレス リダクション機能をイネーブルにする場合は、プライベート VLAN の STP トポロジが一致するように、ネットワーク内のすべての装置の MAC アドレス リダクション機能をイネーブルにするよう推奨します。

- プライベート VLAN が設定されているネットワーク内で、一部の装置の MAC アドレス リダクション機能をイネーブルにし、他の装置でディセーブルにした場合は（混在環境）、プライマリ VLAN や、関連付けられたすべての独立 VLAN およびコミュニティ VLAN に対してルート ブリッジが共通となるように、デフォルトのブリッジ プライオリティを使用します。MAC アドレス リダクション機能がシステム上でイネーブルであるかどうかに関係なく、この機能の対象範囲に矛盾がないようにしてください。MAC アドレス リダクション機能では個々のレベルだけが許可されています。すべての中間値は、範囲として内部的に使用されます。プライベート VLAN および MAC アドレス リダクション機能を持つルート ブリッジをディセーブルにし、ルート ブリッジとする装置に、ルート ブリッジ以外で使用される最も高いプライオリティの範囲よりもさらに高いプライオリティを設定する必要があります。
- セカンダリ VLAN には VACL を適用できません（第 35 章「VLAN アクセス制御リスト（VACL）の設定」を参照）。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにする場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定する際、その設定がプライマリ VLAN ですでに設定されている場合有効になりません。
- プライベート VLAN でトラフィックを伝送しない装置のトランクから、プライベート VLAN をプルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service（QoS; サービス品質）を適用できます（第 41 章「PFC QoS の設定」を参照）。
- プライベート VLAN を設定する場合に、sticky Address Resolution Protocol（ARP; アドレス解決プロトコル）がデフォルトでイネーブルとなり、レイヤ 3 プライベート VLAN インターフェイスで学習される ARP エントリは、sticky ARP エントリになります。セキュリティ上の理由から、プライベート VLAN ポートの sticky ARP エントリには期限切れがありません。sticky ARP の設定については、「sticky ARP の設定」（P.36-37）を参照してください。
- プライベート VLAN インターフェイスの ARP エントリを表示して確認することを推奨します。
- sticky ARP は、ARP エントリ（IP アドレス、MAC アドレス、および送信元 VLAN）が期限切れしないようにすることにより、MAC アドレス スプーフィングを防ぎます。Release 12.2(18)SXF 以降のリリースでは、インターフェイス単位で sticky ARP を設定できます。sticky ARP の設定については、「sticky ARP の設定」（P.36-37）を参照してください。プライベート VLAN sticky ARP には、次の注意事項および制約事項が適用されます。
  - レイヤ 3 プライベート VLAN インターフェイスで学習される ARP エントリは、sticky ARP エントリです。
  - MAC アドレスは違っても、IP アドレスが同じ装置を接続すると、メッセージが表示され、ARP エントリは作成されません。
  - プライベート VLAN ポートの sticky ARP エントリには期限がないため、MAC アドレスが変更された場合は、プライベート VLAN ポートの ARP エントリを手動で削除する必要があります。プライベート VLAN の ARP エントリを手動で追加または削除する方法は、次のとおりです。

```
Router(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

Router(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

- プライマリ VLAN およびセカンダリ VLAN では VLAN マップを設定できます（「VLAN アクセス マップの適用」（P.35-9）を参照）。ただし、プライベート VLAN のプライマリ VLAN とセカンダリ VLAN には、同じ VLAN マップを設定することを推奨します。

- フレームがプライベート VLAN 内でレイヤ 2 転送される場合、入力側と出力側で同じ VLAN マップが適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップは入力側で適用されます。
  - ホスト ポートからプロミスキャス ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - プロミスキャス ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN で設定された VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、プライマリ VLAN とセカンダリ VLAN の両方に VLAN マップを適用する必要があります。
- 発信されるすべてのプライベート VLAN トラフィックに Cisco IOS 出力 Access Control List（ACL; アクセス制御リスト）を適用するには、プライマリ VLAN のレイヤ 3 VLAN インターフェイス上でこの ACL を設定します（第 33 章「ネットワーク セキュリティの設定」を参照）。
- プライマリ VLAN のレイヤ 3 VLAN インターフェイスに適用された Cisco IOS ACL は、関連する独立 VLAN およびコミュニティ VLAN にも自動的に適用されます。
- Cisco IOS ACL を独立 VLAN またはコミュニティ VLAN には適用しないでください。独立 VLAN およびコミュニティ VLAN に適用される Cisco IOS ACL の設定は、VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。
- プライベート VLAN がレイヤ 2 でホストを独立していても、ホストはレイヤ 3 で相互に通信できます。
- プライベート VLAN では、次の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能をサポートしています。
  - プライベート VLAN ポートを SPAN 送信元ポートとして設定できます。
  - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN 上で VLAN-based SPAN（VSPAN）を使用したり、単一の VLAN 上で SPAN を使用したりして、出力トラフィックまたは入力トラフィックを個別にモニタすることができます。
  - SPAN の詳細については、第 52 章「ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定」を参照してください。

プライベート VLAN ポートの設定

プライベート VLAN ポートを設定する場合、次の注意事項を考慮してください。

- ポートをプライマリ VLAN、独立 VLAN、またはコミュニティ VLAN に割り当てる場合は、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定する VLAN に割り当てられているレイヤ 2 アクセス ポートは、この VLAN がプライベート VLAN の設定に含まれている場合、非アクティブです。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- Port Aggregation Protocol（PAgP）または Link Aggregation Control Protocol（LACP）EtherChannel に属するポートを、プライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定は非アクティブです。

- 設定ミスによって STP ループが発生しないようにするため、および STP コンバージェンスを高速化するためには独立ホスト ポートおよびコミュニティ ホスト ポート上で PortFast および Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）ガードをイネーブルにします（第 21 章「オプションのスパニング ツリー プロトコル（STP）機能の設定」を参照）。STP をイネーブルに設定すると、STP によってすべての PortFast 設定済みレイヤ 2 LAN ポートに BPDU ガード機能が適用されます。プロミスキャス ポートでは、PortFast および BPDU をイネーブルにしないでください。
- プライベート VLAN の設定で使用される VLAN を削除すると、この VLAN に関連付けられたプライベート VLAN ポートが非アクティブになります。
- プライベート VLAN ポートは、ネットワーク装置をトランク接続し、トランクからプライマリ VLAN およびセカンダリ VLAN が削除されていない限りさまざまなネットワーク装置上で使用できます。
- プライベート VLAN 内で関連付けられているすべてのプライマリ、独立、およびコミュニティ VLAN は、トランク間で同じトポロジを維持する必要があります。同じトポロジを維持するためには、関連付けられた VLAN すべてで、同じ STP ブリッジ パラメータおよびトランク ポート パラメータを設定することを強く推奨します。

他の機能との制限事項

プライベート VLAN を設定する場合、次の他の機能との設定上の制限事項を考慮してください。

（注）　場合によっては、エラー メッセージなしで設定が受け入れられますが、コマンドは無効になります。

- プライベート VLAN が設定されたスイッチでは、代替ブリッジングを設定しないでください。
- ポートが現在プライベート VLAN モードで、そのプライベート VLAN 設定では、ポートがプライマリ、独立、またはコミュニティ ポートであると示されている場合、ポートはプライベート VLAN 機能によってだけ影響されます。ポートがそれ以外のモード（Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）など）の場合、プライベート ポートとして機能しません。
- 次のその他の機能が設定されているインターフェイスに、プライベート VLAN ポートを設定しないでください。
  - PAgP
  - LACP
  - 音声 VLAN
- プライベート VLAN ポートに IEEE 802.1x ポートベース認証を設定できますが、802.1x をポート セキュリティ、音声 VLAN、またはユーザ単位 ACL と一緒にプライベート VLAN ポートに設定しないでください。
- IEEE 802.1Q マッピングは、通常どおり動作します。トラフィックは設定のとおり dot1Q ポートとの間で、Inter-Switch Link（ISL; スイッチ間リンク）VLAN から受信したかのように、再マッピングされます。
- Release 12.2(18)SXE よりも前のリリースでは、プライベート VLAN 内のポートにポート セキュリティを設定できません。
- Remote SPAN（RSPAN）VLAN をプライベート VLAN のプライマリ VLAN またはセカンダリ VLAN として設定しないでください。SPAN の詳細については、第 52 章「ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定」を参照してください。

- プライベート VLAN ホストまたはプロミスキャス ポートは、SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートとして設定した場合、ポートは非アクティブとなります。
- 宛先 SPAN ポートを、独立ポートにしないでください（ただし、送信元 SPAN ポートは独立ポートにできます）。VSPAN は、プライマリ VLAN またはセカンダリ VLAN の両方にまたがるように設定できます。またはユーザが入力トラフィックか出力トラフィックにだけ関係する場合は、いずれか 1 つを補うように設定することもできます。
- Supervisor Engine 1 でプロトコル フィルタリングがイネーブルである場合、プライベート VLAN ポートの必要な Local Target Logic（LTL）バケットすべてを適切なセカンダリ VLAN インデックスを使用してプログラミングする必要があります。
- 異なる VLAN 間でショートカットを使用する場合（これらの VLAN のいずれかがプライベートである場合）、プライマリ VLAN と独立 VLAN、コミュニティ VLAN の両方を考慮してください。セカンダリ VLAN（実際の送信元）は常にレイヤ 2 FID テーブルのプライマリ VLAN に再マッピングされるため、プライマリ VLAN を宛先および仮想送信元の両方として使用する必要があります。
- プライマリ VLAN のプロミスキャス ポート上でスタティック MAC アドレスを設定する場合は、すべての関連するセカンダリ VLAN にこれと同じスタティック アドレスを追加する必要があります。セカンダリ VLAN のホスト ポート上でスタティック MAC アドレスを設定する場合は、関連するプライマリ VLAN にこれと同じスタティック MAC アドレスを追加する必要があります。プライベート VLAN ポートからスタティック MAC アドレスを削除した場合は、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。

  （注） プライベート VLAN の 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連する VLAN に複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。元のダイナミック MAC アドレスが削除されるか、期限切れになった場合は、複製されたアドレスは MAC アドレス テーブルから削除されます。

- プライベート VLAN ポートを EtherChannel として設定しないでください。ポートがプライベート VLAN の設定に含まれている間は、そのポートの EtherChannel 設定は非アクティブです。
- これらの制限事項は、12 ポートのグループをセカンダリ ポートとして設定する場合に適用されます。

  すべてのリリースで、「12 ポート制限」が次の 10 Mb、10/100 Mb、100 Mb イーサネット スイッチング モジュールに適用されます。WS-X6324-100FX、WS-X6348-RJ-45、WS-X6348-RJ-45V、WS-X6348-RJ-21V、WS-X6248-RJ-45、WS-X6248A-TEL、WS-X6248-TEL、WS-X6148-RJ-45、WS-X6148-RJ-45V、WS-X6148-45AF、WS-X6148-RJ-21、WS-X6148-RJ-21V、WS-X6148-21AF、WS-X6024-10FL-MT

  Release 12.2(17a)SX よりも前のリリースでは、「12 ポート制限」が次のイーサネット スイッチング モジュールに適用されます。WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6524-100FX-MM

  Release 12.2(17a)SX 以降のリリースでは、「12 ポート制限」が次のイーサネット スイッチング モジュールに適用されません。WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6524-100FX-MM（CSCea67876）

12 のポートからなるグループ（1 ～ 12、13 ～ 24、25 ～ 36、37 ～ 48）内のポートの 1 つが以下のいずれかである場合は、ポートを独立ポートまたはコミュニティ VLAN ポートとして設定しないでください。

- トランク ポート
- SPAN 宛先ポート
- プロミスキャス プライベート VLAN ポート
- CSCsb44185 が解決されているリリースの、**switchport mode dynamic auto** または **switchport mode dynamic desirable** コマンドで設定されているポート。

12 個のポートの 1 つが上記のいずれかの場合、および上記の特性がある場合、他の 11 個のポートの独立またはコミュニティ VLAN 設定は非アクティブです。これらのポートを再びアクティブにするには、独立 VLAN ポートまたはコミュニティ VLAN ポートの設定を削除して、**shutdown** および **no shutdown** コマンドを入力します。

- これらの制限事項は、24 ポートのグループをセカンダリ ポートとして設定する場合に適用されます。

  すべてのリリースで、「24 ポート制限」が WS-X6548-GE-TX および WS-X6148-GE-TX 10/100/1000 Mb イーサネット スイッチング モジュールに適用されます。

  24 のポートからなるグループ（1 ～ 24、25 ～ 48）内のポートの 1 つが以下のいずれかである場合は、ポートを独立ポートまたはコミュニティ VLAN ポートとして設定しないでください。

  - トランク ポート
  - SPAN 宛先ポート
  - プロミスキャス プライベート VLAN ポート
  - CSCsb44185 が解決されているリリースの、**switchport mode dynamic auto** または **switchport mode dynamic desirable** コマンドで設定されているポート。

  24 個のポートの 1 つが上記のいずれかの場合、および上記の特性がある場合、他の 23 個のポートの独立またはコミュニティ VLAN 設定は非アクティブです。これらのポートを再びアクティブにするには、独立 VLAN ポートまたはコミュニティ VLAN ポートの設定を削除して、**shutdown** および **no shutdown** コマンドを入力します。

プライベート VLAN の設定

ここでは、次の設定情報について説明します。

（注） VLAN がまだ定義されていない場合は、プライベート VLAN の設定プロセスを実行して、VLAN を定義します。

プライベート VLAN としての VLAN の設定

VLAN をプライベート VLAN として設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan vlan_ID`	VLAN コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-vlan)# private-vlan {community | isolated | primary}` `Router(config-vlan)# no private-vlan {community | isolated | primary}`	VLAN をプライベート VLAN として設定します。 プライベート VLAN の設定を消去します。 **（注）** これらのコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。
ステップ 3	`Router(config-vlan)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show vlan private-vlan [type]`	設定を確認します。

次に、VLAN 202 をプライマリ VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

次に、VLAN 303 をコミュニティ VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

次に、VLAN 440 を独立 VLAN として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan 440
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

セカンダリ VLAN とプライマリ VLAN の関連付け

セカンダリ VLAN をプライマリ VLAN に関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan primary_vlan_ID`	プライマリ VLAN の VLAN コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-vlan)# private-vlan association {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	セカンダリ VLAN をプライマリ VLAN に関連付けます。
	`Router(config-vlan)# no private-vlan association`	セカンダリ VLAN の関連付けをすべて消去します。
ステップ 3	`Router(config-vlan)# end`	VLAN コンフィギュレーション モードを終了します。
ステップ 4	`Router# show vlan private-vlan [type]`	設定を確認します。

セカンダリ VLAN をプライマリ VLAN と関連付ける際、次の情報に注意してください。

- *secondary_vlan_list* パラメータにはスペースを入れないでください。カンマで区切って複数の項目を入力できます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。
- *secondary_vlan_list* パラメータには、複数のコミュニティ VLAN ID を入れることができます。
- *secondary_vlan_list* パラメータには、1 つの独立 VLAN ID を入れることができます。
- セカンダリ VLAN をプライマリ VLAN に関連付けるには、*secondary_vlan_list* を入力するか、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN の関連付けを消去するには、*secondary_vlan_list* を指定して **remove** キーワードを使用します。
- これらのコマンドは、VLAN コンフィギュレーション サブモードを終了するまで有効になりません。

次に、コミュニティ VLAN 303 ～ 307、309、および独立 VLAN 440 をプライマリ VLAN 202 に関連付けて、設定を確認する方法を示します。

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan association 303-307,309,440
Router(config-vlan)# end
Router# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

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

（注）　独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan primary_vlan_ID`	プライマリ VLAN のインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# private-vlan mapping {secondary_vlan_list | add secondary_vlan_list | remove secondary_vlan_list}`	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングして、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
	`Router(config-if)# [no] private-vlan mapping`	セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show interface private-vlan mapping`	設定を確認します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際は、次の情報に注意してください。

- **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされるプライベート VLAN 入力トラフィックにだけ作用します。
- *secondary_vlan_list* パラメータにはスペースを入れないでください。カンマで区切って複数の項目を入力できます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。
- セカンダリ VLAN をプライマリ VLAN にマッピングするには、*secondary_vlan_list* パラメータを入力するか、または *secondary_vlan_list* を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライマリ VLAN の間のマッピングを消去するには、*secondary_vlan_list* パラメータを指定して **remove** キーワードを使用します。

次に、プライベート VLAN 303 ～ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可して、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Router#
```

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

レイヤ 2 インターフェイスをプライベート VLAN ホスト ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport**	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	Router(config-if)# **switchport mode private-vlan** {**host** | **promiscuous**} Router(config-if)# **no switchport mode private-vlan**	レイヤ 2 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。 プライベート VLAN ポートの設定を消去します。
ステップ 4	Router(config-if)# **switchport private-vlan host-association** *primary_vlan_ID secondary_vlan_ID* Router(config-if)# **no switchport private-vlan host-association**	レイヤ 2 ポートをプライベート VLAN と関連付けます。 関連付けを消去します。
ステップ 5	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 6	Router# **show interfaces** [*type*[1] *slot/port*] **switchport**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット インターフェイス 5/1 をプライベート VLAN ホスト ポートとして設定して、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport mode private-vlan host
Router(config-if)# switchport private-vlan host-association 202 303
Router(config-if)# end
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
➔ Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
➔ Administrative private-vlan host-association: 202 (VLAN0202) 303 (VLAN0303)
Administrative private-vlan mapping: none
➔ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

プライベート VLAN プロミスキャス ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN インターフェイスをレイヤ 2 スイッチング用に設定します。 • LAN インターフェイスをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	`Router(config-if)# switchport mode private-vlan {host | promiscuous}` `Router(config-if)# no switchport mode private-vlan`	レイヤ 2 ポートをプライベート VLAN プロミスキャス ポートとして設定します。 プライベート VLAN ポートの設定を消去します。
ステップ 4	`Router(config-if)# switchport private-vlan mapping` *primary_vlan_ID* {*secondary_vlan_list* | **add** *secondary_vlan_list* | **remove** *secondary_vlan_list*} `Router(config-if)# no switchport private-vlan mapping`	プライベート VLAN プロミスキャス ポートをプライマリ VLAN、および選択したセカンダリ VLAN にマッピングします。 プライベート VLAN プロミスキャス ポートと、プライマリ VLAN やセカンダリ VLAN の間のマッピングを消去します。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show interfaces` [*type*[1] *slot/port*] `switchport`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

レイヤ 2 インターフェイスをプライベート VLAN プロミスキャス ポートとして設定する際、次の情報に注意してください。

- *secondary_vlan_list* パラメータにはスペースを入れないでください。カンマで区切って複数の項目を入力できます。各項目として入力できるのは、単一のプライベート VLAN ID、またはハイフンで連結したプライベート VLAN ID の範囲です。
- セカンダリ VLAN をプライベート VLAN プロミスキャス ポートにマッピングするには、*secondary_vlan_list* の値を入力するか、または *secondary_vlan_list* の値を指定して **add** キーワードを使用します。
- セカンダリ VLAN とプライベート VLAN プロミスキャス ポートの間のマッピングを消去するには、*secondary_vlan_list* の値を指定して **remove** キーワードを使用します。

次に、ファスト イーサネット インターフェイス 5/2 をプライベート VLAN プロミスキャス ポートとして設定し、そのインターフェイスをプライベート VLAN にマッピングする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/2
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)# switchport private-vlan mapping 202 303,440
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none ((Inactive))
Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 440 (VLAN0440)
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

プライベート VLAN のモニタ

表 15-1 に、プライベート VLAN のアクティビティをモニタするためのイネーブル EXEC コマンドを示します。

表 15-1　プライベート VLAN のモニタ コマンド

コマンド	目的
show interfaces status	インターフェイス（それが属する VLAN を含む）のステータスを表示します。
show vlan private-vlan [type]	スイッチのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa2/0/1, Gi3/0/1, Gi3/0/2
10      502       community         Fa2/0/11, Gi3/0/1, Gi3/0/4
10      503       non-operational
```

CHAPTER 16

Cisco IP Phone サポートの設定

この章では、Catalyst 6500 シリーズ スイッチに Cisco IP Phone を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

Cisco IP Phone のサポートの概要

ここでは、Cisco IP Phone サポートについて説明します。

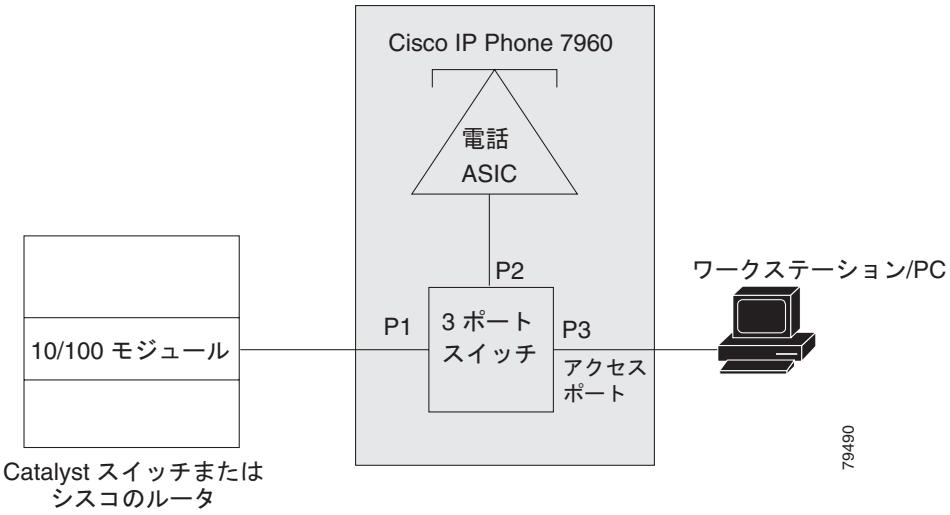
Cisco IP Phone の接続

Cisco IP Phone は、統合型 3 ポート内蔵 10/100 スイッチを装備しています。各ポートは、次の装置との接続専用です。

- ポート 1 は、スイッチに接続します。
- ポート 2 は、内蔵 10/100 インターフェイスで、Cisco IP Phone トラフィックを伝送します。
- ポート 3 は、PC またはその他の装置に接続します。

図 16-1 に、スイッチと PC の間に、Cisco IP Phone を接続する方法を示します。

図 16-1　　Cisco IP Phone とスイッチの接続



Cisco IP Phone の音声トラフィック

Cisco IP Phone は、音声トラフィックをレイヤ 3 の IP precedence 値とレイヤ 2 の Class of Service（CoS; サービス クラス）値と一緒に伝送します。この値は両方ともデフォルトで 5 に設定されています。Cisco IP Phone 通話の音質は、音声トラフィックが不均一に送信される場合、劣化する可能性があります。予測しやすい音声トラフィック フローを提供するために、音声トラフィックのレイヤ 3 IP precedence 値またはレイヤ 2 CoS 値を信頼するように Quality of Service（QoS; サービス品質）を設定できます（第 41 章「PFC QoS の設定」を参照）。

（注） WS-X6548-RJ-45 および WS-X6548-RJ-21 スイッチング モジュールのポートは、受信するレイヤ 2 CoS 値を信頼するように設定できます（QoS ポートアーキテクチャ 1p1q0t/1p3q1t）。WS-X6548-RJ-45 および WS-X6548-RJ-21 スイッチング モジュールは、Cisco IP Phone に電力を供給できません。レイヤ 3 IP precedence 値を使用する QoS ポリシーは、これ以外のスイッチング モジュール上で設定します。

接続された Cisco IP Phone のレイヤ 2 アクセス ポートについては、1 つの Virtual LAN（VLAN; 仮想 LAN）を音声トラフィック用、もう 1 つの VLAN は Cisco IP Phone に接続している装置からのデータ トラフィック用に使用するように設定できます。

スイッチのレイヤ 2 アクセス ポートが、Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）パケットを送信するように設定することができます。CDP は、接続する Cisco IP Phone が、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 プライオリティ値によるタグ付きの音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値によるタグ付きのアクセス VLAN による送信
- タグなしのアクセス VLAN（レイヤ 2 CoS プライオリティ値なし）による送信

（注）　すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値を伝送します（デフォルト値は音声トラフィックについては 5、音声制御トラフィックについては 3）。

Cisco IOS ソフトウェア コマンドを使用して、Cisco IP Phone 上のアクセス ポートに接続する装置から送信されるデータ トラフィックが使用するフレーム タイプを設定できません。

Cisco IP Phone のデータ トラフィック

（注）　Cisco IP Phone に接続されている装置からのタグなしトラフィックは、Cisco IP Phone のアクセス ポートの信頼状態にかかわらず、そのまま Cisco IP Phone を通過します。

Cisco IP Phone のアクセス ポートに接続されている装置（図 16-1 を参照）からのタグ付きデータ トラフィック（802.1Q または 802.1p フレーム タイプのトラフィック）を処理するには、スイッチのレイヤ 2 アクセス ポートに対して接続された Cisco IP Phone が、Cisco IP Phone のアクセス ポートに CDP パケットの送信を設定して、次のいずれかのモードを設定するように指定します。

- 信頼モード - Cisco IP Phone のアクセス ポートを介して受信したすべてのトラフィックは、そのまま Cisco IP Phone を通過します。
- 信頼できないモード - Cisco IP Phone のアクセス ポート経由で受信する 802.1Q または 802.1p フレームのすべてのトラフィックは、設定されたレイヤ 2 CoS 値でマーキングされます。デフォルトのレイヤ 2 CoS 値は 0 です。信頼できないモードがデフォルト設定です。

Cisco IP Phone の電源構成

ここでは、Cisco IP Phone 電源構成について説明します。

- 「Cisco IP Phone へのローカル電力供給」（P.16-3）
- 「Cisco IP Phone へのインライン パワー供給」（P.16-4）

Cisco IP Phone へのローカル電力供給

ローカル電源には 2 種類あります。

- Cisco IP Phone に接続されている電源装置
- Cisco IP Phone へ接続されているツイストペア イーサネット ケーブルを通じてパッチパネルを経由する電源装置

Cisco IP Phone が、スイッチング モジュールのポート上でローカルに電力が供給されていると、スイッチング モジュールはその存在を検出できません。スーパーバイザ エンジンは、Cisco IP Phone の CDP メッセージを通じて Cisco IP Phone を検出します。

ローカルに電力が供給されている Cisco IP Phone が、ローカル電力を失って、モードが **auto** に設定されている場合は、スイッチング モジュールが Cisco IP Phone を検出し、スーパーバイザ エンジンに通知して、Cisco IP Phone にインライン パワーを供給します。

Cisco IP Phone へのインライン パワー供給

インライン パワーは、インライン パワー ドータカードをサポートするスイッチング モジュールからの電源です。インライン パワーは、ツイストペア イーサネット ケーブルを通じて Cisco IP Phone に供給されます。

（注）　インライン パワーをサポートするスイッチング モジュールの詳細については、次の URL にある『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

スイッチング モジュール ポートは、電力が供給されていない Cisco IP Phone を検出すると、スーパーバイザ エンジンに、電力を供給されていない Cisco IP Phone の存在と、それがどのモジュール、ポートであるかを通知します。そのポートが **auto** モードに設定されている場合、スーパーバイザ エンジンは、Cisco IP Phone を動かすのに十分なシステム電力があるかどうかを判別します。十分な電力がある場合は、スーパーバイザ エンジンが、利用可能なシステム総電力量から、Cisco IP Phone が必要とするデフォルトの電力割り当て量を差し引き、電力をポートに供給するように指示するメッセージをスイッチング モジュールに対して送信します。Cisco IP Phone に供給する十分な電力がない場合、スーパーバイザ エンジンは、ポートへの電力供給が少ないことを示すメッセージをスイッチング モジュールに送信します。

Cisco IP Phone は、所要電力量が異なる場合があります。スーパーバイザ エンジンは最初に、デフォルトで設定されている 7 W（42 V で 167 mA）を、Cisco IP Phone に割り当てます。Cisco IP Phone との CDP メッセージ交換によって正確な電力量を判別すると、スーパーバイザ エンジンが割り当て電力を加減します。

たとえば、デフォルトの電力割り当て量は 7 W です。6.3 W を必要とする Cisco IP Phone をポートに接続します。スーパーバイザ エンジンは Cisco IP Phone に 7 W を割り当てたうえで電源をオンにします。Cisco IP Phone が動作を開始すると、CDP メッセージを通じて、実際の所要電力量をスーパーバイザ エンジンに通知します。スーパーバイザ エンジンは電力割り当て量を所要量まで減らします。

Cisco IP Phone の電源を Command-Line Interface（CLI; コマンドライン インターフェイス）または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を通じてオフにしたり、取り外したりする場合、スーパーバイザ エンジンはスイッチング モジュールに、ポートの電源をオフにするようにメッセージを送信します。その分の電力は利用可能なシステム総電源量に戻されます。

注意　Cisco IP Phone のケーブルをポートに接続し、電源をオンにすると、スーパーバイザ エンジンは回線上でリンクが起動するまで 4 秒間待機します。この 4 秒の間に、Cisco IP Phone のケーブルを取り外し、ネットワーク装置を接続すると、そのネットワーク装置が損傷することがあります。ネットワーク装置を取り外し、別のネットワーク装置を接続する場合は、10 秒以上待機してから行うようにしてください。

その他の Cisco IP Phone 機能

Catalyst 6500 シリーズ スイッチは、第 46 章「IEEE 802.1X ポートベースの認証の設定」に記述されているように、Cisco IP Phone の Authentication, Authorization, and Accounting （AAA）をサポートします。

Catalyst 6500 シリーズ スイッチも Cisco Emergency Responder（Cisco ER）の自動追跡をサポートし、電話ネットワークでの緊急コールの管理を支援します。詳細については、以下の URL を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

Cisco IP Phone サポートのデフォルト設定

Cisco IP Phone サポート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 機能がイネーブルに設定されている場合、タグなしのすべてのトラフィックは、ポートのデフォルトの CoS プライオリティで送信されます。

CoS は、802.1p または 802.1Q のタグ付きトラフィックについては信頼されていません。

Cisco IP Phone サポート設定時の注意事項および制約事項

Cisco IP Phone サポートを設定するとき、次の注意事項および制約事項が適用されます。

- 設定情報を Cisco IP Phone に送信するには、Cisco IP Phone に接続されている Catalyst 6500 シリーズ スイッチポートで Cisco 検出プロトコル（CDP）をイネーブルにしなければなりません。
- 音声 VLAN はレイヤ 2 LAN ポートにだけ設定できます。
- WS-X6548-RJ-45 および WS-X6548-RJ-21 スイッチング モジュールのポートは、受信するレイヤ 2 CoS 値を信頼するように設定できます（QoS ポートアーキテクチャ 1p1q0t/1p3q1t）。WS-X6548-RJ-45 および WS-X6548-RJ-21 スイッチング モジュールは、Cisco IP Phone に電力を供給できません。
- 10/100 Mbps ポートに QoS ポート アーキテクチャ 1p4t/2q2t を設定して、受信するレイヤ 2 CoS 値を信頼するようにすることはできません。スイッチングモジュールのレイヤ 3 IP precedence 値を QoS ポート アーキテクチャ 1p4t/2q2t で信頼するようにポリシーを設定します。
- 次に示す条件の場合、Cisco IP Phone および Cisco IP Phone に接続されている装置は同じ VLAN に存在し、必ず同じ IP サブネットに存在する必要があります。
  - 両方が 802.1p またはタグなしフレームを使用する場合
  - Cisco IP Phone が 802.1p フレームを使用し、装置はタグなしフレームを使用する場合
  - Cisco IP Phone がタグなしフレームを使用し、装置は 802.1p フレームを使用する場合
  - Cisco IP Phone は 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである場合
- Cisco IP Phone と Cisco IP Phone に接続されている装置は、同じ VLAN とサブネット内に存在していても異なるフレーム タイプを使用する場合、通信できません。同じサブネット内にある装置間のトラフィックがルーティングされないためです（フレーム タイプが違う場合ルーティングされません）。

- Cisco IOS ソフトウェア コマンドを使用して、Cisco IP Phone 上のアクセス ポートに接続されている装置から送信されるトラフィックが使用するフレームタイプを設定できません。
- 音声 VLAN が設定されているポートでポート セキュリティをイネーブルにし、Cisco IP Phone に接続されている PC がある場合、ポート上の最大許容セキュア アドレスを 3 つ以上に設定します。
- 音声 VLAN には、スタティック セキュア Media Access Control（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 に設定されているポートはセキュアポートにすることができます（第 47 章「ポート セキュリティの設定」を参照）。
- すべての設定において、音声トラフィックはレイヤ 3 IP precedence 値を伝送します（デフォルト値は音声トラフィックについては 5、音声制御トラフィックについては 3）。

Cisco IP Phone サポートの設定

ここでは、Cisco IP Phone サポートの設定方法について説明します。

- 「音声トラフィックのサポートの設定」（P.16-6）
- 「データ トラフィックのサポートの設定」（P.16-8）
- 「インライン パワー サポートの設定」（P.16-9）

（注）　音声 VLAN は、Catalyst ソフトウェア マニュアルでは *補助 VLAN* と呼ばれています。

音声トラフィックのサポートの設定

Cisco IP Phone が音声トラフィックを伝送する方法を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface fastethernet slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# switchport voice vlan {voice_vlan_ID | dot1p | none | untagged}`	Cisco IP Phone が音声トラフィックを伝送する方法を設定します。
	`Router(config-if)# no switchport voice vlan`	設定を消去します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show interfaces fastethernet slot/port switchport` `Router# show running-config interface fastethernet slot/port`	設定を確認します。

Cisco IP Phone が音声トラフィックを伝送する方法を設定する際、次の情報に注意してください。

- 音声 VLAN ID を入力して、CDP パケットを送信します。CDP パケットは、音声トラフィックを音声 VLAN ID およびレイヤ 2 CoS 値（デフォルトは 5）によるタグ付き 802.1Q フレームで伝送するように Cisco IP Phone を設定します。Valid VLAN IDs are from 1 to 4094. スイッチは 802.1Q 音声トラフィックをアクセス VLAN に送ります。
- **dot1p** キーワードを入力して、CDP パケットを送信します。CDP パケットは、音声トラフィックを VLAN ID 0 およびレイヤ 2 の CoS 値（デフォルトは、音声トラフィックの場合 5、音声制御トラフィックの場合 3）によるタグ付き 802.1p フレームで伝送するように Cisco IP Phone を設定します。スイッチは 802.1p 音声トラフィックをアクセス VLAN に送ります。
- **untagged** キーワードを入力して、Cisco IP Phone が、タグなし音声トラフィックを伝送するように設定する CDP パケットを送信します。スイッチはタグなし音声トラフィックをアクセス VLAN に入れます。
- **none** キーワードを入力して、Cisco IP Phone が独自の設定を使用し、タグなし音声トラフィックを伝送できるようにします。スイッチはタグなし音声トラフィックをアクセス VLAN に入れます。
- すべての設定において、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。
- QoS の設定方法の詳細については、第 41 章「PFC QoS の設定」を参照してください。
- ポートをレイヤ 2 アクセス ポートとして設定する方法、およびアクセス VLAN の設定方法の詳細については、「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」（P.10-16）を参照してください。

次に、ファスト イーサネット ポート 5/1 に対して、Cisco IP Phone が VLAN 101 を音声 VLAN として使用するように指示する CDP パケットを送信するように、設定する例を示します

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```

次に、ファスト イーサネット ポート 5/1 の設定を確認する例を示します。

```
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

データ トラフィックのサポートの設定

Cisco IP Phone がデータ トラフィックを伝送する方法を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface fastethernet slot/port`	設定するポートを選択します。
ステップ 2	`Router(config-if)# mls qos trust extend [cos cos_value]`	Cisco IP Phone がデータ トラフィックを伝送する方法を設定します。
	`Router(config-if)# no mls qos trust extend`	設定を消去します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show interfaces fastethernet slot/port switchport` `Router# show running-config interface fastethernet slot/port`	設定を確認します。

Cisco IP Phone がデータ トラフィックを伝送する方法を設定する際、次の情報に注意してください。

- CDP パケットを送信して、Cisco IP Phone 上のアクセス ポートと接続している装置から受信したタグ付きトラフィックを Cisco IP Phone が信頼するように設定するには、**cos** キーワードおよび CoS 値を入力しないでください。
- CDP パケットを送信して、Cisco IP Phone 上のアクセス ポートと接続している装置から受信したタグ付きトラフィックを Cisco IP Phone がマーキングするように設定するには、**cos** キーワードおよび CoS 値を入力してください（有効値は 0 ～ 7 です）。
- Cisco IOS ソフトウェア コマンドを使用しても、Cisco IP Phone 上のアクセス ポートに接続する装置から送信されるデータ トラフィックへのタグの有無を設定できません。

次に、ファスト イーサネット ポート 5/1 が CDP パケットを送信して、Cisco IP Phone にアクセス ポートを信頼できないポートとして設定すること、および CoS 3 を使用する Cisco IP Phone 上のアクセス ポートと接続している装置から受信したすべてのタグ付きトラフィックをマーキングすることを通知するように設定する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# mls qos trust extend cos 3
```

次に、ファスト イーサネット ポート 5/1 が CDP パケットを送信して、Cisco IP Phone にアクセス ポートを信頼できるポートとして設定することを通知するように設定する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# mls qos trust extend
```

次に、ファスト イーサネット ポート 5/1 の設定を確認する例を示します。

```
Router# show queueing interface fastethernet 5/1 | include Extend
  Extend trust state: trusted
```

インライン パワー サポートの設定

インライン パワー サポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface fastethernet** *slot/port*	設定するポートを選択します。
ステップ 2	Router(config-if)# **power inline** {**auto** | **never**}	インライン パワー サポートを設定します。
	Router(config-if)# **no power inline**	設定を消去します。
ステップ 3	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show power inline** [**fastethernet** *slot/port*]	設定を確認します。

インライン パワーを設定する際、次の情報に注意してください。

- Cisco IP Phone の自動検出を設定するには、**auto** キーワードを入力します。
- Cisco IP Phone の自動検出をディセーブルにするには、**never** キーワードを入力します。

次に、ファスト イーサネット ポート 5/1 のインライン パワーをディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline never
```

次に、ファスト イーサネット ポート 5/1 のインライン パワーをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline auto
```

次に、ファスト イーサネット ポート 5/1 のインライン パワー設定を確認する例を示します。

```
Router# show power inline fastethernet 5/1
Interface  Admin    Oper     Power        Device
                            (Watts)
---------- ----- ---------- ------- --------------------
Fa5/1      auto  on           6.3   cisco phone device
```

CHAPTER 17

IEEE 802.1Q トンネリングの設定

この章では、Catalyst 6500 シリーズ スイッチ上で IEEE 802.1Q トンネリングを設定する手順について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- The WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6148-GE-TX、および WS-X6148V-GE-TX スイッチング モジュールは IEEE 802.1Q トンネリングをサポートしません。

この章で説明する内容は、次のとおりです。

802.1Q トンネリングの機能概要

802.1Q トンネリングにより、サービス プロバイダーは、1 つの VLAN を使用して複数の VLAN を持つカスタマーをサポートすることができます。同時に、カスタマーの VLAN ID を保護したり、異なるカスタマー VLAN のトラフィックを分離しておくことができます。

802.1Q トンネリングをサポートするように設定されたポートは、トンネル ポートといいます。トンネリングを設定する場合は、トンネル ポートをトンネリング専用で、トンネル VLAN となる VLAN に割り当てます。カスタマー トラフィックを分離するには、カスタマーごとに個別のトンネル VLAN が 1 つ必要ですが、この 1 つのトンネル VLAN でカスタマーの VLAN をすべてサポートできます。

802.1Q トンネリングは、ポイントツーポイント トンネル設定に制限されません。トンネル VLAN 内の任意のトンネル ポートが、トンネルの入口および出口になります。802.1Q トンネルには、カスタマー スイッチに接続するのに必要な数のトンネル ポートがあります。

カスタマー スイッチはトランクに接続されていますが、802.1Q トンネリングを使用すると、サービス プロバイダー スイッチは 1 つのサービス プロバイダー VLAN のみを使用してすべてのカスタマー VLAN を伝送し、すべてのカスタマー VLAN を直接伝送することはありません。

802.1Q トンネリングを使用すると、タグ付きカスタマー トラフィックはカスタマー装置上の 802.1Q トランク ポートから発信し、トンネル ポートを経由してサービス プロバイダー エッジ スイッチに着信します。カスタマー装置上の 802.1Q トランク ポートとトンネル ポート間のリンクは、非対称リンクといいます。これは、一端が 802.1Q トランク ポートとして設定され、もう一端がトンネル ポートとして設定されているからです。カスタマーごとに一意のアクセス VLAN ID に、トンネル ポートを割り当てます。図 17-1（P.17-2）および図 17-2（P.17-2）を参照してください。

図 17-1　サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネル ポート

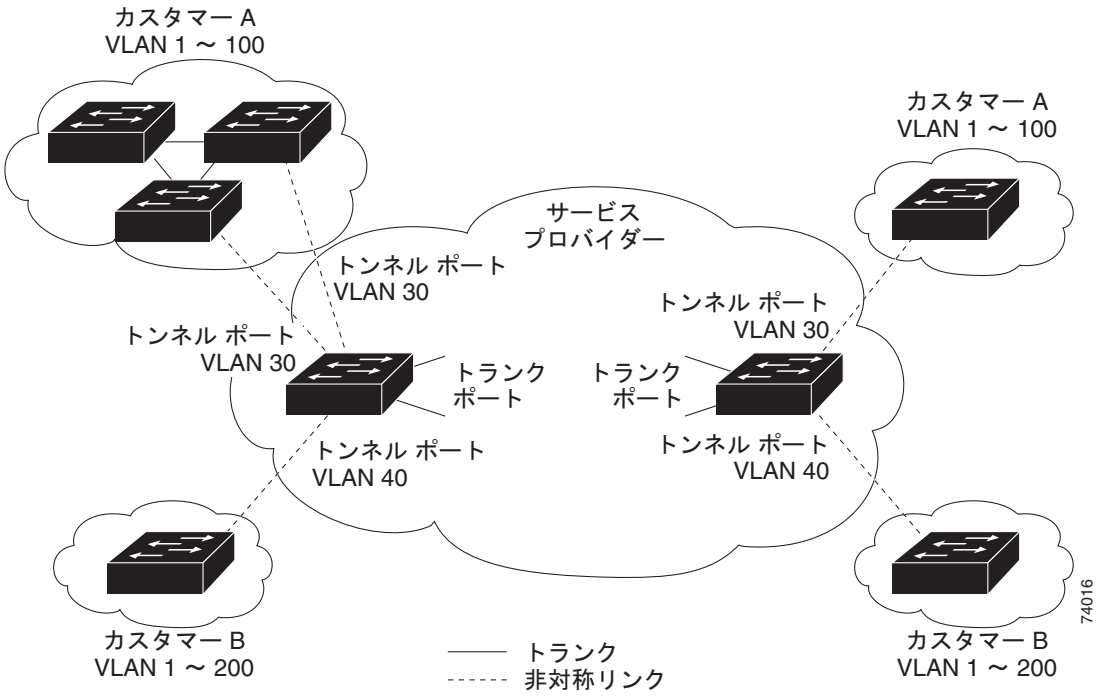
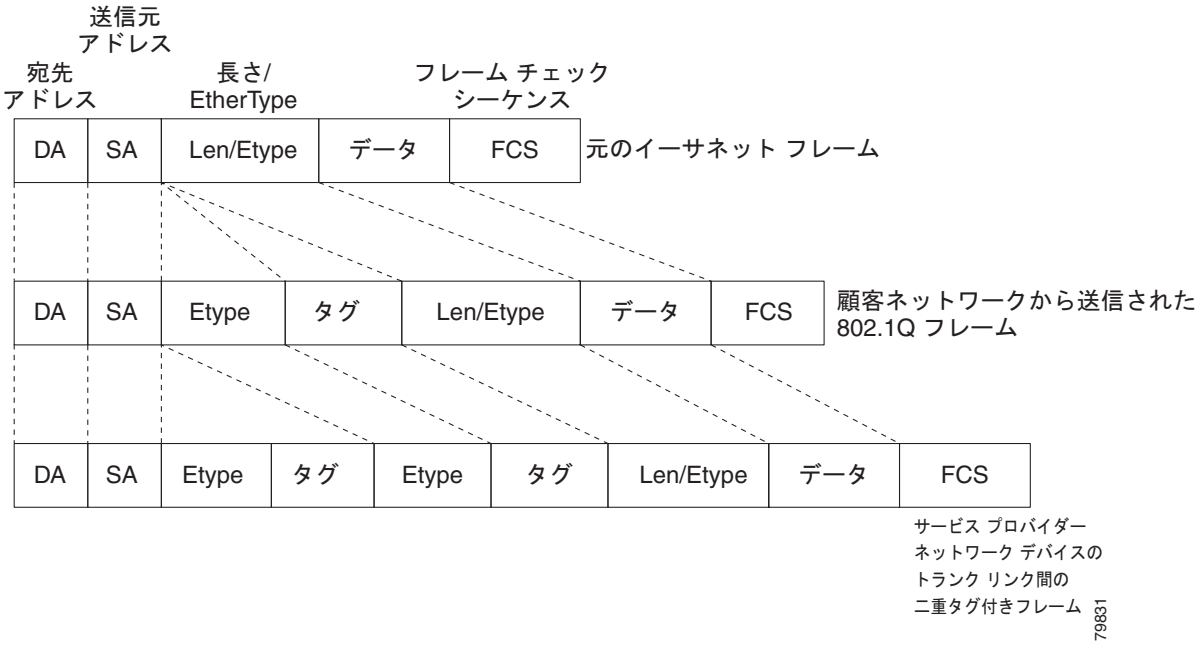


図 17-2　タグなし、802.1Q タグ付き、および、二重タグ付きイーサネット フレーム



802.1Q トランク ポートから送信されたタグ付きカスタマー トラフィックを受信したトンネル ポートは、受信した 802.1Q タグをフレーム ヘッダーから削除しません。802.1Q タグを変更しないでそのまま残し、2 バイトの Ethertype フィールド（0x8100）を追加し、そのあとにプライオリティ（Class of Service（CoS; サービス クラス））および VLAN を格納する 2 バイトのフィールドを追加します。受信したカスタマー トラフィックは、トンネル ポートが割り当てられた VLAN に送信されます。この Ethertype 0x8100 トラフィック（受信した 802.1Q タグが変更されないトラフィック）は、トンネル トラフィックと呼ばれます。

トンネル トラフィックを伝送する VLAN は 802.1Q トンネルです。VLAN 内のトンネル ポートが、トンネルの入口および出口になります。

トンネル ポートは異なるネットワーク装置上に設定することもできます。トンネルは他のネットワーク リンクおよび他のネットワーク装置を通過して、出口トンネル ポートに到着します。トンネルを介しての通信が必要なカスタマー装置に対応するために、トンネルにはトンネル ポートを必要なだけ設定することができます。

出口トンネル ポートは 2 バイトの Ethertype フィールド（0x8100）および 2 バイト長のフィールドを削除して、802.1Q タグを変更せずに、トラフィックをカスタマー装置上の 802.1Q トランク ポートに送信します。カスタマー装置上の 802.1Q トランク ポートは 802.1Q タグを削除して、トラフィックを適切なカスタマー VLAN に送ります。

（注）　トンネル トラフィックは、2 番目の 802.1Q タグがサービスプロバイダー ネットワーク装置間のトランク リンク上にある場合のみ、そのタグを伝送します。この場合、外部タグはサービスプロバイダーが割り当てた VLAN ID を含み、内部タグはカスタマーが割り当てた VLAN ID を含みます。

802.1Q トンネリングの設定時の注意事項および制約事項

802.1Q トンネリングの設定をネットワークに設定する場合、次の注意事項と制約事項に従ってください。

- トラフィックをトンネルに送ったり、トンネルからトラフィックを削除したりする場合は、非対称リンクを使用します。
- 非対称リンクだけを形成するようにトンネル ポートを設定します。
- トンネルごとに専用の VLAN を 1 つずつ設定します。
- トンネリングに使用する VLAN にはトンネル ポートだけを割り当てます。
- トンネル VLAN を伝送するようにトランクを特別に設定する必要はありません。
- トンネル ポートはトランクではありません。ポートがトンネル ポートとして設定されている間、トランキングを設定するコマンドは非アクティブになります。
- トンネル ポートは、カスタマー MAC（メディア アクセス制御）アドレスを学習します。
- トンネル ポートが設定されていない装置間でトンネル トラフィックを伝送する場合は、Inter-Switch Link（ISL; スイッチ間リンク）トランクを使用することを推奨します。802.1Q トランクには 802.1Q ネイティブ VLAN 機能が備わっているため、802.1Q トランクにトンネリングを設定する場合は注意してください。設定ミスによって、トンネル トラフィックが非トンネル ポートに送信されることがあります。

- デフォルトでは、dot1q トランクのネイティブ VLAN トラフィックはタグなしで送信され、サービス プロバイダー ネットワーク内で二重タグを付けることはできません。このため、ネイティブ VLAN トラフィックが正常にトンネリングされない場合があります。ネイティブ VLAN トラフィックは、必ず非対称リンクでタグ付きで送信するようにしてください。ネイティブ VLAN 出力トラフィックをタグ付きにして、タグなしの出力トラフィックはすべて廃棄するには、グローバルな **vlan dot1q tag native** コマンドを入力します。
- トンネル ポートにジャンボ フレームのサポートを設定します。
  - 「ジャンボ フレームのサポートの設定」（P.9-10）を参照してください。
  - 「ジャンボ フレームのサポートの設定」に記載されている、ジャンボ フレームをサポートしていないモジュールをメモしてください。
- ジャンボ フレーム長と 802.1Q タグの合計が最大フレーム サイズを超えない限り、ジャンボ フレームをトンネリングすることができます。
- トンネル トラフィックには Ethertype フィールドと Length フィールドがあり、スイッチ内に 802.1Q タグが保持されるため、次の制限が適用されます。
  - レイヤ 2 フレームに格納されたレイヤ 3 パケットは、トンネル トラフィックでは識別できません。
  - レイヤ 3 以上のパラメータは、トンネル トラフィックでは識別できません（レイヤ 3 宛先や送信元アドレスなど）。
  - パケット内ではレイヤ 3 アドレスを識別できないため、トンネル トラフィックはルーティングできません。
  - スイッチは、トンネル トラフィックに対して MAC レイヤ フィルタリングだけを提供できます（VLAN ID、および送信元や宛先の MAC アドレス）。
  - スイッチはトンネル トラフィックに対して MAC レイヤ アクセス制御および Quality of Service（QoS; サービス品質）だけを提供できます。
  - QoS は、802.1Q の 2 バイトの Tag Control Information フィールドに格納されて受信された CoS 値を検出できません。
- 非対称リンク上で、トンネル ポートの VLAN が 802.1Q トランクのネイティブ VLAN と一致しない場合、Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）はネイティブ VLAN の不一致をレポートします。802.1Q トンネル機能を使用する場合、VLAN が一致する必要はありません。VLAN の不一致を前提とする設定の場合は、メッセージを無視してください。
- 非対称リンクでは 1 つのポートだけがトランクになるため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランク ポートを設定します。
- 802.1Q トンネリング機能は、プライベート VLAN をサポートするように設定されたポートには設定できません。
- 次のレイヤ 2 プロトコルは、非対称リンクで接続された装置間で機能します。
  - CDP
  - UniDirectional Link Detection（UDLD; 単一方向リンク検出）
  - PAgP
  - LACP
- PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。
- CDP は、トンネル ポートで自動的にディセーブルになります。

- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、次の装置間で機能しません。
  - 非対称リンクで接続された装置
  - トンネルを介して通信する装置

（注）　レイヤ 2 プロトコル トンネリングがイネーブルの場合、VTP はトンネル化された装置間で機能します。設定の詳細については、第 18 章「レイヤ 2 プロトコル トンネリングの設定」を参照してください。

- EtherChannel を非対称リンクとして設定するには、EtherChannel 内のすべてのポートを同じトンネリング設定にする必要があります。レイヤ 2 フレーム内のレイヤ 3 パケットは識別できないため、MAC アドレスベースのフレーム配信を行うように、EtherChannel を設定する必要があります。

レイヤ 2 プロトコル トンネリングを設定する場合は、次に示す設定時の注意事項に*必ず*従ってください。

- サービス プロバイダーのすべてのエッジ スイッチでは、次のように、802.1Q トンネル ポート上で PortFast BPDU フィルタリングをイネーブルにする必要があります。

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

（注）　PortFast BPDU フィルタリングは、トンネル ポートで自動的にイネーブルになります。

- ネイティブ VLAN タギングに対して、1 つまたは複数の VLAN を使用可能にする必要があります（**vlan dot1q tag native** オプション）。使用可能なすべての VLAN を使用している場合に、**vlan dot1q tag native** オプションをイネーブルにしようとしても、イネーブルになりません。
- サービス プロバイダーのすべてのコア スイッチで、ネイティブ VLAN 出力トラフィックにタグを付け、タグなしネイティブ VLAN 入力トラフィックを廃棄するには、次のコマンドを入力します。

```
Router(config)# vlan dot1q tag native
```

- すべてのカスタマー スイッチで、**vlan dot1q tag native** オプションをグローバルなイネーブルまたはディセーブルの*いずれか一方*にします。

（注）　このオプションがイネーブルになっているスイッチとディセーブルになっているスイッチが混在している場合は、すべてのトラフィックが廃棄されます。したがって、すべてのカスタマー スイッチでこのオプションを各スイッチと同じに設定する必要があります。

レイヤ 2 プロトコル トンネリングを設定する場合は、*必要に応じて*、次に示す設定時の注意事項に従ってください。

- すべての BPDU が廃棄されているため、次のように、レイヤ 2 プロトコル トンネル ポート上でスパニング ツリー PortFast をイネーブルにすることができます。

```
Router(config-if)# spanning-tree portfast trunk
```

- カスタマーがサービス プロバイダー側のスイッチを認識できないようにするには、次のように 802.1Q トンネル ポート上で CDP をディセーブルにする必要があります。

```
Router(config-if)# no cdp enable
```

802.1Q トンネリングの設定

ここでは、802.1Q トンネリングの設定について説明します。

注意　トンネリングに使用するすべての VLAN 内に適切なトンネル ポートだけがあり、トンネルごとに VLAN が 1 つずつ使用されていることを確認します。VLAN へのトンネル ポートの割り当てが誤っていると、トラフィックが正しく転送されません。

802.1Q トンネル ポートの設定

特定のポート上で 802.1Q トンネリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	`Router(config-if)# switchport mode dot1q-tunnel` `Router(config-if)# no switchport mode dot1q-tunnel`	レイヤ 2 ポートをトンネル ポートとして設定します。 トンネル ポートの設定を消去します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show dot1q-tunnel [{interface` *type interface-number*`}]`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート 4/1 にトンネリングを設定して、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
Router# show dot1q-tunnel interface
```

ネイティブ VLAN トラフィックにタグを付けるためのスイッチの設定

vlan dot1q tag native コマンドは、ネイティブ VLAN トラフィックにタグを付けて、802.1Q トランク上で 802.1Q タグ付きフレームのみを許可するようにスイッチを設定するグローバル コマンドです。ネイティブ VLAN 内のタグなしトラフィックを含めて、タグなしフレームはすべて廃棄されます。

ネイティブ VLAN 内のトラフィックにタグを付けるようにスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# vlan dot1q tag native`	ネイティブ VLAN トラフィックにタグを付けるようにスイッチを設定します。
	`Router(config)# no vlan dot1q tag native`	設定を消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show vlan dot1q tag native`	設定を確認します。

次に、ネイティブ VLAN トラフィックにタグを付けるようにスイッチを設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# vlan dot1q tag native
Router(config)# end
Router# show vlan dot1q tag native
```

CHAPTER 18

レイヤ 2 プロトコル トンネリングの設定

この章では、Catalyst 6500 シリーズ スイッチにレイヤ 2 プロトコル トンネリングを設定する手順について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6148-GE-TX、WS-X6148V-GE-TX スイッチング モジュールでは、レイヤ 2 プロトコル トンネリングをサポートしません。

この章で説明する内容は、次のとおりです。

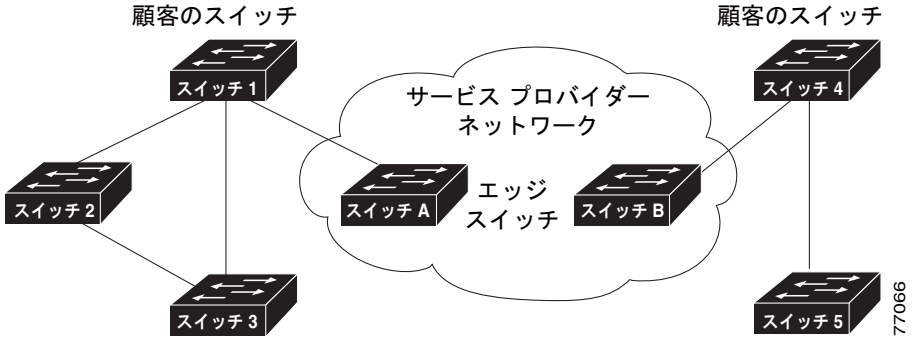
レイヤ 2 プロトコル トンネリングの機能概要

レイヤ 2 プロトコル トンネリングを使用すると、ネットワークを介してレイヤ 2 Protocol Data Unit（PDU; プロトコル データ ユニット）（Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、および VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル））をトンネリングできます。ここでは、次の用語を使用します。

- エッジ スイッチ - カスタマー スイッチに接続され、サービス プロバイダー ネットワークの境界に配置されたスイッチ（図 18-1 を参照）。
- レイヤ 2 プロトコル トンネル ポート - 特定のトンネル化プロトコルをカプセル化したり、カプセル化を解除することができるエッジ スイッチのポート。レイヤ 2 プロトコル トンネル ポートは Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドを使用して設定します。
- トンネル化 PDU - CDP、STP、または VTP PDU

レイヤ 2 プロトコル トンネリングがない場合、トンネル ポートは STP と VTP パケットを廃棄し、CDP パケットを処理します。この PDU の処理方法に応じて、カスタマーのスイッチに異なるスパニング ツリー ドメイン（異なるスパニング ツリー ルート）が作成されます。たとえば、スイッチ 1 の VLAN 用 STP（図 18-1 を参照）は、スイッチ 4 およびスイッチ 5 に基づくコンバージェンス パラメータを考慮しないで、スイッチ 1、2、3 のスパニング ツリー トポロジ を構築します。カスタマーに単一のスパニング ツリー ドメインを提供するために、制御プロトコル PDU（CDP、STP、および VTP）に対して、BPDU をトンネル化する一般的な方式が作成されています。このプロセスは、Generic Bridge PDU Tunneling（GBPT）といいます。

図 18-1　　レイヤ 2 プロトコル トンネリング ネットワークの設定



GBPT は、入力エッジ スイッチ内で PDU をソフトウェアでカプセル化してから、ハードウェアでマルチキャストすることにより PDU トンネリングを拡張する方式です。サービス プロバイダー ネットワーク内のすべてのスイッチは、カプセル化されたこれらのフレームをデータ パケットとして処理し、もう一方の端に転送します。出力エッジ スイッチはカプセル化されたこれらの特殊フレームを待ち受けて、カプセル化を解除し、これらをトンネルの外へ転送します。

カプセル化では、PDU 内の宛先 MAC（メディア アクセス制御）アドレスも書き換えられます。入力エッジ スイッチは、レイヤ 2 トンネル ポート上で受信された PDU の宛先 MAC アドレスを、シスコシステムズ独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）で書き換えます。次に、PDU はレイヤ 2 トンネル ポートのネイティブ VLAN（仮想 LAN）にフラッディングされます。ポート上でレイヤ 2 プロトコル トンネリングをイネーブルにした場合、イネーブル化されたプロトコルの PDU は送信されません。ポート上でレイヤ 2 プロトコル トンネリングをディセーブルにした場合、ディセーブル化されたプロトコルは、そのポート上でレイヤ 2 プロトコル トンネリングがディセーブルになる前と同じように動作します。

レイヤ 2 プロトコル トンネリングのサポートの設定

（注）
- 802.1Q トンネル ポートで受信されたカプセル化 PDU は、スイッチ上の同じ VLAN にある別のトンネル ポートから伝送されます。
- レイヤ 2 トンネリング ポートにジャンボ フレームのサポートを設定します。
  - 「ジャンボ フレームのサポートの設定」（P.9-10）を参照してください。
  - 「ジャンボ フレームのサポートの設定」に記載されている、ジャンボ フレームをサポートしていないモジュールをメモしてください。

特定のポート上でレイヤ 2 プロトコル トンネリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します。 • LAN ポートをレイヤ 2 インターフェイスとして設定するには、キーワードを指定せずに **switchport** コマンドを 1 度入力する必要があります。そのあとで、キーワードとともにさらに **switchport** コマンドを入力してください。 • インターフェイスに対して **switchport** コマンドを一度も入力していない場合に限り、必須です。
ステップ 3	`Router(config-if)# l2protocol-tunnel [cdp|drop-threshold [`*packets*`]|shutdown-threshold [`*packets*`]|stp|vtp]` `Router(config-if)# no l2protocol-tunnel [cdp|drop-threshold|shutdown-threshold|stp|vtp]`	レイヤ 2 ポートを、指定されたプロトコルのレイヤ 2 プロトコル トンネル ポートとして設定します。 設定を消去します。
ステップ 4	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show l2protocol-tunnel [interface` *type*[1] *slot/port*`|summary]`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

レイヤ 2 ポートをレイヤ 2 プロトコル トンネル ポートとして設定する際、次の情報に注意してください。

- 任意で、ポートに drop-threshold を指定することもできます。1 ～ 4096 の drop-threshold 値は、特定のインターフェイス上で、特定のプロトコルに対し、1 秒間に処理されるパケット数を決定します。処理パケット数が drop-threshold 値を超えると、その特定のプロトコルの PDU は、1 秒間の残りの時間に廃棄されます。shutdown-threshold 値を指定しない場合、値は 0 です（shutdown-threshold はディセーブルです）。
- 任意で、ポートに shutdown-threshold を指定することもできます。1 ～ 4096 の shutdown-threshold 値は、特定のインターフェイス上で、特定のプロトコルに対し、1 秒間に処理されるパケット数を決定します。処理パケット数が shutdown-threshold 値を超えると、ポートは errdisable ステートになります。shutdown-threshold 値を指定しない場合、値は 0 です（shutdown-threshold はディセーブルです）。

（注）　次のコマンドの **l2ptguard** キーワードの詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

- **errdisable detect cause**
- **errdisable recovery cause**

次に、CDP、STP、および VTP に対して、ポート 5/1 にレイヤ 2 プロトコル トンネリングおよび shutdown-threshold を設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# end
Router# show l2protocol-tunnel summary
Port    Protocol        Threshold
                        (cos/cdp/stp/vtp)
----------------------------------------
Fa5/1   cdp stp vtp     0/10  /10  /10          down trunk
Router#
```

次に、ポート 5/1 のカウンタ情報を表示する例を示します。

```
Router# show l2protocol-tunnel interface fastethernet 5/1
Port    Protocol        Threshold           Counters
                        (cos/cdp/stp/vtp)   (cdp/stp/vtp/decap)
------------------------------------------------------------------
Router#
```

次に、ポート 5/1 のレイヤ 2 プロトコル トンネリング設定を消去する例を示します。

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# no l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# no l2protocol-tunnel cdp
Router(config-if)# no l2protocol-tunnel stp
Router(config-if)# no l2protocol-tunnel vtp
Router(config-if)# end
Router# show l2protocol-tunnel summary
Port    Protocol        Threshold
                        (cos/cdp/stp/vtp)
----------------------------------------
Router#
```

次に、レイヤ 2 プロトコル トンネリング ポートのカウンタを消去する例を示します。

```
Router# clear l2protocol-tunnel counters
Router#
```

CHAPTER 19

標準準拠 IEEE Multiple Spanning Tree（MST）の設定

この章では、Catalyst 6500 シリーズ スイッチに標準準拠 IEEE Multiple Spanning Tree（MST）プロトコルを設定する方法について説明します。

（注）

- IEEE MST プロトコルは、先行標準状態からリリース状態に移行しました。この章では、Release 12.2(18)SXF 以降のリリースでサポートされる標準準拠 MST 実装について説明しています。第 20 章「スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定」では、Release 12.2(18)SXF よりも前のリリースでサポートされていた先行標準 MST 実装について説明しています。
- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

MST の概要

ここでは MST について説明します。

MST の概要

MST は、複数の Virtual LAN（VLAN; 仮想 LAN）をスパニング ツリー インスタンスにマッピングします。各インスタンスには他のスパニング ツリー インスタンスとは別のスパニング ツリー トポロジがあります。このアーキテクチャにより、データ トラフィック用に複数の転送パスが提供され、ロード バランシングが使用可能になり、多くの VLAN をサポートするために必要なスパニング ツリー インスタンスの数が減少します。MST では、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）には影響しないため、ネットワークのフォールトトレランスが改善されます。

MST の最も一般的な初期配置は、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 レイヤへの配置です。この配置により、サービスプロバイダー環境で必要な一種の高可用性ネットワークを提供することになります。

MST は、明示的なハンドシェイクを通じてラピッド スパニング ツリー コンバージェンスを提供しています。これにより 802.1D 転送遅延を解消して、迅速にルート ブリッジ ポートと指定ポートをフォワーディング ステートに移行させることができます。

MST は、スパニング ツリー動作を改善し、以下の Spanning Tree Protocol（STP スパニング ツリー プロトコル）バージョンと後方互換性を維持しています。

- オリジナルの 802.1D スパニング ツリー
- 既存のシスコ独自 Multiple Instance STP（MISTP）
- 既存の Cisco Per-VLAN Spanning Tree Plus（PVST+）
- Rapid Per-VLAN Spanning Tree Plus（Rapid PVST+）

PVST+ および Rapid PVST+機能の詳細については、第 20 章「スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定」を参照してください。Port Fast、UplinkFast、ルートガードなどの他のスパニング ツリー機能の詳細については、第 21 章「オプションのスパニング ツリー プロトコル（STP）機能の設定」を参照してください。

（注）

- IEEE 802.1w は、Rapid SpanningTree Protocol（RSTP; 高速スパニング ツリー プロトコル）を定義しており、IEEE802.1D に組み込まれました。
- IEEE 802.1s は MST を定義しており、IEEE 802.1Q に組み込まれました。

MST 領域

MST インスタンスに参加するスイッチに対して、常に同じ MST コンフィギュレーション情報を使用してスイッチを設定する必要があります。同じ MST コンフィギュレーションを持つ相互接続されたスイッチの集合体が MST 領域を構成します（図 19-1（P.19-5）を参照）。

MST コンフィギュレーションは、各スイッチが属する MST 領域を制御します。このコンフィギュレーションには、領域名、リビジョン番号、MST VLAN とインスタンスの割り当てマップが含まれています。

1 つの領域に同じ 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を持つことができ、各メンバには RSTP Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を処理する能力がなければなりません。ネットワーク内の MST 領域数には制限がありませんが、各領域は最大で 65 のスパニング ツリー インスタンスをサポートできます。インスタンスは、0 ～ 4094 の領域の任意の番号で識別されます。1 つの VLAN を同時に割り当てることのできるスパニング ツリー インスタンスは 1 つだけです。

内部スパニング ツリー（IST）、Common and Internal Spanning-Tree（CIST）、および共通スパニング ツリー（CST）

これらのセクションでは、Internal Spanning Tree（IST; 内部スパニング ツリー）、Common and Internal Spanning-Tree（CIST）、および Common Spanning Tree（CST; 共通スパニング ツリー）について説明します。

IST、CIST、および CST の概要

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他のスパニング ツリー プロトコルとは異なり、MST は IST、CIST、CST スパニング ツリーを確立し、維持します。

- IST は 1 つの MST 領域で稼動するスパニング ツリーです。

  各 MST 領域内では、MST 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 は領域の特殊インスタンスで、IST と呼ばれています。他のすべての MST インスタンスは 1 ～ 4094 の番号が振られています。

  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。他のすべてのスパニング ツリー インスタンス情報は、MSTP レコード（M レコード）に含まれていて、MST BPDU 内でカプセル化されています。MST BPDU はすべてのインスタンスの情報を伝送するため、複数のスパニング ツリー インスタンスをサポートするために処理しなければならない BPDU の数は大幅に削減されます。

  同じ領域内にあるすべての MST インスタンスは同じプロトコル タイマーを共有していますが、各 MST インスタンスにはルート ブリッジ ID、ルート パス コストなどの独自のトポロジ パラメータがあります。デフォルトでは、すべての VLAN は IST に割り当てられています。

  MST インスタンスは領域に対してローカルです。たとえば、領域 A と B が相互接続されている場合でも、領域 A の MST インスタンス 1 は 領域 B の MST インスタンス 1 から独立しています。

- CIST は、各 MST 領域にある IST の集合です。
- CST は MST 領域と単一のスパニング ツリーを相互接続します。

1 つの領域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 802.1w、802.1s、802.1D 標準をサポートするスイッチ間で動作するスパニング ツリー アルゴリズムによって形成されます。MST 領域内にある CIST は領域外にある CST と同じです。

詳細については、「MST 領域内のスパニング ツリー動作」（P.19-4）および「MST 領域間のスパニング ツリー動作」（P.19-4）を参照してください。

MST 領域内のスパニング ツリー動作

IST は領域内のすべての MST スイッチを接続します。IST が収束する際に、IST のルートが（802.1s 標準の実装前には *IST マスター*と呼ばれていた）CIST リージョナル ルートとなります（図 19-1（P.19-5）を参照）。CIST リージョナル ルートは、ネットワーク内に領域が 1 つしかない場合は CIST ルートでもあります。CIST ルートが MST 領域外にある場合、領域の境界にある MST 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。

MST スイッチは、初期化時に、自身が CIST と CIST リージョナル ルートであると主張するため、CIST ルートと CIST リージョナル ルートへのパス コストを 0 に設定する BPDU を送信します。スイッチは、さらにすべての MST インスタンスも初期化し、自身がこれらすべてのルートであると主張します。スイッチが現在ポートに格納されているものよりも上位の MST ルート情報（小さいスイッチ ID、低いパス 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。

初期化中に、領域内に独自の CIST リージョナル ルートを持つ多くのサブ領域が形成される場合があります。スイッチは、上位の IST 情報を同じ領域のネイバから受信すると、古いサブ 領域を脱退して真の CIST リージョナル ルートが含まれる新しいサブ 領域に加入します。これにより、真の CIST リージョナル ルートが含まれるものを除くすべてのサブ 領域が縮小します。

正しく動作するために、MST 領域内のすべてのスイッチは同じ CIST リージョナル ルートを承認する必要があります。したがって、領域内にある任意の 2 つのスイッチは、共通 CIST リージョナル ルートに収束する場合、MST インスタンスに対するポート ロールのみを同期します。

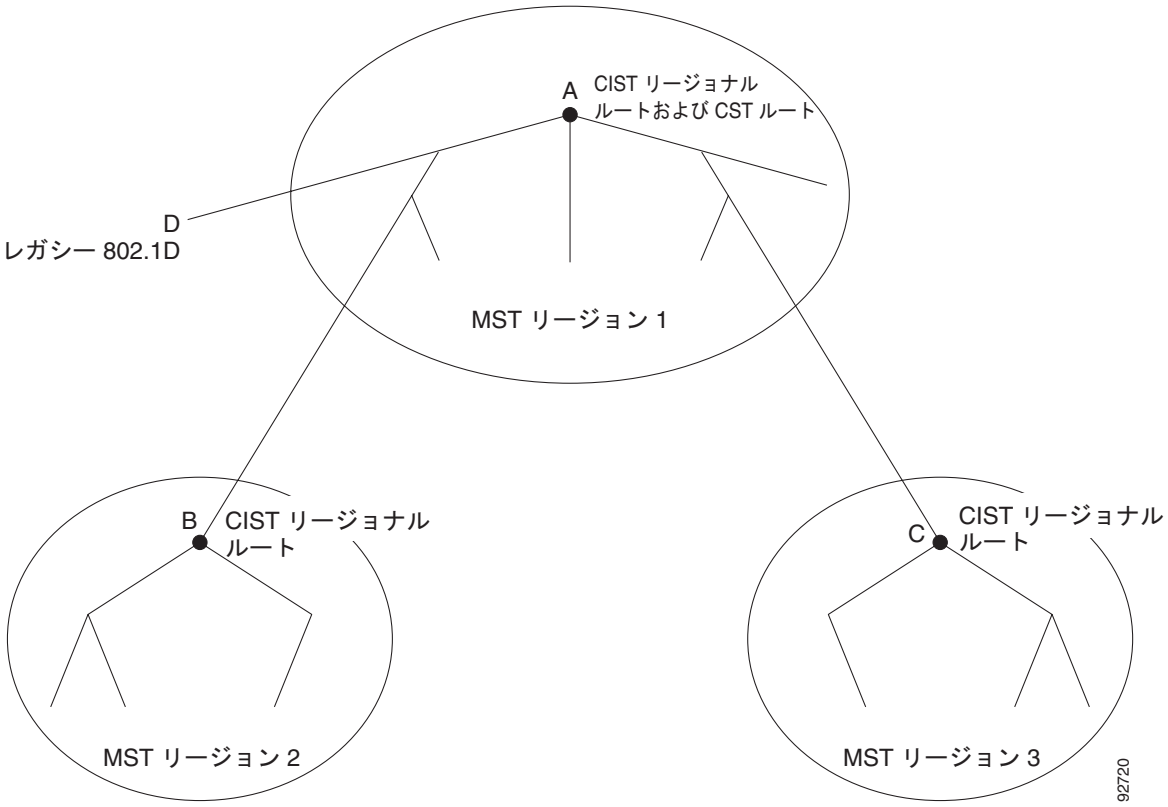
MST 領域間のスパニング ツリー動作

複数の領域または 802.1D スイッチがネットワーク内にある場合、MST が CST を確立して維持します。これには、ネットワーク内のすべての MST 領域とすべての 802.1D STP スイッチが含まれます。MST インスタンスは領域の境界で IST と結合して CST になります。

IST は領域内のすべての MST スイッチを接続し、スイッチ ドメイン全体を網羅する CIST 内のサブツリーとして認識されます。サブツリーのルートは CIST リージョナル ルートです。MST 領域は、隣接する STP スイッチおよび MST 領域からは仮想スイッチとして認識されます。

図 19-1 は、3 つの MST 領域および 802.1D スイッチ（D）があるネットワークを示しています。領域 1 の CIST リージョナル ルート（A）は CIST ルートでもあります。領域 2 の CIST リージョナル ルート（B）および領域 3 の CIST リージョナル ルート（C）は、CIST 内の各サブツリーのルートです。

図 19-1　MST 領域、CIST リージョナル ルート、および CST ルート



CST インスタンスのみが BPDU を送受信し、MST インスタンスがスパニング ツリー情報を BPDU に追加して、隣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。このため、BPDU 送信に関連したスパニング ツリー パラメータ（たとえば hello 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、すべての MST インスタンスに影響します。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。

MST スイッチは、バージョン 3 BPDU または 802.1D STP BPDU を使用して 802.1D スイッチと通信します。MST スイッチは MST BPDU を使用して MST スイッチと通信します。

IEEE 802.1s 用語

先行標準実装で使用されている MST 命名規則の中には、*内部*および*リージョナル*パラメータの ID を識別するために変更されたものもあります。これらのパラメータは、ネットワーク全体で使用されている外部パラメータとは違い、MST 領域のみで使用されます。CIST はネットワーク全体にまたがる唯一のスパニング ツリー インスタンスなので、CIST パラメータでは、内部修飾子や領域の修飾子ではなく、外部修飾子が必要です。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートのコストです。このコストは、MST 領域内では変化しません。MST 領域は CIST に対して単一のスイッチのように見えることに注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチとどの領域にも属さないスイッチとの間で計算されたルート パス コストです。
- CIST リージョナル ルートは、先行標準実装では IST マスターと呼ばれていました。CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。それ以外の場合は、領域内で CIST ルートに最も近いスイッチが CIST リージョナル ルートです。CIST リージョナル ルートは IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートのコストです。このコストは、IST（インスタンス 0）にのみ関連します。

表 19-1 では、IEEE 標準の用語とシスコ先行標準の用語とを比較します。

表 19-1　先行標準用語と標準用語

IEEE 標準定義	シスコ先行標準実装	シスコ標準実装
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
MST Instance（MSTI; MST インスタンス）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

スパニング ツリー トポロジを計算するためにコンフィギュレーション BPDU の MST はメッセージ有効期間および最大エージング タイムの情報を使用しません。その代わりに、ルートへのパス コストおよび IP Time to Live（TTL; 存続可能時間）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で、領域内の最大ホップを設定してそれをその領域内にある IST およびすべての MST インスタンスに適用できます。ホップ カウントは、メッセージ有効期間情報と同じ結果（再設定の開始）となります。インスタンスのルート ブリッジは、常にコスト 0 でホップ カウントが最大値に設定されている BPDU（または M レコード）を送信します。スイッチがこの BPDU を受信すると、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。ホップ カウントが 0 になると、スイッチは BPDU を廃棄して、ポートに維持され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および最大エージング タイムの情報は、領域全体で同じままです。同じ値が、境界にある領域の指定ポートによって伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは MST 領域を次の STP 領域のいずれかに接続します。

- RSTP を稼動する単一のスパニング ツリー領域
- PVST+ または Rapid PVST+ を稼動する単一のスパニング ツリー領域
- 異なる MST コンフィギュレーションを持つ別の MST 領域

境界ポートは LAN にも接続されています。LAN の指定スイッチは、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のいずれかです。

802.1s 標準には境界ポートの定義はありません。802.1Q-2002 標準では、ポートが受信できるメッセージを内部（同一領域内から発信）と外部の 2 種類に分別します。メッセージが外部の場合、CIST のみが受信します。CIST の役割がルートまたは代替ルートの場合、または外部 BPDU がトポロジ変更の場合、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 が CIST 部分を受信し、各 MST インスタンスが関連する M レコードを受信します。シスコ先行標準の実装では、外部メッセージを受信するポートを境界ポートとして扱います。そのため、ポートは内部メッセージと外部メッセージの両方を受信できません。

MST 領域には、スイッチと LAN の両方が含まれます。セグメントは、その指定ポートの領域に属します。したがって、セグメントの指定ポートとは異なる領域にあるポートが境界ポートとなります。この定義により、領域の内側にある 2 つのポートが異なる領域に属するポートとセグメントを共有することができるので、内部メッセージと外部メッセージの両方をポートで受信できる可能性があります。

シスコ先行標準実装からの主な変更点は、指定ポートが STP 互換モードで動作しない場合は境界ポートとして定義されないことです。

（注）　セグメントに 802.1D STP スイッチがある場合、メッセージは常に外部と見なされます。

先行標準からのその他の変更として、RSTP またはレガシー 802.1s スイッチ の送信側スイッチ ID が含まれる場所へ、CIST リージョナル ルート ブリッジ ID フィールドが挿入されるという点があります。一貫した送信側スイッチ ID を近接スイッチに送信することにより、領域全体が単一の仮想スイッチとして動作します。この例では、A または B がセグメントで指定されているかどうかにかかわらず、スイッチ C はルートの送信側スイッチ ID が同一である BPDU を受信します。

標準準拠 IEEE MST 実装

標準準拠 MST 実装には、標準を満たすために必要な機能と、現在公表されている標準にまだ採用されていない先行標準機能の中で望ましい機能の一部が含まれています。ここでは、標準準拠 MST 実装について説明します。

- 「ポート ロール命名の変更」（P.19-8）
- 「従来の標準と標準準拠スイッチとの間でのスパニング ツリーの相互運用スイッチ」（P.19-8）
- 「単一方向リンク障害の検出」（P.19-9）

ポート ロール命名の変更

境界の役割は、最終 MST 標準で削除されましたが、この境界の概念は標準準拠実装では維持されています。ただし、領域の境界にある MST インスタンス（MSTI）ポートは対応する CIST ポートのステートに従わない可能性があります。現在、次の 2 つの状態が存在します。

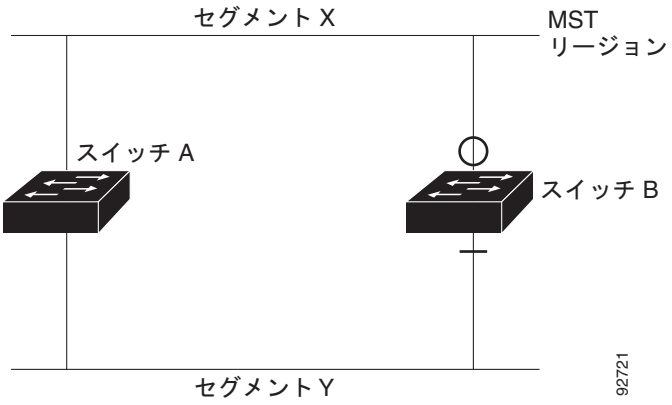
- 境界ポートが CIST リージョナル ルートのルート ポートである - CIST インスタンス ポートは、提案されて同期が取られている場合、すべての対応 MSTI ポートで同期化された（したがって転送された）あとでのみ合意を送り返してフォワーディング ステートに移行することができます。ここで MSTI ポートに、マスターの役割が含まれます。
- 境界ポートが CIST リージョナル ルートのルート ポートではない - MSTI ポートが CIST ポートのステートと役割に従います。標準で提供される情報は少ないので、BPDU（M レコード）を受信しないときに MSTI ポートを代わりにブロックできる理由を理解するのが難しい場合もあります。この場合、境界の役割がすでに存在していなくても、**show** コマンドを入力する際に、出力の *type* カラムで境界としてポートが識別されます。

従来の標準と標準準拠スイッチとの間でのスパニング ツリーの相互運用スイッチ

先行標準スイッチの自動検出が失敗することもあるため、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先行標準ポートを識別できます。標準および先行標準スイッチとの間で領域を形成することはできませんが、CIST を使用する前に相互運用することはできます。この特定のケースでは、さまざまなインスタンスにおけるロード バランシング機能のみが失われます。ポートが先行標準 BPDU を受信する際に、Command Line Interface（CLI; コマンドライン インターフェイス）はポート設定に応じてさまざまなフラグを表示します。先行標準 BPDU 伝送用に設定されていないポートでスイッチが最初に先行標準 BPDU を受信するときに Syslog メッセージも表示されます。

図 19-2 は、先行標準スイッチに接続されている標準準拠スイッチを表しています。A が標準準拠スイッチで B が先行標準スイッチで、いずれも同じ領域に設定されているとします。A は CIST のルート ブリッジで、B にはセグメント X にルート ポート（BX）、およびセグメント Y に代替ポート（BY）があります。セグメント Y がフラップして、BY のポートが単一の先行標準 BPDU を送信する前に代替ポートとなる場合、AY は先行標準スイッチが Y に接続されていることを検出できず、標準 BPSU を送信し続けます。ポート BY は境界に固定され、A と B との間のロード バランシングは実行できません。同じ問題はセグメント X にも存在しますが、B はトポロジ変更を送信する場合があります。

図 19-2　　標準準拠および先行標準スイッチの相互運用



（注）　標準 MST 実装と先行標準 MST 実装との間では、相互運用を最小限にすることを推奨します。

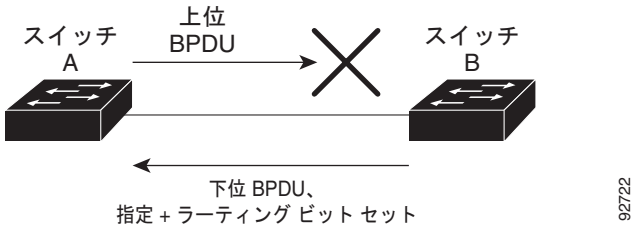
単一方向リンク障害の検出

この機能は、IEEE MST 標準にはありませんが、標準準拠実装には含まれています。ブリッジング ループが発生する可能性のある単一方向リンク障害を検出するために、ソフトウェアが受信した BPDU のポート ロールとステートの一貫性をチェックします。

指定ポートが矛盾を検出すると役割は維持されますが、状態は廃棄ステートに戻ります。これは、接続に矛盾が生じた場合、ブリッジング ループを開始するよりも接続を中断する方が好ましためです。

図 19-3 は、一般的にブリッジング ループを作成する単一方向リンク障害を示します。スイッチ A はルート ブリッジで、その BPDU はスイッチ B へのリンクで損失されます。RSTP および MST BPDU には、送信ポートの役割とステートが含まれます。この情報を使用して、スイッチ A は、スイッチ B が A の送信した上位 BPDU に反応せず、スイッチ B が指定スイッチでルート ブリッジではないことを検出できます。この結果、スイッチ A は B のポートをブロックする（またはブロックし続ける）ため、ブリッジング ループが回避されます。

図 19-3　　単一方向リンク障害の検出



IEEE 802.1D-1998 STP とのインターオペラビリティ

MST を稼動しているスイッチは、802.1D スイッチと相互運用できるようにする内蔵プロトコル移行機能をサポートします。このスイッチが 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、そのポートの 802.1D BPDU のみを送信します。MST スイッチは、802.1D BPDU、異なる領域と関連付けられている MST BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることも検出できます。

ただし、スイッチが 802.1D BPDU を受信しなくなっても、自動的に MST モードに戻ることはありません。これは、802.1D スイッチが指定スイッチでない場合、802.1D スイッチがリンクから削除されているかどうかを検出できないためです。さらにスイッチは、このスイッチに接続されているスイッチがその領域に加入した場合、引き続きポートに境界の役割を割り当てる可能性もあります。プロトコル移行プロセスを再起動する（近接スイッチと強制的に再ネゴシエーションする）には、**clear spanning-tree detected-protocols** イネーブル EXEC コマンドを使用します。

リンク上のすべての 802.1D スイッチが RSTP スイッチの場合、RSTP BPDU のように MST BPDU を処理できます。したがって、MST スイッチがバージョン 0 コンフィギュレーションと Topology Change Notification（TCN; トポロジ変更通知）BPDU、または境界ポート上のバージョン 3 MST BPDU のいずれかを送信します。境界ポートは、境界ポートの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。

RSTP の概要

RSTP は、ポイントツーポイント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。スパニング ツリーの再設定は 1 秒以内に実行できます（802.1D スパニング ツリーのデフォルト設定の場合は 50 秒かかります）。

ここでは、RSTP の機能について説明します。

ポート ロールとアクティブ トポロジ

RSTP では、ポート ロールを割り当ててアクティブ トポロジを学習することで、スパニング ツリーの高速コンバージェンスを実現しています。「ルート ブリッジの選定」（P.20-5）で説明しているように、RSTP は、802.1D STP を構築して、最高のスイッチ プライオリティ（最小プライオリティ値）を持つスイッチをルート ブリッジとして選択します。次に RSTP は、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 - スイッチがルート ブリッジにパケットを転送する際に最適パス（最小コスト）を提供します。
- 指定ポート - 指定スイッチに接続します。LAN からルート ブリッジにパケットを転送する際に最小パス コストとなります。指定スイッチが LAN に接続されるポートを指定ポートと呼びます。
- 代替ポート - 現在のルート ポートが提供するルート ブリッジへの代替パスを提供します。
- バックアップ ポート - 指定ポートが提供する、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 ポートは、2 つのポートがループバック内でポイントツーポイント リン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複数ある場合のみ、存在できます。
- ディセーブル ポート - スパニング ツリーの動作中の役割が指定されていないポートです。

ルート ポートまたは指定のポート ロールを割り当てられたポートは、アクティブ トポロジに含まれます。代替ポートまたはバックアップのポート ロール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。

ネットワーク全体で一貫したポート ロールがある安定したトポロジでは、RSTP により各ルート ポートおよび指定ポートは即座にフォワーディング ステートに移行し、すべての代替ポートおよびバックアップ ポートは必ず廃棄ステートになります（802.1D でのブロッキングと同様）。ポート ステートは、フォワーディングおよびラーニング プロセスの動作を制御します。表 19-2 に、802.1D と RSTP ポート ステートの比較を示します。

表 19-2　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	アクティブ トポロジ内のポートの有無
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 実装製品との整合性をはかるために、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 にはスイッチ、スイッチ ポート、または LAN に障害が発生したあとに、短時間で接続を回復する機能があります。エッジ ポート、新規ルート ポート、およびポイントツーポイント リンクで接続されたポートに対して、次のような高速コンバージェンス機能を提供します。

- 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 スイッチにあるエッジ ポートとしてポートを設定した場合、エッジ ポートは即座にフォワーディング ステートに移行します。エッジ ポートは Port Fast 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のみです。
- ルート ポート - RSTP が新規ルート ポートを選択した場合、古いルート ポートをブロックし即座に新規ルート ポートがフォワーディング ステートに移行します。
- ポイントツーポイント リンク - ポイントツーポイント リンクを介してポートを別のポートに接続してローカル ポートが指定ポートになる場合、ループのないトポロジを実現するために、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ます。

  スイッチ A はポイントツーポイント リンクを介してスイッチ B に接続されており、すべてのポートがブロッキング ステートになります（図 19-4 を参照）。スイッチ A のプライオリティがスイッチ B のプライオリティよりも小さい値であると仮定します。スイッチ A が提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）をスイッチ B に送信して、スイッチ A 自身が指定スイッチであると提案します。

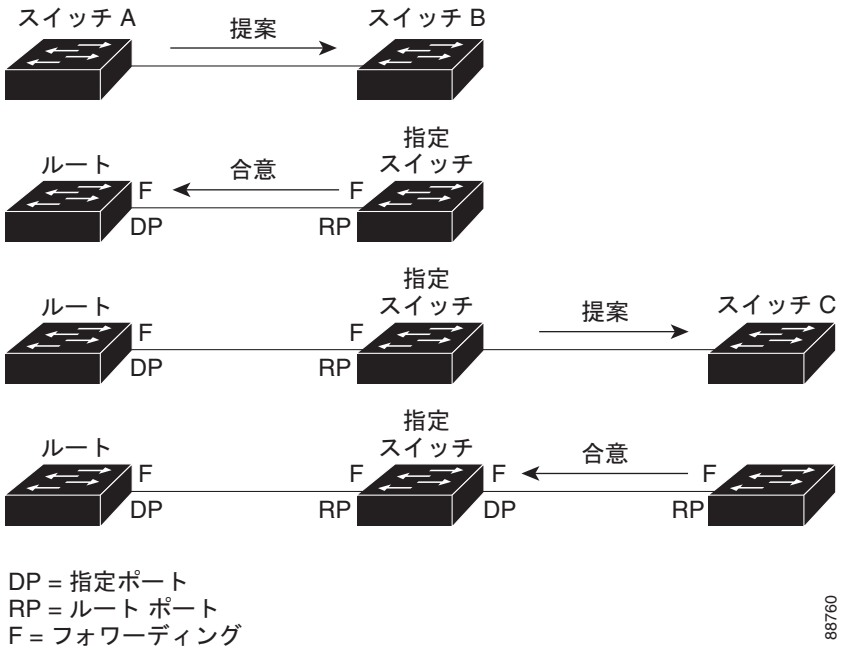
  スイッチ B が提案メッセージを受信すると、提案メッセージを受信したポートを新しいルート ポートとして選択し、すべての非エッジ ポートを強制的にブロッキング ステートにします。さらに、その新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

  スイッチ A は、スイッチ B から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 はそのすべての非エッジ ポートをブロックしており、さらにスイッチ A と B はポイントツーポイント リンクで接続されているため、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、同様の一連のハンドシェイク メッセージが交換されます。スイッチ C スイッチは B に接続されたポートをルート ポートとして選択し、両端のポートはすぐにフォワーディング ステートに移行します。このハンドシェイク プロセスの繰り返しによってアクティブ トポロジにスイッチが追加されます。ネットワークが収束するにつれて、この提案合意ハンドシェイクがルートからスパニング ツリーのリーフに進みます。

スイッチ は、ポートの二重モードからリンク タイプを判断します。つまり、全二重ポートはポイントツーポイント接続と見なされ、半二重ポート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 コマンドを使用して、デュプレックス設定で制御されたデフォルト設定を上書きできます。

図 19-4　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 ロールの同期化

スイッチのポートの 1 つで提案メッセージを受信し、そのポートが新しいルート ポートとして選択されると、RSTP は他のすべてのポートを新しいルート情報と強制的に同期化させます。

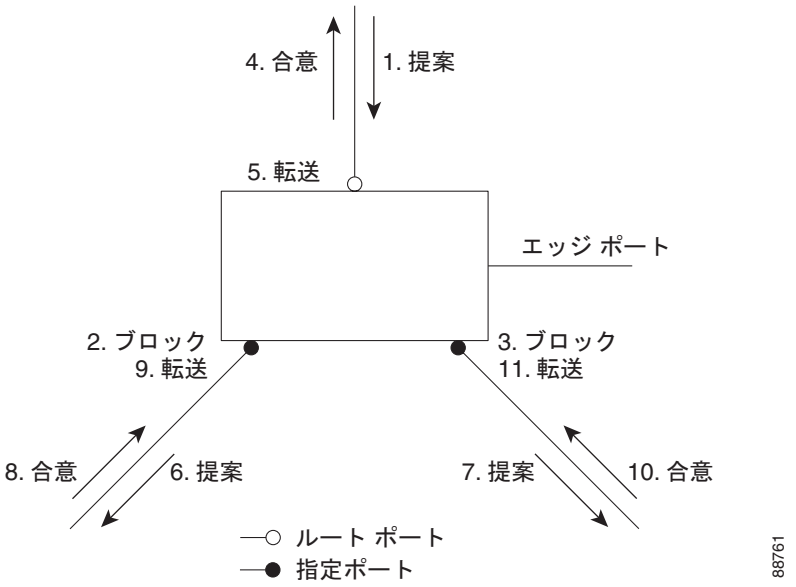
他のポートがすべて同期化されると、スイッチはルート ポートで受信した上位のルート情報と同期化されます。次のような場合、スイッチの個別のポートが同期されます。

- ポートがブロッキング ステートの場合
- エッジ ポート（ネットワークのエッジ上に設定されているポート）の場合

指定ポートがフォワーディング ステートでエッジ 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と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 ステートに移行します。一般に、RSTP がポートをルート情報と強制的に同期させ、ポートが上記のどの条件も満たしていない場合、その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 リンクによって接続されたスイッチがそれぞれのポート ロールについて合意すると、RSTP はポートのステートを即座にフォワーディング ステートに移行させます。図 19-5 に、このイベント シーケンスを示します。

図 19-5　高速コンバージェンス時のイベント シーケンス



ブリッジ プロトコル データ ユニットの形式と処理

ここでは、ブリッジ プロトコル データ ユニット（BPDU）の形式と処理について説明します。

- 「BPDU 形式と処理の概要」（P.19-13）
- 「上位 BPDU 情報の処理」（P.19-14）
- 「下位 BPDU 情報の処理」（P.19-14）

BPDU 形式と処理の概要

RSTP BPDU の形式は、プロトコル バージョンが 2 に設定されている点を除き、802.1D BPDU の形式と同じです。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 のプロトコル情報が存在しないことを意味します。表 19-3 に、RSTP フラグ フィールドを示します。

表 19-3　RSTP BPDU フラグ

ビット	機能
0	Topology Change（TC; トポロジの変更）
1	提案
2–3:	ポート ロール
00	不明
01	代替ポートまたはバックアップ 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

表 19-3　RSTP BPDU フラグ （続き）

ビット	機能
6	合意
7	Topology Change Acknowledgement（TCA; トポロジ変更の確認）

送信スイッチは、自身をその LAN の指定スイッチとして提案する提案フラグを RSTP の BPDU に設定します。提案メッセージでは、ポート ロールは常に指定ポートに設定されます。

送信スイッチは、前の提案を受け入れる合意フラグを RSTP の BPDU に設定します。合意メッセージ内のポート ロールは、常にルート ポートに設定されます。

RSTP には 個別の TCN BPDU はありません。トポロジの変更を示すには、トポロジの変更（TC）フラグを使用します。ただし、802.1D スイッチとインターオペラビリティを保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニング フラグとフォワーディング フラグは、送信ポートのステートに応じて設定されます。

上位 BPDU 情報の処理

上位 BPDU は、現在ポートに格納されているものよりも上位のルート情報（小さいスイッチ ID、低いパス コストなど）を持つ BPDU です。

ポートが上位 BPDU を受信すると、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てから合意メッセージを送信します。BPDU が 802.1D BPDU の場合、スイッチは提案フラグを設定せずにポートの転送遅延タイマーを開始します。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。

ポートで上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、合意メッセージを送信します。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

下位 BPDU は、現在ポートに格納されているものよりも下位のルート情報（大きいスイッチ ID、高いパス コストなど）を持つ BPDU です。

指定ポートが下位 BPDU を受信すると、その指定ポートは自身の情報で即座に応答します。

トポロジの変更

スパニング ツリー トポロジの変更を処理する際の RSTP と 802.1D との違いは以下のとおりです。

- 検出 - 802.1D では、ブロッキング ステートとフォワーディング ステートとの間の*どのような*移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が生じるのは、ブロッキング ステートからフォワーディング ステートに移行する場合*だけ*です（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジ ポートでステートが変更されても、トポロジの変更は発生しません。RSTP スイッチはトポロジの変更を検出すると、TC 通知を受信するものを除いたすべての非エッジ ポートで学習済みの情報を削除します。
- 通知 - RSTP は、802.1D のように TCN BPDU を使用しません。ただし、802.1D とインターオペラビリティを保つために、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 802.1D スイッチから TCN メッセージを受信すると、TCA ビットが設定された 802.1D コンフィギュレーション BPDU で応答します。ただし、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（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 が設定されたコンフィギュレーション BPDU を受信した場合、TC 時間タイマーがリセットされます。

  この動作方法は、802.1D スイッチをサポートする場合にのみ必要です。RSTP の BPDU には、TCA ビットが設定されません。
- 伝播 - RSTP スイッチが指定ポートまたはルート ポート経由で別のスイッチから TC メッセージを受信すると、そのすべての非エッジ ポート、指定ポート、およルート ポート（受信ポートを除く）にトポロジ変更が伝播されます。スイッチは、これらのすべてのポートの TC 時間タイマーを開始し、これらのポート上で学習した情報をフラッシュします。
- プロトコルの移行 - 802.1D スイッチとの下位互換性を保つために、RSTP は 802.1D コンフィギュレーション BPDU と TCN BPDU をポート単位で選択的に送信します。

  ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU を送信する最短時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブの間、スイッチは目的のポートで受信されたすべての BPDU を処理し、プロトコル タイプは無視します。

  ポートの移行遅延タイマーの期限が切れたあとに、スイッチが 802.1D BPDU を受信した場合、スイッチは 802.1D スイッチに接続されたと認識し、802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチがポートで 802.1D BPDU を使用している場合に、タイマー満了後に RSTP BPDU を受信すると、スイッチはタイマーを再起動し、そのポートで RSTP BPDU の使用を開始します。

MST の設定

ここでは、MST の設定手順について説明します。

デフォルトの MST 設定

表 19-4 に、デフォルトの MST 設定を示します。

表 19-4　デフォルトの MST 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+ および MST がディセーブル）
スイッチ プライオリティ（CIST ポート単位に設定可能）	32768
スパニング ツリー ポート プライオリティ（CIST ポート単位に設定可能）	128
スパニング ツリー ポート コスト（CIST ポート単位に設定可能）	1000 Mbps: 4 100 Mbps: 19 10 Mbps: 100
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
最大ホップ カウント	20 ホップ

MST 設定時の注意事項および制約事項

MST を設定する際に、以下の注意事項と制約事項に従ってください。

- 802.1s MST 標準により、最大 65 個の MST インスタンスを使用可能です。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 MST はサポートされていますが、1 度にアクティブにすることのできるバージョンは 1 つだけです。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、MST コンフィギュレーションを伝播しません。コマンドライン インターフェイス（CLI）または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して、MST 領域内にある各スイッチ上で、MST コンフィギュレーション（領域名、リビジョン番号、VLAN/インスタンス間のマッピング）を手動で設定する必要があります。
- ネットワーク内の冗長パス全体でロード バランシングを機能させるためには、すべての VLAN/インスタンス間マッピングの割り当てを一致させなければなりません。一致しない場合、すべてのトラフィックが単一リンクに流れます。
- PVST+ および MST クラウド、または Rapid-PVST と MST クラウドとの間でロード 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 CIST リージョナル ルートが CST のルートでなければなりません。MST クラウドが複数の MST 領域で構成されている場合、MST 領域の 1 つに CST ルートが含まれていなければならず、その他のすべての MST 領域には MST クラウド内に含まれるルートへのパスが、PVST+ または Rapid-PVST+ クラウドよりも良好なものでなければなりません。
- ネットワークを多数の領域に分割することは推奨しません。ただし、そのような状況が避けられないような場合には、スイッチド LAN を非レイヤ 2 装置と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。
- 既存の MST インスタンスに対して VLAN の追加または削除を行うと、その MST インスタンスについてスパニング ツリーの再計算が開始され、その MST インスタンスに対するすべての VLAN のトラフィックが中断されます。

MST 領域設定の指定と MST のイネーブル化

複数のスイッチを同じ MST 領域に設定するには、同じ VLAN/インスタンス間マッピング、同じコンフィギュレーション リビジョン番号、および同じ MST 名を設定する必要があります。

1 つの領域には、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を持つことができ、各メンバには RSTP BPDU を処理する能力がなければなりません。ネットワーク内の MST 領域数には制限がありませんが、各領域は最大で 65 のスパニング ツリー インスタンスのみをサポートできます。1 つの VLAN を同時に割り当てることのできるスパニング ツリー インスタンスは 1 つだけです。

MST 領域の設定を指定して MST をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# 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。

	コマンド	目的
ステップ 3	`Router(config-mst)# instance instance_id vlan vlan_range`	VLAN を MST インスタンスにマッピングします。 • *instance_id* に対して、範囲は 0 ～ 4094 です。 • **vlan** *vlan_range* に対して、範囲は 1 ～ 4094 です。 VLAN を MST インスタンスにマッピングすると、マッピングは差分で、コマンドに指定された VLAN は以前にマッピングされた VLAN に追加されるか、または VLAN から削除されます。 VLAN 範囲を指定する場合にはハイフンを使用します。たとえば VLAN 1 ～ 63 を MST インスタンス 1 にマッピングする場合は、**instance 1 vlan 1-63** とします。 連続した VLAN を指定する場合には、カンマを使用します。たとえば VLAN 10、20、30 を MST インスタンス 1 にマッピングする場合は、**instance 1 vlan 10, 20, 30** とします。
ステップ 4	`Router(config-mst)# name instance_name`	インスタンス名を指定します。*name* 文字列は、最大 32 文字で大文字と小文字を区別します。
ステップ 5	`Router(config-mst)# revision version`	設定のリビジョン番号を指定します。範囲は 0 ～ 65535 です。
ステップ 6	`Router(config-mst)# show pending`	入力した設定を表示して、確認します。
ステップ 7	`Router(config)# exit`	すべての変更を適用し、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	`Router(config)# spanning-tree mode mst`	MST と RSTP をイネーブルにします。 **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規モードで再開されるため、トラフィックを中断できます。 MST と PVST+、または MST と Rapid PVST+ を同時に実行できません。
ステップ 9	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 10	`Router# show running-config`	設定を確認します。
ステップ 11	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

デフォルトに戻すには、以下のように実行します。

- デフォルトの MST 領域設定に戻るには、**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。
- デフォルトの VLAN/インスタンス間マッピングに戻るには、**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るには、**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るには、**no revision** MST コンフィギュレーション コマンドを使用します。
- Rapid PVST+ をイネーブルにするには、**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 コマンドを入力します。

次に、MST コンフィギュレーション モードを開始して、VLAN10 ～ 20 を MST インスタンス 1 にマッピングし、その領域の名前を *region1* に設定し、コンフィギュレーション リビジョンを 1 に設定し、入力した設定を表示し、変更を適用して、グローバル コンフィギュレーション モードに戻る例を示します。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 10-20
Router(config-mst)# name region1
Router(config-mst)# revision 1
Router(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instances configured 2
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Router(config-mst)# exit
Router(config)#
```

ルート ブリッジの設定

スイッチは、マッピングされた VLAN グループのスパニング 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 プライオリティおよびスイッチの MAC アドレスで構成されるスイッチ ID が関連付けられます。VLAN のグループに対して、最小のスイッチ ID を持つスイッチがルート ブリッジとなります。

スイッチがルート ブリッジになるように設定するには、スイッチが指定したスパニング ツリー インスタンスのルート ブリッジとなるように、**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）から非常に小さな値へと変更します。このコマンドを入力する際に、スイッチがルート ブリッジのスイッチ プライオリティを確認します。拡張システム ID をサポートしているため、24576 という値でスイッチが指定したスパニング ツリー インスタンスのルート ブリッジとなる場合、そのスイッチは指定したインスタンスに対する自身のプライオリティを 24576 に設定します。

インスタンスに指定されているルート ブリッジのスイッチ プライオリティが 24576 を下回る場合、スイッチは自身のプライオリティを最も小さなスイッチ プライオリティを下回る 4096 に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 20-2（P.20-3）を参照）。

ネットワークを構成するスイッチに拡張システム ID をサポートするものとサポートしないものがある場合、拡張システム ID をサポートするスイッチがルート ブリッジになることはありません。拡張システム ID は、VLAN 番号が古いソフトウェアを実行している接続スイッチのプライオリティよりも大きくなるように、スイッチ プライオリティ値を増やします。

各スパニング ツリー インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチでなければなりません。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 ブリッジ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（レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間における最大ブリッジ ホップ数）を指定するには、MST インスタンス 0 でのみ利用可能な **diameter** キーワードを指定します。ネットワーク直径を指定すると、スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、コンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注） ルート ブリッジとして設定されているスイッチを使用する場合、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** 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しないでください。

スイッチをルート ブリッジとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-config)# spanning-tree mst` *instance_id* **root primary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	（任意）スイッチをルート ブリッジとして設定します。 • *instance_id* に対して、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、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。範囲は 0 ～ 4094 です。 • （任意）**diameter** *net_diameter* に対して、任意の 2 つのエンド ステーション間における最大レイヤ 2 ホップ数を設定します。範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 に対してのみ使用できます。 • （任意）**hello-time** *seconds* に対して、ルート ブリッジによって作成されるコンフィギュレーション メッセージの間隔を秒で指定します。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	`Router(config-config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst` *instance_id*	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

デフォルトのスイッチ設定に戻るには、**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 ブリッジの設定

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 ブリッジ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 ブリッジになる可能性が高くなります。この場合、ネットワーク上の他のスイッチがデフォルトのブリッジ プライオリティ 32768 を使用していて、ルート ブリッジになる可能性がないと仮定しています。

このコマンドを複数のスイッチに対して実行すると、複数のバックアップ ルート ブリッジを設定できます。プライマリ ルート ブリッジ を設定する際に使用するのと同じネットワーク直径と hello-time 値を **spanning-tree mst** *instance_id* **root primary** グローバル コンフィギュレーション コマンドで使用してください。

スイッチをセカンダリ ルート ブリッジとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst` *instance_id* **root secondary** [**diameter** *net_diameter* [**hello-time** *seconds*]]	（任意）スイッチをセカンダリ ルート ブリッジとして設定します。 • *instance_id* に対して、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、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。範囲は 0 ～ 4094 です。 • （任意）**diameter** *net_diameter* に対して、任意の 2 つのエンド ステーション間におけるスイッチの最大数を設定します。範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 に対してのみ使用できます。 • （任意）**hello-time** *seconds* に対して、ルート ブリッジによって作成されるコンフィギュレーション メッセージの間隔を秒で指定します。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 ブリッジを設定するときに使用したものと同じネットワーク直径および hello タイムを使用してください （「ルート ブリッジの設定」（P.19-19）を参照）。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst` *instance_id*	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

デフォルトのスイッチ設定に戻るには、**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

ループが発生すると、MST はポート プライオリティを使用して、フォワーディング ステートに置くインターフェイスを選択します。MST に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値（小さな数値）を、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値（大きな数値）を割り当てることができます。すべてのインターフェイスが同じプライオリティ値を使用している場合には、MST はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残り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 MST ポート プライオリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {{`*type*[1] *slot/port*`} | {`**port-channel** *number*`}}`	（任意）設定するインターフェイスを指定します。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	`Router(config-if)# 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* に対して、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、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。範囲は 0 ～ 4094 です。 • *priority* に対して、値の範囲は 16 単位で、0 ～ 240 です。デフォルト値は 128 です。数値が小さいほど、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、240 です。これ以外の値は拒否されます。
ステップ 4	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface` *interface_id* or `Router# show spanning-tree mst` *instance_id*	設定を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

（注）　**show spanning-tree mst interface** *interface_id* イネーブル 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ステートの場合のみです。それ以外は、**show running-config interface** イネーブル EXEC コマンドを使用して設定を確認します。

インターフェイスをデフォルトの設定に戻すには、**no spanning-tree mst** *instance_id* **port-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。

パス コストの設定

MST 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から抽出されます。ループが発生すると、MST はコストを使用して、フォワーディング ステートに置く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低いコスト値を、最後に選択させたいインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスが同じコスト値を使用している場合には、MST はインターフェイス番号が最も小さいインターフェイスをフォワーディング ステートにして、残り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 MST コストを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	（任意）設定するインターフェイスを指定します。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	`Router(config-if)# spanning-tree mst` *instance_id* `cost` *cost*	コストを設定します。 ループが発生すると、MST はパス コストを使用して、フォワーディング ステートに置くインターフェイスを選択します。パス コストの低い方が高速で伝送されます。 • *instance_id* に対して、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、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。範囲は 0 ～ 4094 です。 • *cost* に対して、範囲は 1 ～ 200000000 で、デフォルト値は、インターフェイスのメディア速度から抽出されます。
ステップ 4	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface` *interface_id* または `Router# show spanning-tree mst` *instance_id*	設定を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

（注） **show spanning-tree mst interface** *interface_id* イネーブル EXEC コマンドは、リンクアップ動作可能ステートのポートの情報のみを表示します。それ以外は、**show running-config** イネーブル EXEC コマンドを使用して設定を確認します。

インターフェイスをデフォルトの設定に戻すには、**no 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

スイッチがルート ブリッジとして選択される可能性が高くなるように、スイッチ プライオリティを設定できます。

（注）　このコマンドを使用する場合には注意が必要です。スイッチ プライオリティを変更する場合、ほとんどの状況で **spanning-tree mst** *instance_id* **root primary** および **spanning-tree mst** *instance_id* **root secondary** 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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst` *instance_id* **priority** *priority*	（任意）スイッチ プライオリティを設定します。 • *instance_id* に対して、単一のインスタンス、ハイフンで区切られたインスタンスの範囲、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。範囲は 0 ～ 4094 です。 • *priority* に対して、値の範囲は 4096 単位で 0 ～ 61440 です。デフォルト値は 32768 です。値が少ない方が、スイッチよりルート ブリッジ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。これ以外の値は拒否されます。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst` *instance_id*	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

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でルート ブリッジによって作成される設定メッセージの間隔を設定できます。

（注）　このコマンドを使用する場合には注意が必要です。hello 時間を変更する場合、ほとんどの状況で **spanning-tree mst** *instance_id* **root primary** および **spanning-tree mst** *instance_id* **root secondary** コマンドを使用することを推奨します。

すべての MST インスタンスに対して hello タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst hello-time` *seconds*	（任意）すべての MST インスタンスに対して hello タイムを設定します。hello タイムは、ルート ブリッジによって作成される設定メッセージの間隔です。これらのメッセージは、スイッチが動作していることを示します。 *seconds* に対して、範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 3	`end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst`	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

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 インスタンスに対して転送遅延時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst forward-time` *seconds*	（任意）すべての MST インスタンスに対して転送時間を設定します。転送遅延は、スパニング ツリー ラーニングおよびリスニング 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* に対して、範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst`	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

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。

伝送ホールド カウントの設定

すべての MST インスタンスに対して伝送ホールド カウントを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree transmit hold-count` *hold_count_value*	すべての MST インスタンスに対して伝送ホールド カウントを設定します。 *hold_count_value* に対して、範囲は 1 ～ 20 です。デフォルトは 6 です。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst`	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree transmit hold-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。

最大エージング タイムの設定

すべての MST インスタンスに対して最大エージング タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst max-age` *seconds*	（任意）すべての MST インスタンスに対して最大エージング タイムを設定します。最大エージング タイムは、スイッチがスパニング ツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。 *seconds* に対して、範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst`	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

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 インスタンスに対して最大ホップ カウントを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# spanning-tree mst max-hops` *hop_count*	（任意）BPDU が廃棄され、ポートで維持されていた情報が期限切れになるまでの、領域内のホップ数を指定します。 *hold_count* に対して、範囲は 1 ～ 255 です。デフォルトは 20 です。
ステップ 3	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst`	設定を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

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

「高速コンバージェンス」（P.19-11）で説明しているように、ポイントツーポイント リンクを介してポートを別のポートに接続し、ローカル ポートを指定ポートにする場合、ループのないトポロジを実現するために、提案合意ハンドシェイクを使用して別のポートへの高速移行をネゴシエーションします。

デフォルトでは、リンク タイプがインターフェイスのデュプレックス モードから制御されます。つまり、全二重ポートはポイントツーポイント接続と見なされ、半二重ポートは共有接続と見なされます。MST を実行しているリモート スイッチの単一ポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書き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。

デフォルトのリンク タイプ設定を上書きするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	（任意）設定するインターフェイスを指定します。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	`Router(config)# spanning-tree link-type point-to-point`	ポートのリンク タイプがポイントツーポイントになるように指定します。
ステップ 4	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface` *interface_id*	設定を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

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、先行標準および 802.1s 標準準拠装置を含めることができます。デフォルトでは、ポートは自動的に先行標準装置を検出しますが、標準および先行標準 BPDU の両方を受信し続けます。装置とネイバ間で不一致が生じた場合、CIST のみがインターフェイスで動作します。

先行標準 BPDU のみを送信するようにポートの設定を選択できます。ポートが STP 互換性モードになっていても、すべての **show** コマンドで先行標準フラグが表示されます。

デフォルトのリンク タイプ設定を上書きするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	（任意）設定するインターフェイスを指定します。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	`Router(config)# spanning-tree mst pre-standard`	ポートが先行標準 BPDU のみを送信するように指定します。
ステップ 4	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface` *interface_id*	設定を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

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

MST を稼動しているスイッチは、802.1D スイッチと相互運用できるようにする内蔵プロトコル移行機能をサポートします。このスイッチが 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、そのポートの 802.1D BPDU のみを送信します。MST スイッチは、802.1D BPDU、異なる領域と関連する MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることも検出できます。

ただし、スイッチが 802.1D BPDU を受信しなくなっても、自動的に MST モードに戻ることはありません。これは、802.1D スイッチが指定スイッチでない場合、802.1D スイッチがリンクから削除されているかどうかを検出できないためです。スイッチは、接続されているスイッチがその領域に加入している場合、ポートに境界の役割を割り当て続け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（近接スイッチと強制的に再ネゴシエーションする）には、**clear spanning-tree detected-protocols** イネーブル 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起動するには、**clear spanning-tree detected-protocols interface** *interface_id* イネーブル EXEC コマンドを入力します。

MST 設定とステータスの表示

スパニング ツリー ステータスを表示するには、1 つまたは複数のイネーブル EXEC コマンドを使用します（表 19-5 を参照）。

表 19-5　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 領域設定を表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれる Message Digest 5（MD5）ダイジェストを表示します。
show spanning-tree mst *instance_id*	指定されたインスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface_id*	指定されたインターフェイスの MST 情報を表示します。

CHAPTER 20

スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定

この章では、Catalyst 6500 シリーズ スイッチに Spanning Tree Protocol（STP; スパニング ツリー プロトコル）および先行標準 IEEE 802.1s Multiple Spanning Tree（MST; 多重スパニング ツリー）プロトコルを設定する手順について説明します。

（注）

- IEEE 802.1s MST プロトコルは、先行標準状態からリリース状態に移行しました。第 19 章「標準準拠 IEEE Multiple Spanning Tree（MST）の設定」では、Release 12.2(18)SXF 以降のリリースでサポートされる標準準拠 MST 実装について説明しています。この章では、Release 12.2(18)SXF よりも前のリリースでサポートされていた 先行標準 MST 実装について説明しています。
- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

（注）

PortFast、UplinkFast、および BackboneFast STP 拡張機能の設定手順については、第 21 章「オプションのスパニング ツリー プロトコル（STP）機能の設定」を参照してください。

STP の機能概要

ここでは、STP の機能について説明します。

STP の概要

STP は、ネットワークの不要なループを排除しながらパスの冗長性を提供する、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 ネットワークが正常に動作するには、2 つのステーション間で存在できるアクティブ パスは 1 つだけです。STP の動作は透過的なので、エンド ステーションが単一の LAN セグメントに接続されているのか、それとも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、エンド ステーションが検知できません。

Catalyst 6500 シリーズ スイッチは、すべての Virtual LAN（VLAN; 仮想 LAN）で STP（IEEE 802.1D ブリッジ プロトコル）を使用します。デフォルトでは、（STP を手動でディセーブルにしない限り）設定されている VLAN ごとに 1 つの STP インスタンスが動作します。STP は、VLAN 単位でイネーブルおよびディセーブルにすることができます。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを形成する必要があります。STP アルゴリズムは、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。レイヤ 2 LAN ポートは定期的に STP フレームを送受信します。ネットワーク装置はこれらのフレームを転送しないで、フレームを使用してループフリー パスを構築します。

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、ネットワーク内でループが発生する原因になります。ネットワークにループが存在する場合、エンド ステーションが重複したメッセージを受信したり、ネットワーク装置が複数のレイヤ 2 LAN ポート上のエンド ステーション Media Access Control（MAC; メディア アクセス制御）アドレスを学習したりする可能性があります。このような状況が、不安定なネットワーク環境につながります。

STP は、ルート ブリッジおよびそのルートからレイヤ 2 ネットワーク上のすべてのネットワーク装置へのループフリー パスを備えたツリーを定義します。STP は冗長データ パスを強制的にスタンバイ（ブロック）ステートにします。スパニング ツリーの 1 つのネットワーク セグメントで障害が発生し、冗長パスが存在する場合、STP アルゴリズムはスパニング 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。

ネットワーク装置上の 2 つのレイヤ 2 LAN ポートがループの一部になっている場合、どちらのポートがフォワーディング ステートになり、どちらのポートがブロッキング ステートになるかは、STP ポート プライオリティおよびポート パス コストの設定によって決まります。STP 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を表すとともに、ポートがトラフィックを渡すのに適した位置にあるかどうかを表します。STP ポート パス コスト値は、メディア速度を表します。

ブリッジ ID の概要

各ネットワーク装置上の各 VLAN には、一意の 64 ビット ブリッジ ID が設定されています。ブリッジ ID はブリッジ プライオリティ値、拡張システム ID、および STP MAC アドレス割り当てで構成されています。

ここでは、次の内容について説明します。

- 「ブリッジ プライオリティ値」（P.20-3）
- 「拡張システム ID」（P.20-3）
- 「STP MAC アドレスの割り当て」（P.20-4）

ブリッジ プライオリティ値

拡張システム ID がイネーブルの場合、ブリッジ プライオリティは 4 ビット値です（表 20-2（P.20-3）および「VLAN のブリッジ プライオリティの設定」（P.20-32）を参照）。

拡張システム ID

12 ビット拡張システム ID フィールドは、ブリッジ ID の一部です（表 20-2（P.20-3）を参照）。64 個の MAC アドレスのみをサポートするシャーシは、常に 12 ビット拡張システム ID を使用します。1,024 個の MAC アドレスをサポートするシャーシでは、拡張システム ID の使用をイネーブルにできます。STP は拡張システム ID として VLAN ID を使用します。「拡張システム ID のイネーブル化」（P.20-25）を参照してください。

表 20-1　拡張システム ID がディセーブルの場合のブリッジ プライオリティ値

ブリッジ プライオリティ値															
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

表 20-2　拡張システム ID がイネーブルの場合のブリッジ プライオリティ値および拡張システム ID

ブリッジ プライオリティ値				拡張システム ID（VLAN ID と同設定）											
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

STP MAC アドレスの割り当て

Catalyst 6500 シリーズ スイッチ シャーシには、STP のようなソフトウェア機能をサポートするために使用可能な 64 個または 1,024 個の MAC アドレスがあります。シャーシの MAC アドレスの範囲を表示するには、**show catalyst6000 chassis-mac-address** コマンドを入力します。

64 個の MAC アドレスを持つシャーシの場合、STP は拡張システム ID と MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

拡張システム ID がイネーブルになっていない場合は、STP は VLAN ごとに 1 つの MAC アドレスを使用して、VLAN ごとに一意のブリッジ ID を作成します。

拡張システム ID がイネーブルになっているネットワークにネットワーク装置がある場合、望ましくないルート ブリッジ選択やスパニング ツリー トポロジ問題を回避するために、レイヤ 2 で接続されているその他すべてのネットワーク装置でも、拡張システム ID をイネーブルにする必要があります。

拡張システム ID がイネーブルの場合、ルート ブリッジのプライオリティは、4096 の倍数プラス VLAN ID になります。拡張システム ID がイネーブルの場合、スイッチ ブリッジ ID（ルート ブリッジの ID を決定するためスパニング ツリー アルゴリズムによって使用され、最小値のほうが優先される）は、4096 の倍数としてのみ指定できます。次の数値のみ利用可能です。0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440。

同じスパニング ツリー ドメイン内の別のブリッジで拡張 システム ID がイネーブルになっていない場合、ブリッジ ID の選択がより細かい粒度のために、そのブリッジがルート ブリッジの所有権を取得する可能性があります。

ブリッジ プロトコル データ ユニット（BPDU）の概要

Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）はルート ブリッジから一方向に送信されます。各ネットワーク装置はコンフィギュレーション BPDU を送信して、スパニング ツリー トポロジを伝達および計算します。各コンフィギュレーション BPDU に含まれる最小限の情報は、次のとおりです。

- 送信側ネットワーク装置がルート ブリッジと見なしているネットワーク装置の固有のブリッジ ID
- ルートまでの STP パス コスト
- 送信側ブリッジのブリッジ ID
- メッセージ エージ
- 送信側ポートの識別子
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

ネットワーク装置が BPDU フレームを伝送すると、そのフレームが伝送される LAN に接続されたすべてのネットワーク装置が BPDU を受信します。ネットワーク装置が BPDU を受信すると、ネットワーク装置はそのフレームを転送するのではなく、フレームに含まれる情報を使用して BPDU を計算し、トポロジに変更があれば、BPDU の送信を開始します。

BPDU 交換によって次の処理が行われます。

- 1 台のネットワーク装置がルート ブリッジとして選定されます。
- パス コストに基づいて、各ネットワーク装置のルート ブリッジまでの最短距離が計算されます。
- LAN セグメントごとに指定ブリッジが選択されます。これはルート ブリッジに最も近いネットワーク装置であり、このネットワーク装置を経由してルートにフレームが転送されます。
- ルート ポートが選択されます。これはブリッジからルート ブリッジまでの最適パスを提供するポートです。
- スパニング ツリーに含まれるポートが選択されます。

ルート ブリッジの選定

VLAN ごとに、最高のブリッジ ID（数値的に最小の ID 値）を持つネットワーク装置がルート ブリッジとして選定されます。すべてのネットワーク装置がデフォルト プライオリティ（32768）に設定されている場合は、VLAN 内で最小の MAC アドレスを持つネットワーク装置がルート ブリッジになります。ブリッジ 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。

ブリッジ プライオリティ値を変更すると、スイッチがルート ブリッジとして選定される確率が変わります。大きなプライオリティ値を設定するとその確率が高くなり、小さなプライオリティ値を設定すると低くなります。

STP ルート ブリッジは、レイヤ 2 ネットワークにおけるスパニング ツリー トポロジの論理上の中心です。レイヤ 2 ネットワーク内のどの場所からも、ルート ブリッジに到達するために必要とされないパスは、すべて STP ブロッキング モードになります。

BPDU には、送信側ブリッジおよびそのポートについて、ブリッジおよび MAC アドレス、ブリッジ 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。STP はこの情報を使用してレイヤ 2 ネットワークのルート ブリッジを選定し、ルート ブリッジへのルート ポートを選定し、各レイヤ 2 セグメントの Designated Port（DP; 指定ポート）を判別します。

STP プロトコル タイマー

表 20-3 に、STP のパフォーマンスに影響する STP プロトコル タイマーを示します。

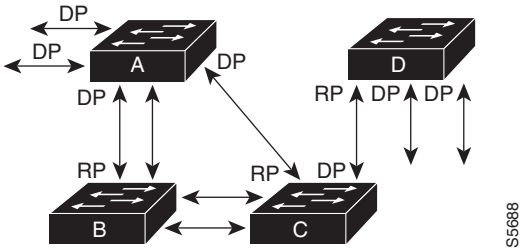
表 20-3　STP プロトコル タイマー

変数	説明
hello タイマー	ネットワーク装置から他のネットワーク装置へ hello メッセージをブロードキャストする間隔を決定します。
転送遅延タイマー	ポートが転送を開始するまでの、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決定します。
最大エージング タイマー	ポートで受信したプロトコル情報がネットワーク装置によって保管される時間を決定します。

スパニング ツリー トポロジの作成

図 20-1 では、スイッチ A がルート ブリッジに選定されます。これは、すべてのネットワーク装置でブリッジ 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です。ただし、トラフィック パターン、転送ポートの数、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 ブリッジであるとは限りません。最適なネットワーク装置がルート ブリッジになるように、装置のプライオリティを上げる（数値を下げる）ことで、ルートとして最適なネットワーク装置を使用する、新しい STP トポロジを強制的に再計算させることができます。

図 20-1　　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 トポロジをデフォルトのパラメータに基づいて計算すると、スイッチド ネットワーク上の送信元から宛先エンド ステーションまでのパスが最適にならない可能性があります。たとえば、現在のルート ポートよりも数値の大きいポートに高速リンクを接続すると、ルート ポートが変更される場合があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B の 1 つのポートが光ファイバ リンクであり、同じスイッチの別のポート（Unshielded Twisted-Pair（UTP; シールドなしツイストペア）リンク）がルート ポートになっていると仮定します。ネットワーク トラフィックを高速の光ファイバ リンクに流した方が効率的です。光ファイバ ポートの STP ポート プライオリティをルート ポートよりも上げると（数値を下げる）、光ファイバ ポートが新しいルート ポートになります。

STP ポート ステート

ここでは、STP ポート ステートについて説明します。

STP ポート ステートの概要

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変化が発生します。レイヤ 2 LAN ポートがスパニング 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可能性があります。ポートは新しいトポロジ情報がスイッチド LAN 経由で伝播されるまで待機し、それからフレーム転送を開始する必要があります。さらに、古いトポロジで転送されたフレームの存続時間を満了させることも必要です。

STP を使用する Catalyst 6500 シリーズ スイッチ上の各レイヤ 2 LAN ポートは、次の 5 種類のステートのいずれかになります。

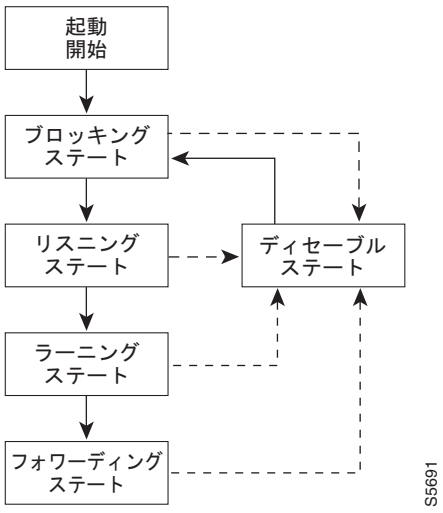
- ブロッキング：レイヤ 2 LAN ポートがフレーム転送に参加していない状態です。
- リスニング：レイヤ 2 LAN ポートがフレーム転送に参加すべきであると STP が判断した場合に、ブロッキング ステートのあとで最初に開始する移行ステートです。
- ラーニング：レイヤ 2 LAN ポートがフレーム転送に参加する準備をしている状態です。
- フォワーディング：レイヤ 2 LAN ポートはフレームを転送します。
- ディセーブル：レイヤ 2 LAN ポートが STP に参加せず、フレームを転送していない状態です。

レイヤ 2 LAN ポートは、次のように 5 種類の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 20-2 に、レイヤ 2 LAN ポートがどのように 5 種類のステートを移行するかを示します。

図 20-2　　レイヤ 2 LAN インターフェイス ステート



STP をイネーブルにすると、Catalyst 6500 シリーズ スイッチ、VLAN、およびネットワーク上のすべてのポートは、電源投入時に必ずブロッキング ステートを経て、それからリスニングおよびラーニングという移行ステートに進みます。設定が適切であれば、各レイヤ 2 LAN ポートはフォワーディング ステートまたはブロッキング ステートで安定します。

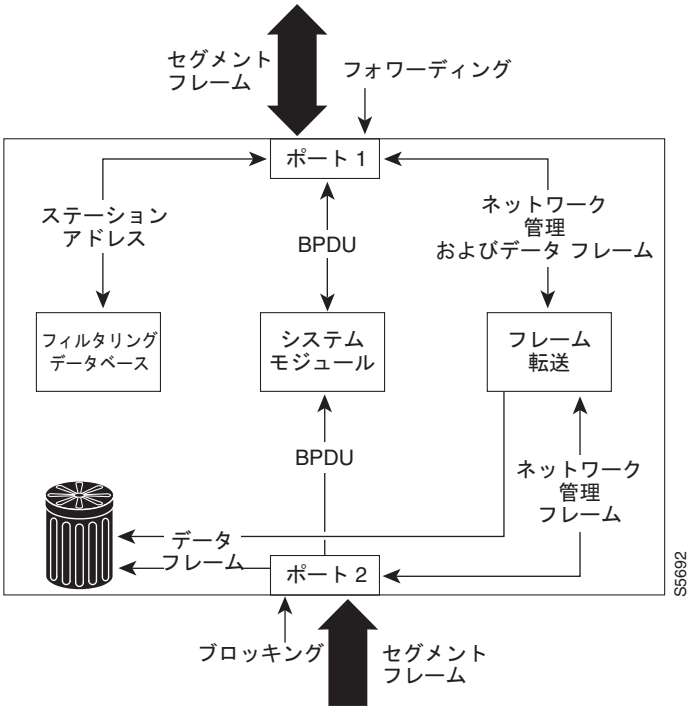
STP アルゴリズムによってレイヤ 2 LAN ポートがフォワーディング ステートになると、次の処理が行われます。

1. レイヤ 2 LAN ポートがリスニング ステートになり、ブロッキング ステートに移行するように指示するプロトコル情報を待ちます。
2. レイヤ 2 LAN ポートが転送遅延タイマーの満了を待ち、その時点でラーニング ステートになり、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、レイヤ 2 LAN ポートはフレーム転送を引き続きブロックしながら、転送データベースのエンド ステーションのロケーション情報を学習します。
4. レイヤ 2 LAN ポートは、転送遅延タイマーの終了とともにフォワーディング ステートになり、学習およびフレーム転送が両方ともイネーブルになります。

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 LAN ポートは、フレーム転送に参加しません（図 20-3 を参照）。初期化後、各レイヤ 2 LAN ポートに BPDU が送信されます。ネットワーク装置は、他のネットワーク装置と BPDU を交換するまでは、そのネットワーク装置をルートと見なします。この BPDU 交換により、ネットワーク上のどのネットワーク装置がルートまたはルート ブリッジであるかが確定します。ネットワークにネットワーク装置が 1 台しか存在しない場合は、BPDU 交換は行われず、転送遅延タイマーが終了し、ポートはリスニング ステートに移行します。初期化後、ポートは必ずブロッキング ステートになります。

図 20-3　　ブロッキング ステートのインターフェイス 2



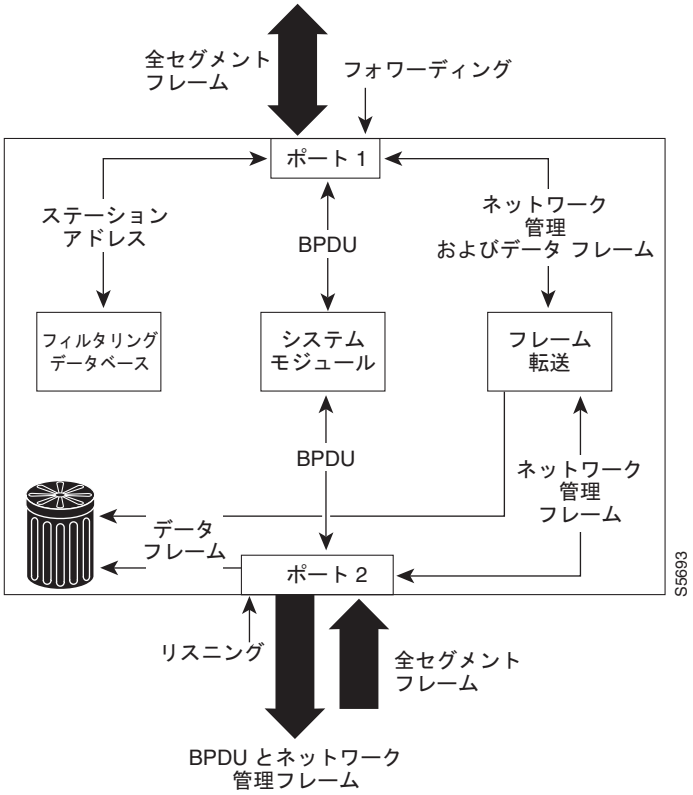
ブロッキング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポート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 データベースに、エンド ステーションのロケーション情報は組み込みません（ブロッキング状態のレイヤ 2 LAN ポートに関する学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を送信しません。
- ネットワーク管理メッセージを受信して応答します。

リスニング ステート

リスニング ステートは、レイヤ 2 LAN ポートがブロッキング ステートを経て最初に開始する移行ステートです。レイヤ 2 LAN ポートがフレーム転送に参加すべきであると STP が判断した場合に、レイヤ 2 LAN ポートはこのステートを開始します。図 20-4 に、リスニング ステートのレイヤ 2 LAN ポートを示します。

図 20-4　　リスニング ステートのインターフェイス 2



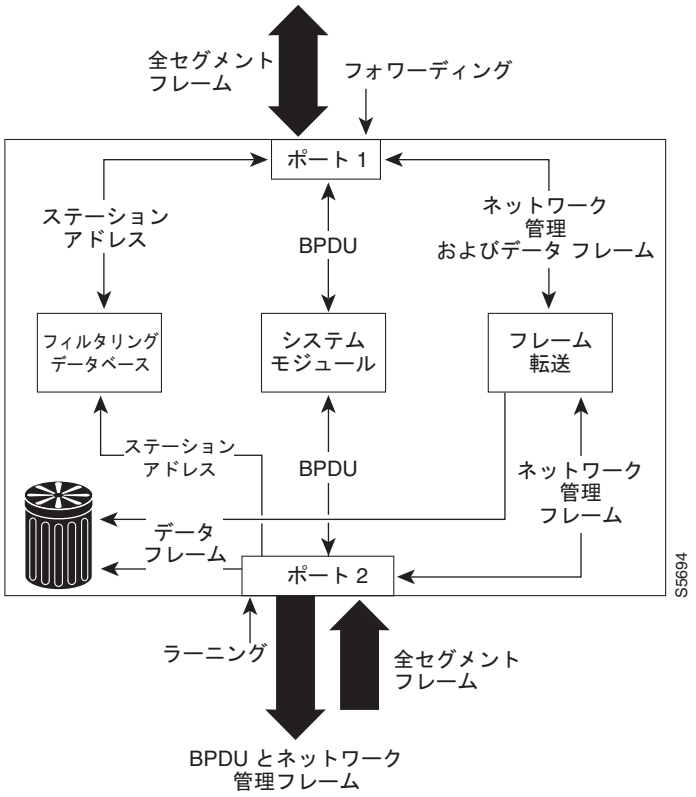
リスニング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他の LAN ポート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 データベースに、エンド ステーションのロケーション情報は組み込みません （この時点で学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

ラーニング ステート

ラーニング ステートのレイヤ 2 LAN ポートは、フレーム転送に参加するための準備を行います。レイヤ 2 LAN ポートは、リスニング ステートからラーニング ステートを開始します。図 20-5 に、ラーニング ステートのレイヤ 2 LAN ポートを示します。

図 20-5　　ラーニング ステートのインターフェイス 2



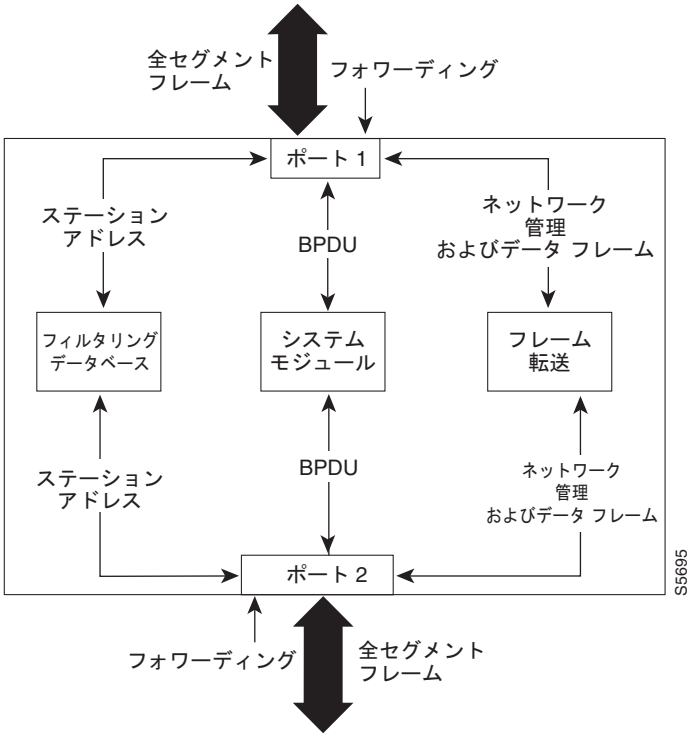
ラーニング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポートからスイッチングされたフレームを廃棄します。
- エンド ステーションのロケーション情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから送られた BPDU を受信し、処理して送信します。
- ネットワーク管理メッセージを受信して応答します。

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 LAN ポートは、フレームを転送します（図 20-6 を参照）。レイヤ 2 LAN ポートは、ラーニング ステートからフォワーディング ステートを開始します。

図 20-6　　フォワーディング ステートのインターフェイス 2



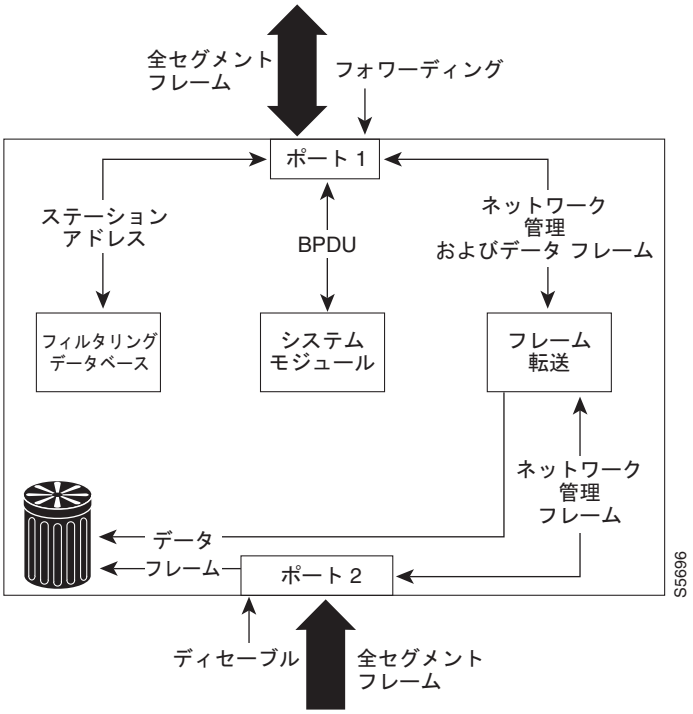
フォワーディング ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを転送します。
- 転送用に他のポートからスイッチングされたフレームを転送します。
- エンド ステーションのロケーション情報をアドレス データベースに組み込みます。
- BPDU を受信し、それをシステム モジュールに転送します。
- システム モジュールから受信した BPDU を処理します。
- ネットワーク管理メッセージを受信して応答します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 LAN ポートは、フレーム転送または STP に参加しません（図 20-7 を参照）。ディセーブル ステートのレイヤ 2 LAN ポートは事実上、動作することはありません。

図 20-7　　ディセーブル ステートのインターフェイス 2



ディセーブル ステートのレイヤ 2 LAN ポートの動作は、次のとおりです。

- 接続セグメントから受信したフレームを廃棄します。
- 転送用に他のポート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 データベースに、エンド ステーションのロケーション情報は組み込みません （学習は行われないため、アドレス データベースは更新されません）。
- BPDU を受信しません。
- システム モジュールから送信用の BPDU を受信しません。

STP および IEEE 802.1Q トランク

802.1Q トランクによって、ネットワークの STP の構築方法に、いくつかの制約が課されます。802.1Q トランクを使用して接続しているシスコのネットワーク装置では、トランク上で許容される VLAN ごとに 1 つの STP インスタンスが維持されます。しかし、他社製の 802.1Q ネットワーク装置では、トランク上で許容されるすべての VLAN に対して 1 つの STP インスタンスしか維持されません。

802.1Q トランクを使用してシスコのネットワーク装置を他社製のネットワーク装置に接続する場合、シスコのネットワーク装置は、トランクの 802.1Q VLAN の STP インスタンスを、他社製の 802.1Q ネットワーク装置のインスタンスと統合します。ただし、VLAN 別の STP 情報はすべて、他社製の 802.1Q ネットワーク装置のクラウドと切り離されて、シスコのネットワーク装置によって維持されます。シスコのネットワーク装置を隔てている他社製の 802.1Q 装置のクラウドは、ネットワーク装置間の単一トランク リンクとして処理されます。

802.1Q トランクの詳細については、第 10 章「レイヤ 2 スイッチング用 LAN ポートの設定」を参照してください。

IEEE 802.1w 高速スパニング ツリー プロトコル（RSTP）の機能概要

（注）　Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）は Rapid per VLAN Spanning Tree（Rapid PVST）モードのスタンドアロンのプロトコルとして利用できます。このモードでは、スイッチが各 VLAN で RSTP インスタンスを実行し、通常の PVST+ アプローチに従います。

ここでは、RSTP について説明します。

IEEE 802.1w RSTP の概要

RSTP を使用すると、物理トポロジまたはその設定パラメータが変更された場合に、ネットワークのアクティブなトポロジの再構成に要する時間を大幅に短縮できます。RSTP は 1 台のスイッチをスパニング ツリーで接続されたアクティブ トポロジのルートとして選定し、ポートがアクティブ トポロジ内にあるかどうかに応じて、ポート ロールをスイッチの各ポートに割り当てます。

RSTP はスイッチ、スイッチ ポート、または LAN に障害が発生したあとに、短時間で接続する機能を提供します。新しいルート ポートとブリッジの反対側の DP の間の明示的なハンドシェイクを利用して、これらのポートがフォワーディング ステートに移行します。RSTP を使用するとスイッチ ポートを設定できるため、スイッチを再初期化した場合に、ポートが直接フォワーディングに移行できます。

802.1w で指定された RSTP は、802.1D で指定された STP よりも優先しますが、STP との互換性は維持されます。

RSTP には、次のように 802.1D ブリッジとの下位互換性があります。

- RSTP は 802.1D で設定された BPDU、および Topology Change Notification（TCN; トポロジ変更通知）BPDU をポート単位で選択して送信します。
- ポートを初期化すると、移行遅延タイマーが開始され、RSTP BPDU が送信されます。移行遅延タイマーがアクティブの間、ブリッジは目的のポートで受信されたすべての BPDU を処理します。
- ポートの移行遅延タイマーの期限が切れたあとに、ブリッジが 802.1D BPDU を受信した場合、ブリッジは 802.1D ブリッジに接続されたと認識し、802.1D BPDU のみの使用を開始します。
- 移行遅延タイマーの期限が切れたあとに、RSTP がポート上で 802.1D BPDU を使用して RSTP BPDU を受信した場合、RSTP は移行遅延タイマーを再起動し、そのポート上で RSTP BPDU の使用を開始します。

RSTP のポート ロール

RSTP では、ポート ロールは次のように定義されています。

- ルート：スパニング ツリー トポロジに対して選定された転送ポート
- 指定：各スイッチド LAN セグメントに対して選定された転送ポート
- 代替：現在のルート ポートが提供するルート ブリッジへの代替パス
- バックアップ：DP が提供するパスのバックアップ（スパニング ツリーのリーフ方向）。バックアップ ポートは、2 つのポートがループバック内でポイントツーポイント リンクまたはブリッジによって接続され、共有 LAN セグメントとの複数の接続がある場合のみ、存在できます。
- ディセーブル：スパニング ツリーの動作中の役割が指定されていないポート

ポート ロールは次のように割り当てられます。

- ルート ポートまたは DP は、アクティブ トポロジにポートを追加します。
- 代替ポートまたはバックアップ ポートは、アクティブ トポロジからポートを除外します。

RSTP ポート ステート

ポート ステートはフォワーディングおよびラーニング プロセスを制御し、廃棄、ラーニング、およびフォワーディングの値を提供します 表 20-4 に、STP ポート ステートと RSTP ポート ステートの比較を示します。

表 20-4　STP と RSTP のポート ステートの比較

動作ステータス	STP ポート ステート	RSTP ポート ステート	アクティブ トポロジに含まれるポート
イネーブル	ブロッキング[1]	廃棄[2]	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

1. IEEE 802.1D のポート ステート指定。
2. IEEE 802.1w のポート ステート指定。RSTP と MST 内では廃棄はブロッキングと同じです。

安定したトポロジでは、RSTP により各ルート ポートおよび DP は必ずフォワーディングに移行し、すべての代替ポートおよびバックアップ ポートは必ず廃棄ステートになります。

Rapid PVST

Rapid PVST は既存の PVST+ 用の設定を使用します。しかしながら、Rapid PVST は RSTP を使用してより速いコンバージェンスを提供します。独立 VLAN は、独自の RSTP インスタンスを実行します。

ダイナミック エントリは、トポロジ変更を受信すると、ポート単位ですぐに消去されます。

UplinkFast および BackboneFast コンフィギュレーションは Rapid PVST モードでは無視され、両機能は RSTP に含まれます。

先行標準 IEEE 802.1s MST の機能概要

ここでは、MST について説明します。

IEEE 802.1s MST の概要

このリリースの MST は、IEEE 規格のドラフト バージョンに基づいています。MST の 802.1s は、802.1Q を改正したものです。MST は、IEEE 802.1w Rapid Spanning Tree（RST）アルゴリズムを複数のスパニング ツリーに拡張します。この拡張により、VLAN 環境で高速コンバージェンスおよびロード バランシングを実行できます。MST のコンバージェンスは、PVST+ よりも高速です。MST は 802.1D STP、802.1w（RSTP）、および Cisco PVST+ アーキテクチャと下位互換性があります。

MST を使用すると、トランク上に複数のスパニング ツリーを作成できます。VLAN をグループ化して、スパニング ツリー インスタンスに関連付けることができます。インスタンスごとに、他のスパニング ツリー インスタンスから独立しているトポロジを設定できます。この新しいアーキテクチャはデータ トラフィック用の複数の転送パスを提供し、ロード バランシングをイネーブルにします。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）には影響しないため、ネットワークのフォールトトレランスが改善されます。

大規模ネットワークでは、ネットワークパスごとに異なる VLAN およびスパニング ツリー インスタンスの割り当てを特定することにより、ネットワークの管理が容易になり、冗長パスを使用できます。スパニング ツリー インスタンスが存在できるのは、互換性のある VLAN インスタンスが割り当てられているブリッジ上のみです。同じ MST コンフィギュレーション情報によって、一連のブリッジを設定する必要があります。このようにすると、ブリッジを特定のスパニング ツリー インスタンス セットに参加させることができます。同じ MST コンフィギュレーションを持つ相互接続されたブリッジは、*MST 領域*といいます。

MST は、MSTP という名前の RSTP の改訂バージョンを使用します。MST 機能には次の特性があります。

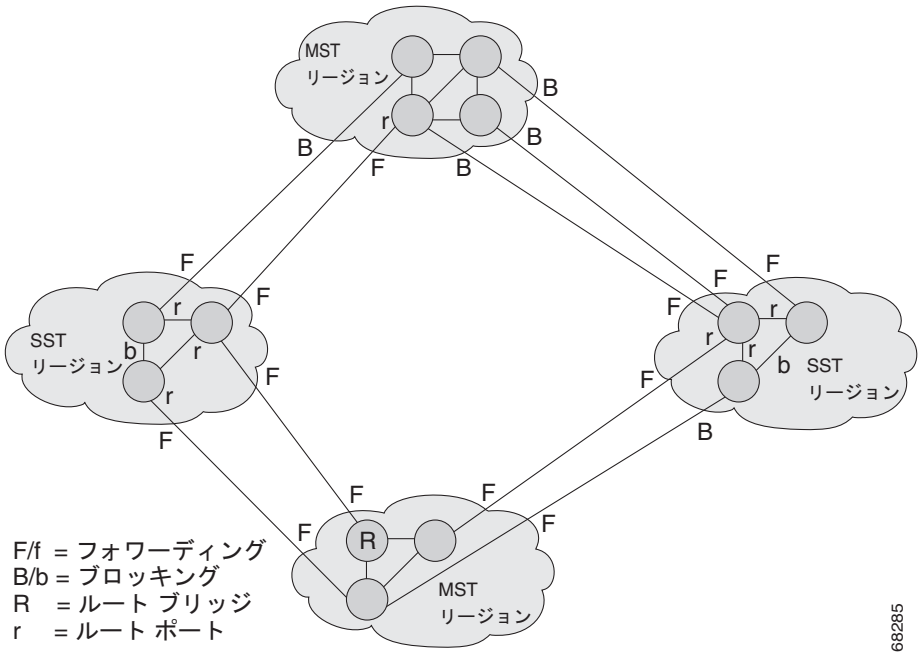
- MST は Internal Spanning Tree（IST; 内部スパニング ツリー）という名前のスパニング ツリーのバリエーションを実行します。IST は、Common Spanning Tree（CST）情報に MST 領域に関する内部情報を追加します。MST 領域は、隣接する Single Spanning Tree（SST）および MST 領域への単一のブリッジとして認識されます。
- MST が稼動しているブリッジは、次のように単一のスパニング ツリー ブリッジとのインターオペラビリティを提供します。
  - MST ブリッジは IST を実行し、IST は CST 情報に MST 領域に関する内部情報を追加します。
  - IST は領域内のすべての MST ブリッジを接続し、ブリッジ ドメイン全体を含む CST 内のサブツリーとして認識されます。MST 領域は、隣接する SST ブリッジおよび MST 領域への仮想ブリッジとして認識されます。
  - Common and Internal Spanning Tree（CIST）は各 MST 領域内の IST、MST 領域を相互接続する CST、および SST ブリッジの集まりです。CIST は MST 領域内では IST と同じであり、MST 領域外では CST と同じです。STP、RSTP、および MSTP はともに、CIST のルートとしてブリッジを 1 つ選定します。
- MST は各 MST 領域内に追加スパニング ツリーを確立し、維持します。これらのスパニング ツリーは MST Instance（MSTI; MST インスタンス）といいます。IST の番号は 0 で、MSTI の番号は 1、2、3 のようになります。MST 領域が相互接続されている場合でも、すべての MSTI は、別の領域内の MSTI から独立している MST 領域に対してローカルです。次のように、MST インスタンスは MST 領域の境界で IST と結合されて CST になります。

  MSTI のスパニング ツリー情報は、MSTP レコード（M レコード）に格納されます。M レコードは常に MST BPDU（MST BPDU）内でカプセル化されます。MSTP で計算された元のスパニング ツリーは、M ツリーといいます。M ツリーは MST 領域内でのみアクティブです。M ツリーは MST 領域の境界で IST と結合され、CST を形成します。
- MST は CST 以外の VLAN 用の PVST+ BPDU を生成して、PVST+ とのインターオペラビリティを提供します。
- MST は、次のような MSTP 内の PVST+ 拡張機能を一部サポートします。
  - UplinkFast および BackboneFast は MST モードでは使用できません。これらは RSTP の一部です。
  - PortFast はサポートされています。
  - BPDU フィルタリングおよび BPDU ガードは、MST モードではサポートされません。
  - ループ ガードおよびルート ガードは MST でサポートされています。MST は VLAN 1 でディセーブル化された機能を維持します。ただし、例外的に、BPDU は VLAN 1 内で送信されます。
  - MAC リダクションがイネーブルであるかのように、MST スイッチは動作します。
  - Private VLAN（PVLAN; プライベート VLAN）の場合、セカンダリ VLAN をプライマリと同じインスタンスにマッピングする必要があります。

MST/PVST 間のインターオペラビリティ

仮想ブリッジ接続された LAN には、SST および MST ブリッジの相互接続された領域が含まれる場合があります。図 20-8 にこの関係を示します。

図 20-8　　相互接続された SST および MST 領域を含むネットワーク



MST 領域は、SST 領域内で稼動する STP に対して、単一の SST または疑似ブリッジとして表れます。疑似ブリッジは次のように動作します。

- ルート ID およびルート パス コストと同じ値が、すべての疑似ブリッジ ポートのすべての BPDU 内で送信されます。疑似ブリッジと単一の SST ブリッジは、次の点で異なります。
  - 疑似ブリッジ BPDU には複数のブリッジ ID があります。近接する SST 領域内では、この違いが STP 動作に影響することはありません。ルート ID およびルート コストが同じであるためです。
  - 疑似ブリッジ ポートから送信された BPDU によっては、メッセージ エージが大幅に異なる場合があります。メッセージ エージは各ホップで 1 秒増加するため、メッセージ エージの差異は秒単位です。
- 疑似ブリッジの特定のポート（領域のエッジのポート）から別のポートへのデータ トラフィックは、疑似ブリッジまたは MST 領域内に完全に含まれるパスを通ります。
- 異なる VLAN に属するデータ トラフィックは、MST によって確立された MST 領域内の異なるパスを経由することがあります。
- ループ防止は次のいずれかの方法で実現します。
  - 境界上の 1 つのフォワーディング ポートを許可し、その他のすべてのポートをブロックして、適切な疑似ブリッジ ポートをブロックします。
  - SST 領域のポートをブロックするように CST パーティションを設定します。

- 疑似ブリッジのポートから送信される BPDU には異なるブリッジ ID が設定されているため、疑似ブリッジは単一の SST ブリッジと異なります。ルート ID およびルート コストは両方のブリッジで同じです。

次に示す注意事項は、PVST+ スイッチと相互作用するように MST スイッチ（すべてが同じ領域内にある）が設定されたトポロジに適用されます。

- MST 領域内のすべての VLAN のルートを、この例のように設定します。

```
Router# show spanning-tree mst interface gigabitethernet 1/1

GigabitEthernet1/1 of MST00 is root forwarding
Edge port: no             (trunk)          port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (PVST)           bpdu guard : disable     (default)
Bpdus sent 10, received 310

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Root FWD 20000     128.1    1-2,4-2999,4000-4094
3        Boun FWD 20000     128.1    3,3000-3999
```

  境界上の MST スイッチに属するポートは PVST+ をシミュレートし、すべての VLAN に PVST+ BPDU を送信します。

  PVST+ スイッチ上でループ ガードをイネーブルにした場合に、MST スイッチの設定が変更されると、ポートがループに一貫性のないステートに変更される場合があります。ループに一貫性のないステートを訂正するには、PVST+ スイッチ上でループ ガードをディセーブルにしてから再びイネーブルにする必要があります。

- MST スイッチの PVST+ 側の内部にある VLAN の一部、またはすべてのルートを特定しないでください。境界上の MST スイッチが DP 上のすべての VLAN または一部の VLAN の PVST+ BPDU を受信すると、ルート ガードによってポートがブロッキング ステートに設定されるためです。CPU の PVST+ 実行速度が遅いスイッチは、MST を実行するスイッチとして指定しないでください。

PVST+ スイッチを 2 つの異なる MST 領域に接続すると、PVST+ スイッチからのトポロジ変更が最初の MST 領域を超えて送信されることはありません。この場合、トポロジ変更の伝播先は、VLAN のマッピング先のインスタンス内に限定されます。このトポロジ変更は最初の MST 領域に対してローカルのままであり、他の領域の CAM エントリは消去されません。トポロジ変更を他の MST 領域全体で認識できるようにするには、VLAN を IST にマッピングするか、またはアクセス リンクを介して PVST+ スイッチを 2 つの領域に接続します。

CST

CST（802.1Q）はすべての VLAN に対する単一のスパニング ツリーです。PVST+ が稼動している Catalyst 6500 シリーズ スイッチでは、VLAN 1 スパニング ツリーが CST に相当します。MST が稼動している Catalyst 6500 シリーズ スイッチでは、IST（インスタンス 0）が CST に相当します。

MST インスタンス

このリリースでは、最大 16 個のインスタンスがサポートされています。各スパニング ツリー インスタンスは、0 ～ 15 のインスタンス ID で識別されます。インスタンス 0 は必須であり、常に存在します。インスタンス 1 ～ 15 は任意です。

MST コンフィギュレーション パラメータ

MST コンフィギュレーションは、次の 3 つからなります。

- 名前：MST 領域を識別する 32 個の文字列（ヌルが埋め込まれる）。
- リビジョン番号：現在の MST コンフィギュレーションのリビジョンを識別する符号なしの 16 ビットの数値。

（注）　MST コンフィギュレーションの一部として必要な場合は、リビジョン番号を設定する必要があります。MST コンフィギュレーションをコミットするたびに、リビジョン番号が自動的に増えることはありません。

- MST コンフィギュレーション テーブル：4096 バイトの配列。符号なし整数として解釈される各バイトは、VLAN に対応しています。各値は、VLAN がマッピングされているインスタンスの番号です。VLAN 0 に対応する先頭バイト、および VLAN 4095 に対応する 4096 番目のバイトは使用されません。常に 0 に設定されます。

各バイトは手動で設定する必要があります。Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）または Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、設定することができます。

MST BPDU には、MST コンフィギュレーション ID およびチェックサムが含まれます。MST BPDU のコンフィギュレーション ID およびチェックサムが自身の MST 領域のコンフィギュレーション ID およびチェックサムと一致する場合のみ、MST ブリッジは MST BPDU を受け付けます。1 つの値が異なる場合、MST BPDU は SST BPDU であると見なされます。

MST 領域

ここでは、MST 領域について説明します。

- 「MST 領域の概要」（P.20-19）
- 「境界ポート」（P.20-20）
- 「IST マスター」（P.20-20）
- 「エッジ ポート」（P.20-20）
- 「リンク タイプ」（P.20-21）

MST 領域の概要

同じ MST コンフィギュレーションを持つ相互接続されたブリッジは、MST 領域といいます。ネットワーク内の MST 領域数に制限はありません。

MST 領域を形成する場合、ブリッジは次のいずれかとなります。

- MST 領域の唯一のメンバである MST ブリッジ。
- LAN によって相互接続された MST ブリッジ。LAN の指定ブリッジの MST コンフィギュレーションは、MST ブリッジと同じです。LAN 上のすべてのブリッジは、MST BPDU を処理できます。

MST コンフィギュレーションが異なる 2 つの MST 領域を接続した場合、MST 領域は次の作業を実行します。

- ネットワーク内の冗長パス間のロード バランシングを行います。2 つの MST 領域が冗長接続されている場合、すべてのトラフィックは、ネットワーク内の MST 領域との 1 つの接続上を通過します。
- RSTP ハンドシェイクを行って、領域間の高速接続をイネーブルにします。ただし、2 つのブリッジ間に比べて、ハンドシェイク速度は低下します。ループを防止するには、領域内のすべてのブリッジが他の領域との接続に関して合意する必要があります。この場合には、遅延が発生します。ネットワークを多数の領域に分割することは推奨しません。

境界ポート

境界ポートは LAN に接続されているポートです。境界ポートの指定ブリッジは、SST ブリッジ、または異なる MST コンフィギュレーションを持つブリッジのいずれかです。DP が STP ブリッジを検出するか、またはコンフィギュレーションが異なる RST や MST ブリッジからアグリーメント メッセージを受信すると、DP は自身が境界ポート上に存在していることを認識します。

境界では、MST ポート ロールは重要ではありません。MST ポートのステートは強制的に IST ポート ステートと同じになります。ポートに境界フラグが設定されている場合、MSTP ポート ロール選択プロセスは境界にポート ロールを割り当てて、IST ポートのステートと同じステートを割り当てます。境界の IST ポートには、バックアップ用のポート ロール以外のすべてのポート ロールを設定できます。

IST マスター

MST 領域の IST マスターは、ブリッジ ID が最小で、かつ CST ルートまでのパス コストが最小であるブリッジです。MST ブリッジが CST のルート ブリッジである場合、この MST ブリッジは MST 領域の IST マスターです。CST ルートが MST 領域の外にある場合、境界にある MST ブリッジの 1 つが IST マスターとして選択されます。同じ領域に属する境界上の他のブリッジが、ルートへ続く境界ポートを最終的にブロックします。

領域の境界にある複数のブリッジのルートへのパスが同一である場合は、わずかに小さいブリッジ プライオリティを設定して、特定のブリッジを IST マスターにすることができます。

領域内のルート パス コストおよびメッセージ エージは一定ですが、ホップするごとに IST パス コストは増加し、残りの IST ホップ数は減少します。IST マスター、パス コスト、およびブリッジの残りのホップ情報を表示するには、**show spanning-tree mst** コマンドを入力します。

エッジ ポート

エッジ ポートは、非ブリッジングの装置（ホストやルータなど）に接続されたポートです。ハブまたはハブで接続されている LAN にブリッジが接続されていない場合、このハブに接続されたポートもエッジ ポートになります。エッジ ポートはリンクがアップした直後に転送を開始できます。

MST の場合は、各ホストまたはルータのすべてのポートをユーザが設定する必要があります。障害発生後に高速接続を確立するには、中間ブリッジのエッジ以外の DP をブロックする必要があります。ポートが、アグリーメントを返信できる別のブリッジに接続されている場合、ポートはすぐに転送を開始します。それ以外の場合、ポートは転送遅延時間を 2 回分待機してから、転送を再開します。MST を使用している場合は、ホストおよびルータに接続されたポートをエッジ ポートとして明示的に設定する必要があります。

設定ミスを防ぐために、ポートが BPDU を受信した場合は、PortFast 動作はオフになります。PortFast の設定および動作ステータスを表示するには、**show spanning-tree mst** *interface* コマンドを入力します。

リンク タイプ

高速接続は、ポイントツーポイント リンク上にのみ確立されます。ホストまたはルータにポートを明示的に設定する必要があります。ただし、ほとんどのネットワークのケーブル配線はこの要件を満たしています。**spanning-tree linktype** コマンドを入力して、すべての全二重リンクをポイントツーポイント リンクとして処理すると、明示的な設定を行う必要がなくなります。

メッセージ エージおよびホップ数

IST および MST インスタンスは、BPDU 内のメッセージ エージ、および最大エージング タイマーの設定を使用しません。IST および MST は IP TTL プロセスとよく似た別個のホップ カウント プロセスを使用します。MST ブリッジごとに最大ホップ数を設定できます。インスタンスのルート ブリッジは、残りのホップ数が最大ホップ数と等しい BPDU（または M レコード）を送信します。BPDU（または M レコード）を受信したブリッジは、受信した残りのホップ数を 1 減らします。ホップ数が減少して 0 になった場合、ブリッジは BPDU（M レコード）を廃棄して、ポートに保持された情報を期限切れにします。ルート以外のブリッジは、減少したホップ数を、生成された BPDU（M レコード）の残りのホップ数として伝播します。

BPDU の RST 部分のメッセージ エージおよび最大エージング タイマーの設定は、領域全体で同じままです。同じ値が、境界にある領域の DP によって伝播されます。

STP のデフォルト設定

表 20-5 に、STP のデフォルト設定を示します。

表 20-5　STP のデフォルト設定

機能	デフォルト値
イネーブル ステート	すべての VLAN でイネーブル化された STP
ブリッジ プライオリティ	32768
STP ポート プライオリティ（ポート単位で設定変更可能、レイヤ 2 アクセス ポートとして設定された LAN ポートで使用される）	128
STP ポート コスト（ポート単位で設定変更可能、レイヤ 2 アクセス ポートとして設定された LAN ポートで使用される）	• 10 ギガビット イーサネット：2 • ギガビット イーサネット：4 • ファスト イーサネット：19 • イーサネット：100
STP VLAN ポート プライオリティ（VLAN 単位で設定変更可能、レイヤ 2 トランク ポートとして設定された LAN ポートで使用される）	128
STP VLAN ポート コスト（VLAN 単位で設定変更可能、レイヤ 2 トランク ポートとして設定された LAN ポートで使用される）	• 10 ギガビット イーサネット：2 • ギガビット イーサネット：4 • ファスト イーサネット：19 • イーサネット：100
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
モード	PVST

STP と MST の設定時の注意事項および制約事項

MST を設定する際に、以下の注意事項と制約事項に従ってください。

- すべての PVST ブリッジのすべての VLAN 上のスパニング ツリーはディセーブルにしないでください。
- PVST ブリッジを CST のルートとして使用しないでください。
- すべての PVST スパニング ツリー ルート ブリッジのプライオリティが、CST ルート ブリッジよりも小さい（数値的に大きい）ことを確認してください。
- トランクが、インスタンスにマッピングされたすべての VLAN を伝送するか、このインスタンスには VLAN をまったく伝送しないことを確認してください。
- スイッチにアクセス リンクを接続しないでください。アクセス リンクによって VLAN が分割されることがあります。
- 既存または新規の論理 VLAN ポートを多数含む任意の MST コンフィギュレーションは、メンテナンス ウィンドウ内で完了する必要があります。差分変更（インスタンスへの新規 VLAN の追加やインスタンス間での VLAN の移動など）があった場合、完全な MST データベースは再初期化されるからです。

STP の設定

ここでは、VLAN 上での STP の設定手順について説明します。

- 「STP のイネーブル化」（P.20-24）
- 「拡張システム ID のイネーブル化」（P.20-25）
- 「ルート ブリッジの設定」（P.20-26）
- 「セカンダリ ルート ブリッジの設定」（P.20-27）
- 「STP ポート プライオリティの設定」（P.20-28）
- 「STP ポート コストの設定」（P.20-30）
- 「VLAN のブリッジ プライオリティの設定」（P.20-32）
- 「hello タイムの設定」（P.20-33）
- 「VLAN の転送遅延時間の設定」（P.20-33）
- 「VLAN の最大エージング タイムの設定」（P.20-34）
- 「Rapid PVST のイネーブル化」（P.20-35）

（注） この章で説明する STP コマンドは任意の LAN ポートに設定できますが、これらのコマンドが有効なのは、**switchport** キーワードを使用して設定した LAN ポートに限られます。

注意 物理的なループの存在しないトポロジであっても、スパニング ツリーをディセーブルにすることは推奨できません。スパニング ツリーは、設定およびケーブル接続の誤りに対するセーフガードの役割を果たします。VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニング ツリーをディセーブルにしないでください。

STP のイネーブル化

（注）　STP は、VLAN 1 および新たに作成されるすべての VLAN で、デフォルトでイネーブルに設定されています。

STP は、VLAN 単位でイネーブルにすることができます。Catalyst 6500 シリーズ スイッチは VLAN ごとに個別の STP インスタンスを維持します（STP をディセーブルに設定した VLAN を除きます）。

VLAN 単位で STP をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan vlan_ID`	VLAN 単位で STP をイネーブルにします。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 20-5（P.20-22）を参照）。
	`Router(config)# default spanning-tree vlan vlan_ID`	すべての STP パラメータを、指定された VLAN のデフォルト値に戻します。
	`Router(config)# no spanning-tree vlan vlan_ID`	指定された VLAN で STP をディセーブルにします。このコマンドについては、次の「注意」を参照してください。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID`	STP がイネーブルになっていることを確認します。

注意　VLAN 内のすべてのスイッチおよびブリッジでスパニング ツリーがディセーブルになっている場合以外は、VLAN 上でスパニング ツリーをディセーブルにしないでください。VLAN 内の一部のスイッチおよびブリッジでスパニング ツリーをディセーブルに設定し、同じ VLAN 内の残りのスイッチおよびブリッジではイネーブルのままにしておくことはできません。このような設定にすると、スパニング ツリーがイネーブルのスイッチおよびブリッジが、ネットワークの物理的トポロジに関して不完全な情報を得るので、予想外の結果が生じる可能性があります。

注意　物理的なループの存在しないトポロジであっても、スパニング ツリーをディセーブルにすることは推奨できません。スパニング ツリーは、設定およびケーブル接続の誤りに対するセーフガードの役割を果たします。VLAN 内に物理的なループが存在しないことを保証できる場合以外は、VLAN でスパニング ツリーをディセーブルにしないでください。

次に、VLAN 200 で STP をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

（注）　STP はデフォルトでイネーブルに設定されているので、**show running** コマンドを入力して設定の結果を表示しても、STP をイネーブルにするために入力したコマンドは表示されません。

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     00d0.00b8.14c8
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     00d0.00b8.14c8
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg FWD 200000    128.196  P2p
Fa4/5            Back BLK 200000    128.197  P2p

Router#
```

（注） VLAN 200 スパニング ツリーを作成するには、VLAN 200 にアクティブなインターフェイスが少なくとも 1 つ必要です。この例では、VLAN 200 内の 2 つのインターフェイスがアクティブです。

拡張システム ID のイネーブル化

（注） 64 個の MAC アドレスをサポートするシャーシの拡張システム ID は、常にイネーブルになっています。

1,024 個の MAC アドレスをサポートするシャーシの拡張システム ID をイネーブルにすることができます（「ブリッジ ID の概要」（P.20-3）を参照）。

拡張システム ID をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree extend system-id` `Router(config)# no spanning-tree extend system-id`	拡張システム ID をイネーブルにします。 拡張システム ID をディセーブルにします。 **（注）** 64 個の MAC アドレスをサポートするシャーシの場合、または拡張範囲 VLAN を設定した場合は、拡張システム ID をディセーブルにできません（「STP のデフォルト設定」（P.20-22）を参照）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID`	設定を確認します。

（注） 拡張システム ID をイネーブルまたはディセーブルにすると、すべてのアクティブな STP インスタンスのブリッジ ID が更新され、これによってスパニング ツリー トポロジが変更される場合があります。

次に、拡張システム ID をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree extend system-id
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary | include Extended
Extended system ID is enabled.
```

ルート ブリッジの設定

Catalyst 6500 シリーズ スイッチは、アクティブな VLAN ごとに STP のインスタンスを個別に維持します。各インスタンスには、ブリッジ プライオリティおよびブリッジの MAC アドレスで構成されるブリッジ ID が関連付けられます。VLAN ごとに、最高のブリッジ ID（数値的に最小の ID 値）を持つネットワーク装置が、その VLAN のルート ブリッジになります。

VLAN インスタンスがルート ブリッジになるように設定するには、**spanning-tree vlan** *vlan_ID* **root** コマンドを入力して、ブリッジ プライオリティをデフォルト値（32768）から非常に小さな値へと変更します。

spanning-tree vlan *vlan_ID* **root** コマンドを入力すると、スイッチは各 VLAN の現在のルート ブリッジのブリッジ プライオリティを確認します。拡張システム ID をディセーブルにすると、8192 という値でスイッチが指定された VLAN のルートになる場合、スイッチによってその VLAN のブリッジ プライオリティは 8192 に設定されます。拡張システム ID をイネーブルにすると、24576 という値でスイッチが指定された VLAN のルートになる場合、スイッチによってその VLAN のブリッジ プライオリティは 24576 に設定されます。

拡張システム ID がディセーブルで、指定された VLAN のルート ブリッジのブリッジ プライオリティが 8192 より小さい場合、スイッチはその VLAN のブリッジ プライオリティを最小のブリッジ プライオリティより 1 小さい値に設定します。

拡張システム ID がイネーブルで、指定された VLAN のルート ブリッジのブリッジ プライオリティが 24576 より小さい場合、スイッチはその VLAN のブリッジ プライオリティを最小のブリッジ プライオリティより 4096 小さい値に設定します（4096 は 4 ビット ブリッジ プライオリティの最下位ビットの値です。表 20-2（P.20-3）を参照）。

（注）　ルート ブリッジになるために必要な値が 1 より小さい場合は、**spanning-tree vlan** *vlan_ID* **root** コマンドは機能しません。

spanning-tree vlan *vlan_ID* **root** コマンドは次の影響を及ぼす可能性があります。

- 拡張システム ID がディセーブルで、VLAN 100 のすべてのネットワーク装置にデフォルト プライオリティ 32768 が設定されている場合に、スイッチ上で **spanning-tree vlan 100 root primary** コマンドを入力すると、VLAN 100 のブリッジ プライオリティが 8192 に設定され、そのスイッチが VLAN 100 のルート ブリッジになります。
- 拡張システム ID がイネーブルで、VLAN 20 のすべてのネットワーク装置にデフォルト プライオリティ 32768 が設定されている場合に、スイッチ上で **spanning-tree vlan 20 root primary** コマンドを使用すると、ブリッジ プライオリティが 24576 に設定され、そのスイッチが VLAN 20 のルート ブリッジになります。

注意　STP の各インスタンスのルート ブリッジは、バックボーン スイッチまたはディストリビューション スイッチでなければなりません。アクセス スイッチを STP 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（レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間における最大ブリッジ ホップ数）を指定するには、**diameter** キーワードを指定します。ネットワーク直径を指定すると、Catalyst 6500 シリーズ スイッチはその直径を持つネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムを自動的に選びます。その結果、STP のコンバージェンスに要する時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。

（注）　STP トポロジを安定した状態に保つには、Catalyst 6500 シリーズ スイッチをルート ブリッジとして設定したあと、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しないでください。

Catalyst 6500 シリーズ スイッチをルート ブリッジとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan vlan_ID root primary [diameter hops [hello-time seconds]]`	Catalyst 6500 シリーズ スイッチをルート ブリッジとして設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 20-5（P.20-22）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID root`	ルート ブリッジ コンフィギュレーションを消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、Catalyst 6500 シリーズ スイッチを VLAN 10 のルート ブリッジとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# end
Router#
```

セカンダリ ルート ブリッジの設定

Catalyst 6500 シリーズ スイッチをセカンダリ ルートとして設定すると、STP ブリッジ プライオリティはデフォルト値（32768）から変更されます。その結果、プライマリ ルート ブリッジに障害が発生した場合に（ネットワーク上の他のネットワーク装置がデフォルトのブリッジ プライオリティ 32768 を使用していると仮定して）、このスイッチが指定された VLAN のルート ブリッジになる可能性が高くなります。

拡張システム ID がイネーブルの場合、STP はブリッジ プライオリティを 28672 に設定します。拡張システム ID がディセーブルの場合は、16384 に設定します。

このコマンドを複数の Catalyst 6500 シリーズ スイッチに対して実行すると、複数のバックアップ ルート ブリッジを設定できます。プライマリ ルート ブリッジを設定するときに使用したものと同じネットワーク直径および hello タイムを使用してください。

Catalyst 6500 シリーズ スイッチをセカンダリ ルート ブリッジとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# [no] spanning-tree vlan vlan_ID root secondary [diameter hops [hello-time seconds]]`	Catalyst 6500 シリーズ スイッチをセカンダリ ルート ブリッジとして設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID root`	ルート ブリッジ設定を消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、Catalyst 6500 シリーズ スイッチを VLAN 10 のセカンダリ ルート ブリッジとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)# end
Router#
```

STP ポート プライオリティの設定

ループが発生すると、STP はポート プライオリティを考慮して、フォワーディング ステートにする LAN ポートを選択します。STP に最初に選択させたい LAN ポートには高いプライオリティ値を、最後に選択させたい LAN ポートには低いプライオリティ値を割り当てることができます。すべての LAN ポートが同じプライオリティ値を使用している場合には、STP は LAN ポート番号が最も小さい LAN ポートをフォワーディング ステートにして、残りの LAN ポートをブロックします。指定できるプライオリティの範囲は 0 ～ 240 であり（デフォルトは 128）、16 単位で設定できます。

LAN ポートがトランク ポートとして設定されている場合は、トランクによって伝送される各 VLAN に異なるポート プライオリティを設定できます。VLAN ポート プライオリティが設定されていない VLAN では、デフォルトでスパニング ツリー ポート プライオリティが使用されます。アクセス ポートの VLAN ポート プライオリティを設定しないでください。

レイヤ 2 LAN インターフェイスの STP ポート プライオリティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {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 2	`Router(config-if)# spanning-tree port-priority port_priority`	LAN インターフェイスのポート プライオリティを設定します。指定できる *port_priority* 値の範囲は 16 単位で、0 ～ 240 です。
	`Router(config-if)# no spanning-tree port-priority`	デフォルトのポート プライオリティ値に戻します。

	コマンド	目的
ステップ 3	`Router(config-if)# spanning-tree vlan vlan_ID port-priority port_priority`	LAN インターフェイスの VLAN ポート プライオリティを設定します。指定できる *port_priority* 値の範囲は 16 単位で、0 ～ 240 です。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1 (P.14-2) を参照）。
	`Router(config-if)# [no] spanning-tree vlan vlan_ID port-priority`	デフォルトの VLAN ポート プライオリティ値に戻します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show spanning-tree interface {type[1] slot/port} | {port-channel port_channel_number}` `Router# show spanning-tree vlan vlan_ID`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 4/4 の STP ポート プライオリティを設定する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 4/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

次に、ファスト イーサネット ポート 4/4 の設定を確認する例を示します。

```
Router# show spanning-tree interface fastethernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0198         Back BLK 200000    160.196  P2p
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Back BLK 200000    160.196  P2p
Router#
```

ファスト イーサネット 4/4 はトランクです。この例のように、複数の VLAN が設定され、アクティブになっています。ポート プライオリティ設定は、この VLAN インターフェイス上のすべての VLAN に適用されます。

（注）　**show spanning-tree interface** コマンドで情報が表示されるのは、ポートが接続され動作している場合に限られます。これらの条件が満たされていない場合は、**show running-config interface** コマンドを使用して設定を確認してください。

次に、ファスト イーサネット ポート 4/4 の VLAN ポート プライオリティを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# ^Z
Router#
```

この例で入力した設定は VLAN 200 にだけ適用されます。200 以外のすべての VLAN のポート プライオリティは 160 のままです

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface fastethernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Desg FWD 200000     64.196  P2p

Router#
```

VLAN 200 のスパニング ツリー情報を表示するには、次のコマンドを使用します。

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg LRN 200000     64.196  P2p
```

STP ポート コストの設定

STP ポート パス コストのデフォルト値は、LAN インターフェイスのメディア速度から決定されます。ループが発生すると、STP はポート コストを考慮して、フォワーディング ステートにする LAN インターフェイスを選択します。STP に最初に選択させたい LAN インターフェイスには低いコスト値を、最後に選択させたい LAN インターフェイスには高いコスト値を割り当てることができます。すべての LAN インターフェイスが同じコスト値を使用している場合には、STP は LAN インターフェイス番号が最も小さい LAN インターフェイスをフォワーディング ステートにして、残りの LAN インターフェイスをブロックします。指定できるコストの範囲は、0 ～ 200000000 です（デフォルトは、メディアによって異なります）。

STP は LAN インターフェイスがアクセス ポートとして設定されている場合にはポート コスト値を使用し、LAN 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場合には VLAN ポート コスト値を使用します。

レイヤ 2 LAN インターフェイスの STP ポート コストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {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 2	`Router(config-if)# spanning-tree cost port_cost`	LAN インターフェイスのポート コストを設定します。*port_cost* 値は、1 ～ 200000000（Release 12.1(2)E 以前のリリースの場合は 1 ～ 65535）の範囲で指定します。
	`Router(config-if)# no spanning-tree cost`	デフォルトのポート コストに戻します。
ステップ 3	`Router(config-if)# [no] spanning-tree vlan vlan_ID cost port_cost`	LAN インターフェイスの VLAN ポート コストを設定します。*port_cost* 値は、1 ～ 200000000 の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
ステップ 4	`Router(config-if)# no spanning-tree vlan vlan_ID cost`	デフォルトの VLAN ポート コストに戻します。
ステップ 5	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show spanning-tree interface {type[1] slot/port} | {port-channel port_channel_number}` `show spanning-tree vlan vlan_ID`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 4/4 の STP ポート コストを変更する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# ^Z
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface fastEthernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 1000      160.196  P2p
VLAN0006         Back BLK 1000      160.196  P2p
VLAN0007         Back BLK 1000      160.196  P2p
VLAN0008         Back BLK 1000      160.196  P2p
VLAN0009         Back BLK 1000      160.196  P2p
VLAN0010         Back BLK 1000      160.196  P2p
Router#
```

次に、VLAN 200 の各ポート VLAN コストにポート プライオリティを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# ^Z
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg FWD 2000       64.196  P2p
```

（注） 他の VLAN（VLAN 1 など）では次に示す出力は、この設定の影響を受けていません。

```
Router# show spanning-tree vlan 1 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Router#
```

（注） **show spanning-tree** 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ステートで、かつ DTP 用に正しく設定されている場合に限られます。これらの条件が満たされていない場合は、**show running-config** コマンドを入力して設定を確認してください。

VLAN のブリッジ プライオリティの設定

（注）　このコマンドは、慎重に使用してください。ブリッジ プライオリティを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan_ID* **root primary** コマンドおよび **spanning-tree vlan** *vlan_ID* **root secondary** コマンドを使用することを推奨します。

拡張システム ID がディセーブルの場合に、VLAN の STP ブリッジ プライオリティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan vlan_ID priority bridge_priority`	拡張システム ID がディセーブルの場合に、VLAN のブリッジ プライオリティを設定します。*bridge_priority* 値は、1 ～ 65535 の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID priority`	デフォルトのブリッジ プライオリティ値に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID bridge [detail]`	設定を確認します。

拡張システム ID がイネーブルの場合に、VLAN の STP ブリッジ プライオリティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# [no] spanning-tree vlan vlan_ID priority {0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440}`	拡張システム ID がイネーブルの場合に、VLAN のブリッジ プライオリティを設定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID priority`	デフォルトのブリッジ プライオリティ値に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID bridge [detail]`	設定を確認します。

次に、拡張システム ID がディセーブルの場合に、VLAN 200 のブリッジ プライオリティを 33792 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 priority 33792
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                        Hello Max  Fwd
Vlan                 Bridge ID          Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          33792 0050.3e8d.64c8    2   20    15  ieee
Router#
```

hello タイムの設定

（注）　このコマンドは、慎重に使用してください。hello タイムを変更するには、ほとんどの状況で **spanning-tree vlan** *vlan_ID* **root primary** コマンドおよび **spanning-tree vlan** *vlan_ID* **root secondary** コマンドを使用することを推奨します。

VLAN の STP hello タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan` *vlan_ID* **hello-time** *hello_time*	VLAN の hello タイムを設定します。*hello_time* 値は、1 ～ 10 秒の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan` *vlan_ID* **hello-time**	デフォルトの hello タイムに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan` *vlan_ID* **bridge** [**detail**]	設定を確認します。

次に、VLAN 200 の hello タイムを 7 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                        Hello Max  Fwd
Vlan                 Bridge ID          Time  Age Delay  Protocol
---------------- --------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    7   20    15  ieee
Router#
```

VLAN の転送遅延時間の設定

VLAN の STP 転送遅延時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan` *vlan_ID* **forward-time** *forward_time*	VLAN の転送時間を設定します。*forward_time* 値は、4 ～ 30 秒の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan` *vlan_ID* **forward-time**	デフォルトの転送時間に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan` *vlan_ID* **bridge** [**detail**]	設定を確認します。

次に、VLAN 200 の転送遅延時間を 21 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                     Hello Max  Fwd
Vlan                 Bridge ID       Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   20    21  ieee
Router#
```

VLAN の最大エージング タイムの設定

VLAN の STP 最大エージング タイムを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree vlan vlan_ID max-age max_age`	VLAN の最大エージング タイムを設定します。*max_age* 値は、6 ～ 40 秒の範囲で指定します。*vlan_ID* の値は 1 ～ 4094 です（予約済み VLAN は除く。表 14-1（P.14-2）を参照）。
	`Router(config)# no spanning-tree vlan vlan_ID max-age`	デフォルトの最大エージング タイムに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID bridge [detail]`	設定を確認します。

次に、VLAN 200 の最大エージング タイムを 36 秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 bridge
                                     Hello Max  Fwd
Vlan                 Bridge ID       Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   36    15  ieee
Router#
```

Rapid PVST のイネーブル化

Rapid PVST は、既存の PVST+ フレームワークを設定や他の機能との相互通信に利用します。また、PVST+ 拡張機能も一部サポートします。

スイッチの Rapid PVST モードをイネーブルにするには、イネーブルモードで **spanning-tree mode rapid-pvst** コマンドを入力します。Rapid PVST モードでスイッチを設定するには、「STP の設定」（P.20-23）を参照してください。

リンク タイプの指定

高速接続は、ポイントツーポイント リンク上にのみ確立されます。スパニング ツリーはポイントツーポイント リンクを、スパニング ツリー アルゴリズムを実行する 2 つのスイッチのみを接続するセグメントとして見なします。スイッチは、すべての全二重リンクはポイントツーポイント リンクで、半二重リンクは共有リンクであると仮定するので、明示的にリンク タイプの設定を避けることができます。特定のリンク タイプを設定するには、**spanning-tree linktype** コマンドを入力します。

プロトコル移行の再起動

MSTP と RSTP の両方を実行する スイッチは、スイッチをレガシー 802.1D スイッチと相互運用できるようにする内蔵プロトコル移行プロセスをサポートします。このスイッチは、レガシー 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、そのポートの 802.1D BPDU のみを送信します。MSTP スイッチは、レガシー BPDU、異なる領域と関連する MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることも検出できます。

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判断できないので、スイッチはこれ以上 802.1D BPDU を受け取らない場合でも、自動的に MSTP モードに戻りません。スイッチは、接続されているスイッチがその領域に加入している場合、ポートに境界の役割を割り当て続ける可能性もあります。

スイッチ全体で、プロトコル移行プロセスを再開するには（近接スイッチと強制的に再ネゴシエーションする）、**clear spanning-tree detected-protocols** イネーブル EXEC コマンドを使用できます。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* イネーブル EXEC コマンドを入力します。

先行標準 IEEE 802.1s MST の設定

Release 12.2SX は MST をサポートしています。ここでは、MST の設定手順について説明します。

MST のイネーブル化

MST をイネーブルにし、設定するには、イネーブル モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show spanning-tree mst configuration`	現在の MST の設定を表示します。
ステップ 2	`Router(config)# spanning-tree mode mst`	MST モードを設定します。
ステップ 3	`Router(config)# spanning-tree mst configuration`	MST のコンフィギュレーション サブモードを開始して、MST 領域を設定します。
	`Router(config)# no spanning-tree mst configuration`	MST の設定を消去します。
ステップ 4	`Router(config-mst)# show current`	MST コンフィギュレーション サブモードから、現在の MST の設定を表示します。
ステップ 5	`Router(config-mst)# name` *name* `revision` *revision_number* `instance` *instance_number* `vlan` *vlan_range*	MST の設定を開始します。
ステップ 6	`Router(config-mst)# no instance` *instance_number*	（任意）インスタンスにマッピングされている VLAN のマッピングをすべて解除します。
ステップ 7	`Router(config-mst)# no instance` *instance_number* `vlan` *vlan_number*	（任意）インスタンスから特定の VLAN のマッピングを解除します。
ステップ 8	`Router(config-mst)# end`	設定を適用して、コンフィギュレーション モードを終了します。
ステップ 9	`Router# show spanning-tree mst config`	グローバル コンフィギュレーション モードから、MST の設定を表示します。

次に、MST をイネーブルにする例を示します。

```
Router# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree mode mst

Router(config)# spanning-tree mst configuration

Router(config-mst)# show current
Current MST configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
Router(config-mst)# name cisco
Router(config-mst)# revision 2
Router(config-mst)# instance 1 vlan 1
Router(config-mst)# instance 2 vlan 1-1000
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1001-4094
2         1-1000
---------------------------------------------------------------------------
Router(config-mst)# no instance 2
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
Router(config-mst)# instance 1 vlan 2000-3000
Router(config-mst)# no instance 1 vlan 2500
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-1999,2500,3001-4094
1         2000-2499,2501-3000
---------------------------------------------------------------------------
Router(config)# exit
Router(config)# no spanning-tree mst configuration
Router(config)# do show spanning-tree mst configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
---------------------------------------------------------------------------
```

MST の設定の表示

MST の設定を表示するには、MST モードで次の作業を行います。

	コマンド	目的
ステップ 1	Router# **show spanning-tree mst configuration**	アクティブな設定を表示します。
ステップ 2	Router# **show spanning-tree mst** [**detail**]	現在動作中の MST インスタンスに関する情報を表示します。
ステップ 3	Router# **show spanning-tree mst** *instance-id* [*detail*]	特定の MST インスタンスに関する情報を表示します。
ステップ 4	Router# **show spanning-tree mst interface** *interface name* [*detail*]	特定のポートの情報を表示します。
ステップ 5	Router# **show spanning-tree mst** *number* **interface** *interface name* [**detail**]	特定のポートおよび特定のインスタンスの MST 情報を表示します。
ステップ 6	Router# **show spanning-tree mst** [*x*] [*interface Y*] *detail*	MST の詳細を表示します。
ステップ 7	Router# **show spanning-tree vlan** *vlan_ID*	MST モードで VLAN 情報を表示します。

次に、MST モードでスパニング ツリー VLAN 設定を表示する例を示します。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 1-10
Router(config-mst)# name cisco
Router(config-mst)# revision 1
Router(config-mst)# ^Z

Router# show spanning-tree mst configuration
Name      [cisco]
Revision  1
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         11-4094
1         1-10
-------------------------------------------------------------------------------

Router# show spanning-tree mst

###### MST00        vlans mapped:  11-4094
Bridge      address 00d0.00b8.1400  priority  32768 (32768 sysid 0)
Root        address 00d0.004a.3c1c  priority  32768 (32768 sysid 0)
            port    Fa4/48          path cost 203100
IST master  this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Root FWD 200000    128.240  P2p Bound(STP)

###### MST01        vlans mapped:  1-10
Bridge      address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root        this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
```

```
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)


Router# show spanning-tree mst 1

###### MST01        vlans mapped:  1-10
Bridge      address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root        this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)

Router# show spanning-tree mst interface fastEthernet 4/4

FastEthernet4/4 of MST00 is backup blocking
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus sent 2, received 368

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- ------------------------------
0        Back BLK 1000      160.196  11-4094
1        Back BLK 1000      160.196  1-10

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus (MRecords) sent 2, received 364

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- ------------------------------
1        Back BLK 1000      160.196  1-10

Router# show spanning-tree mst 1 detail

###### MST01        vlans mapped:  1-10
Bridge      address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root        this switch for MST01

FastEthernet4/4 of MST01 is backup blocking
Port info             port id        160.196  priority    160  cost        1000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.197
Timers:message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 123, received 1188

FastEthernet4/5 of MST01 is designated forwarding
Port info             port id        128.197  priority    128  cost      200000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.197
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1188, received 123
```

```
FastEthernet4/48 of MST01 is boundary forwarding
Port info             port id        128.240  priority    128  cost      200000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.240
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 78, received 0

Router# show spanning-tree vlan 10

MST01
  Spanning tree enabled protocol mstp
  Root ID    Priority    32769
             Address     00d0.00b8.1400
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00d0.00b8.1400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p

Router# show spanning-tree summary
Root bridge for:MST01
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
MST00                     1        0         0        2          3
MST01                     1        0         0        2          3
---------------------- -------- --------- -------- ---------- ----------
2 msts                    2        0         0        4          6
Router#
```

MST インスタンス パラメータの設定

MST インスタンス パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree mst X priority Y`	MST インスタンスのプライオリティを設定します。
ステップ 2	`Router(config)# spanning-tree mst X root [primary | secondary]`	ブリッジを MST インスタンスのルートとして設定します。
ステップ 3	`Router# show spanning-tree mst`	設定を確認します。

次に、MST インスタンス パラメータを設定する例を示します。

```
Router(config)# spanning-tree mst 1 priority ?
  <0-61440>  bridge priority in increments of 4096

Router(config)# spanning-tree mst 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440

Router(config)# spanning-tree mst 1 priority 49152
Router(config)#

Router(config)# spanning-tree mst 0 root primary
 mst 0 bridge priority set to 24576
 mst bridge max aging time unchanged at 20
 mst bridge hello time unchanged at 2
 mst bridge forward delay unchanged at 15
Router(config)# ^Z
Router#

Router# show spanning-tree mst

###### MST00        vlans mapped:  11-4094
Bridge      address 00d0.00b8.1400  priority  24576 (24576 sysid 0)
Root        this switch for CST and IST
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Desg FWD 200000    128.240  P2p Bound(STP)

###### MST01        vlans mapped:  1-10
Bridge      address 00d0.00b8.1400  priority  49153 (49152 sysid 1)
Root        this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)

Router#
```

MST インスタンス ポートのパラメータの設定

MST インスタンス ポートのパラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# spanning-tree mst x cost y`	MST インスタンス ポートのコストを設定します。
ステップ 2	`Router(config-if)# spanning-tree mst x port-priority y`	MST インスタンス ポートのプライオリティを設定します。
ステップ 3	`Router# show spanning-tree mst x interface y`	設定を確認します。

次に、MST インスタンス ポートのパラメータを設定する例を示します。

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree mst 1 ?
  cost           Change the interface spanning tree path cost for an instance
  port-priority  Change the spanning tree port priority for an instance

Router(config-if)# spanning-tree mst 1 cost 1234567
Router(config-if)# spanning-tree mst 1 port-priority 240
Router(config-if)# ^Z

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus (MRecords) sent 125, received 1782

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
1        Back BLK 1234567   240.196  1-10

Router#
```

プロトコル移行の再起動

MSTP と RSTP の両方を実行するスイッチは、スイッチをレガシー 802.1D スイッチと相互運用できるようにする内蔵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 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、そのポートの 802.1D BPDU のみを送信します。MSTP スイッチは、レガシー BPDU、異なる領域と関連する MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信するときに、ポートが領域の境界にあることも検出できます。

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判断できないので、スイッチはこれ以上 802.1D BPDU を受け取らない場合でも、自動的に MSTP モードに戻りません。スイッチは、接続されているスイッチがその領域に加入している場合、ポートに境界の役割を割り当て続ける可能性もあります。

スイッチ全体で、プロトコル移行プロセスを再開するには（近接スイッチと強制的に再ネゴシエーションする）、**clear spanning-tree detected-protocols** イネーブル EXEC コマンドを使用できます。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* イネーブル EXEC コマンドを入力します。

次に、プロトコル移行を再起動する例を示します。

```
Router# clear spanning-tree detected-protocols interface fastEthernet 4/4
Router#
```

CHAPTER 21

オプションのスパニング ツリー プロトコル（STP）機能の設定

この章では、オプションの Spanning Tree Protocol（STP; スパニング ツリー プロトコル）機能を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

（注） STP の設定手順については、第 20 章「スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定」を参照してください。

PortFast の機能概要

STP PortFast を使用すると、アクセス ポートとして設定されたレイヤ 2 LAN ポートが、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、ただちにフォワーディング ステートを開始します。1 台のワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上で PortFast を使用すると、STP のコンバージェンスを待たずに、装置がただちにネットワークに接続されます。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。PortFast 用に設定されているポートでも、STP は稼動しています。PortFast 対応ポートは、必要に応じて、ブロッキング ステートにただちに移行できます（これは、上位 BPDU を受信したときに発生することがあります）。トランク ポート上で PortFast をイネーブルにできます。PortFast には、設定値と異なる動作値を設定できます。

注意　PortFast の目的は、アクセス ポートが STP のコンバージェンスを待つ時間を最小限に抑えることです。したがって、PortFast はアクセス ポート上でのみ使用する必要があります。スイッチに接続されたポート上で PortFast をイネーブルにすると、一時的なブリッジング ループが発生するおそれがあります。

BPDU ガードの機能概要

BPDU ガードがポート上でイネーブルになっている場合、BPDU ガードは BPDU を受信するポートをシャットダウンします。BPDU ガードがグローバルに設定されている場合は、BPDU ガードは PortFast 動作ステートのポート上でのみ有効です。有効な設定では、PortFast レイヤ 2 LAN インターフェイスは BPDU を受信しません。PortFast レイヤ 2 LAN インターフェイスが BPDU を受信した場合、許可されていない装置が接続された場合と同じように、無効な設定として通知されます。このように BPDU ガード機能では、管理者が手動でレイヤ 2 LAN インターフェイスを再び作動させなければならないので、無効な設定に対する安全な対処が可能になります。BPDU ガードはインターフェイス レベルで設定可能です。インターフェイス レベルで設定された BPDU ガードは、PortFast 設定に関係なく、ポートが BPDU を受信するとすぐにポートをシャットダウンします。

（注）　グローバルにイネーブル化された BPDU ガードは、PortFast 動作ステートのすべてのインターフェイスに適用されます。

PortFast BPDU フィルタリングの機能概要

PortFast BPDU フィルタリングを使うことで、管理者は特定ポート上での BPDU 送信や BPDU 受信をシステムで禁止することができます。

グローバルに設定された PortFast BPDU フィルタリングは、動作中のすべての PortFast ポートに適用されます。PortFast 動作ステートのポートは、ホストに接続されていると見なされ、通常 BPDU を廃棄します。動作中の PortFast ポートが BPDU を受信すると、ポートはすぐに PortFast 動作ステータスを失います。この場合、PortFast BPDU フィルタリングはこのポート上でディセーブルになり、STP はポート上で BPDU の送信を再開します。

PortFast BPDU フィルタリングはポート単位で設定することもできます。PortFast BPDU フィルタリングがポート上で明示的に設定されている場合、BPDU は送信されず、受信したすべての BPDU は廃棄されます。

注意　ホストに接続されていないポートに PortFast BPDU フィルタリングを設定すると、ブリッジング ループが発生することがあります。

PortFast BPDU フィルタリングをグローバルにイネーブルにし、ポート設定を PortFast BPDU フィルタリングのデフォルトに設定すると（「PortFast BPDU フィルタリングのイネーブル化」（P.21-11）を参照）、PortFast は PortFast BPDU フィルタリングをイネーブルまたはディセーブルにします。

ポート設定がデフォルトに設定されていない場合、PortFast 設定は PortFast BPDU フィルタリングに影響しません。表 21-1 に、使用可能な PortFast BPDU フィルタリングの組み合わせを示します。PortFast BPDU フィルタリングを使用すると、エンド ホストの接続直後に、アクセス ポートがフォワーディング ステートに直接移行できます。

表 21-1　PortFast BPDU フィルタリングのポート設定

ポート単位の設定	グローバル コンフィギュレーション	PortFast のステート	PortFast BPDU フィルタリングのステート
デフォルト	イネーブル	イネーブル	イネーブル[1]
デフォルト	イネーブル	ディセーブル	ディセーブル
デフォルト	ディセーブル	適用不可	ディセーブル
ディセーブル	適用不可	適用不可	ディセーブル
イネーブル	適用不可	適用不可	イネーブル

1. ポートは 10 以上の BPDU を送信します。このポートがいずれかの BPDU を受信した場合、PortFast および PortFast BPDU フィルタリングはディセーブルになります。

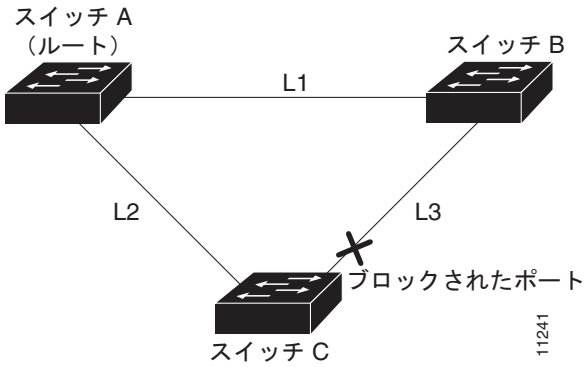
UplinkFast の機能概要

UplinkFast は、直接接続されたリンクの障害発生後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、（Virtual LAN（VLAN; 仮想 LAN）ごとの）レイヤ 2 LAN インターフェイスの集合であり、どの時点でも、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。つまり、アップリンク グループは、（転送を行う）ルート ポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

（注）　UplinkFast は、配線クローゼット スイッチに使用すると最も効果的です。それ以外の用途には、この機能は有用でない場合もあります。

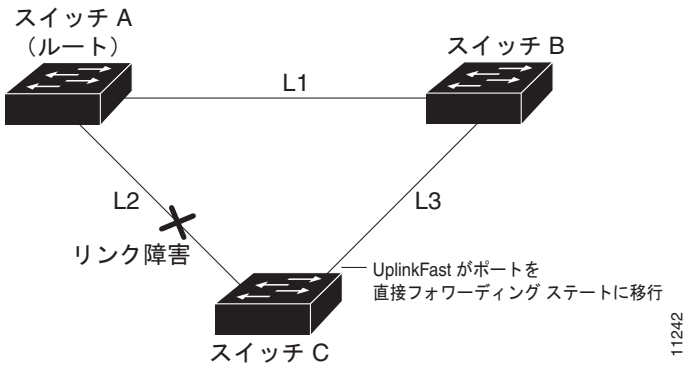
図 21-1 は、リンク障害が発生していないときのトポロジ例です。スイッチ A（ルート ブリッジ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 LAN インターフェイスは、ブロッキング ステートです。

図 21-1　　直接リンク障害が発生する前の UplinkFast の例



スイッチ C が、現在アクティブ リンクであるルート ポート上の L2 でリンク障害（*直接*リンク障害）を検出すると、UplinkFast はスイッチ C でブロックされていたポート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、ただちにフォワーディング ステートに移行させます（図 21-2 を参照）。このスイッチ オーバーに要する時間は 1 ～ 5 秒です。

図 21-2　　直接リンク障害が発生したあとの UplinkFast の例



BackboneFast の機能概要

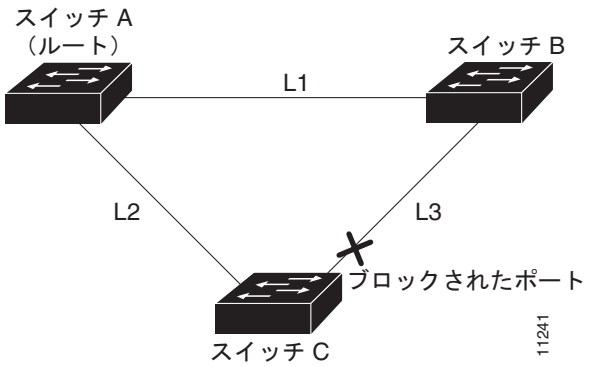
ネットワーク装置上のルート ポートまたはブロックされたポートが、そのポートの指定ブリッジから下位 BPDU を受信すると、BackboneFast が開始されます。下位 BPDU により、1 台のネットワーク装置をルート ブリッジおよび指定ブリッジの両方として識別します。ネットワーク装置が下位 BPDU を受信すると、ネットワーク装置はそのネットワーク装置が直接接続されていないリンク（*間接*リンク）で障害が発生した（つまり、指定ブリッジからルート ブリッジへの接続が切断された）ものと見なします。標準的な STP ルールに従う場合、ネットワーク装置は設定されている最大エージング タイム（STP の **max-age** コマンドで指定）の間下位 BPDU を無視します。

ネットワーク装置は、ルート ブリッジへの代替パスの有無を判別します。下位 BPDU がブロックされたポートに到達した場合には、ネットワーク装置のルート ポートおよびその他のブロックされたポートがルート ブリッジへの代替パスになります（セルフループ ポートはルート ブリッジ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には、すべてのブロック ポートがルート ブリッジ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、かつブロックされたポートがない場合には、ネットワーク装置はルート ブリッジへの接続が切断されたものと見なし、ルートの最大エージング タイムを満了させ、通常の STP ルールに従ってルート ブリッジになります。

ネットワーク装置にルート ブリッジへの代替パスがある場合、ネットワーク装置はそれらの代替パスを使用して、ルート リンク クエリー Protocol Data Unit（PDU; プロトコル データ ユニット）と呼ばれる新しい種類の PDU を送信します。ネットワーク装置はルート ブリッジへのすべての代替パスに対して、ルート リンク クエリー PDU を送信します。ルートへの代替パスがまだ存在していることが判明すると、ネットワーク装置は、下位 BPDU を受信したポートの最大エージング タイムを満了させます。ルート ブリッジへのすべての代替パスが、ネットワーク装置とルート ブリッジ間の接続が切断されていることを示している場合には、ネットワーク装置は、下位 BPDU を受信したポートの最大エージング 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 ブリッジに引き続き接続できる場合には、ネットワーク装置は、下位 BPDU を受信したすべてのポートを Designated Port（DP; 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 ステートから、リスニング ステートおよびラーニング 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 21-3 は、リンク障害が発生していないときのトポロジ例です。スイッチ A（ルート ブリッジ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ 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 LAN インターフェイスは、ブロッキング ステートです。

図 21-3　　間接リンク障害が発生する前の BackboneFast の例



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、この障害を検出できません。一方、スイッチ B は L1 を通じてルート ブリッジに直接接続されているので、この障害を検出し、自身をルートに選定し、スイッチ C に対して自身がルートであることを表す BPDU の送信を開始します。スイッチ C がスイッチ B から下位 BPDU を受信すると、スイッチ C は間接障害が発生したことを推測します。この時点で、BackboneFast により、スイッチ C のブロック ポートは、そのポートに設定されている最大エージング タイムの満了を待たずに、ただちにリスニング ステートに移行します。BackboneFast はさらに、スイッチ C のレイヤ 2 LAN 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 までのパスを提供します。このスイッチ オーバーに要する時間は、約 30 秒（デフォルトの転送遅延時間である 15 秒が設定されている場合、その 2 倍）です。図 21-4 に、BackboneFast がリンク L1 で発生した障害に応じてどのようにトポロジを再設定するかを示します。

図 21-4　　間接リンク障害が発生したあとの BackboneFast の例

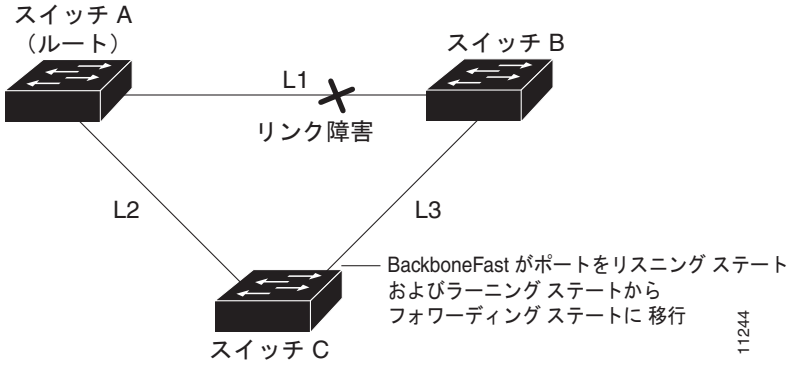
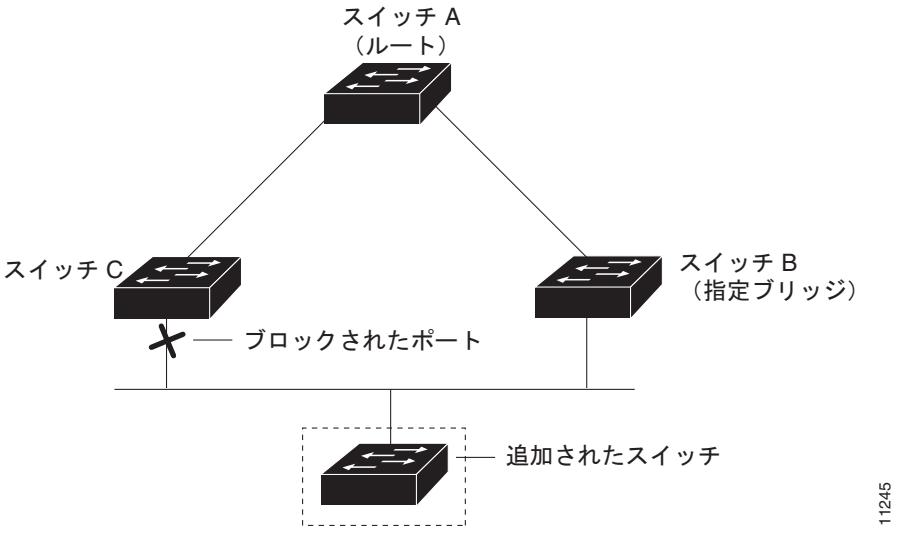


図 21-5 に示すメディア共有型トポロジに新しいネットワーク装置が組み込まれた場合、BackboneFast は起動されません。これは、認識している指定ブリッジ（スイッチ B）から下位 BPDU が着信していないためです。新しいネットワーク装置は、自らがルート ブリッジであることを伝える下位 BPDU の送信を開始します。しかし、他のネットワーク装置はこれらの下位 BPDU を無視します。その結果、新しいネットワーク装置はスイッチ B がルート ブリッジであるスイッチ A への指定ブリッジであることを学習します。

図 21-5　　メディア共有型トポロジにおけるネットワーク装置の追加



EtherChannel ガードの機能概要

EtherChannel ガードは正しく設定されていない EtherChannel を検出します（Catalyst 6500 シリーズ スイッチのインターフェイスが EtherChannel として設定されているが、他の装置のインターフェイスまたはその一部が同じ EtherChannel に設定されていない場合など）。

他の装置の設定に誤りがあることが検出されると、EtherChannel ガードは Catalyst 6500 シリーズ スイッチのインターフェイスを errdisable ステートにします。

ルート ガードの機能概要

STP ルート ガード機能を使用すると、ポートがルート ポートやブロックされたポートにならなくなります。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロックされた）ステートになります。

ループ ガードの機能概要

ループ ガードを使用すると、ポイントツーポイント リンク上の単一方向リンクの障害によって発生することがあるブリッジング ループを防止することができます。グローバルにイネーブル化されたループ ガードは、システム上のすべてのポイントツーポイント ポートに適用されます。ループ ガードはルート ポートおよびブロックされたポートを検出し、これらのポートがセグメント上の DP から BPDU を受信し続けるようにします。ループ ガードがイネーブルになっているルート ポートまたはブロックされたポートが DP からの BPDU の受信を停止した場合、このポートはポート上に物理リンク エラーがあると想定して、ループに一貫性のないブロッキング ステートに移行します。ポートが BPDU を受信すると、ただちにこのループに一貫性のないステートから回復します。

ループ ガードはポート単位でイネーブルにすることができます。ループ ガードをイネーブルにすると、すべてのアクティブ インスタンスまたはポートが属する VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにした場合は、指定したポートに対してディセーブルになります。ループ ガードをディセーブルにすると、ループに一貫性のないすべてのポートがリスニング ステートに移行します。

チャネル上でループ ガードをイネーブルにしたあとに、最初のリンクが単一方向リンクになると、ループ ガードは影響を受けたポートがチャネルから削除されるまで、チャネル全体をブロックします。図 21-6 に、三角型のスイッチ設定におけるループ ガードを示します。

図 21-6　ループ ガードが設定された三角型のスイッチ設定

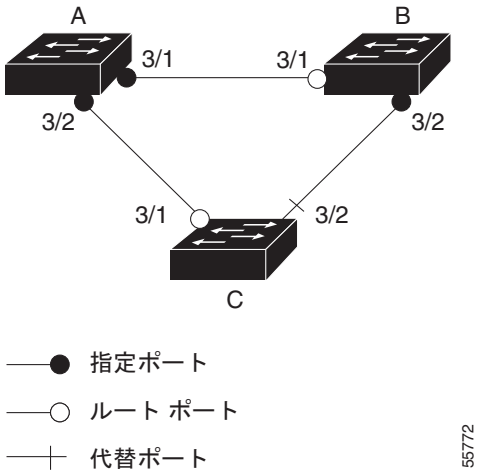


図 21-6 に、次の設定を示します。

- スイッチ A およびスイッチ B はディストリビューション スイッチです。
- スイッチ C はアクセス スイッチです。
- ループ ガードは、スイッチ A、B、C のポート 3/1 および 3/2 でイネーブルです。

ルート スイッチ上でループ ガードをイネーブルにしても影響はありませんが、ルート スイッチが非ルート スイッチになると、保護機能が有効になります。

ループ ガードを使用するときは、次の注意事項に従ってください。

- PortFast 対応ポートでは、ループ ガードをイネーブルにできません。
- ルート ガードがイネーブルの場合は、ループ ガードをイネーブルにできません。

ループ ガードは、次のように他の機能と相互作用します。

- ループ ガードは UplinkFast または BackboneFast の機能には影響しません。
- ポイントツーポイント リンクに接続されていないポート上でループ ガードをイネーブルにしても、機能しません。
- ルート ガードは、強制的に、ポートを常にルート ポートとして指定された状態にします。ポートがルート ポートまたは代替ポートの場合のみ、ループ ガードは有効です。特定のポート上でループ 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。
- ループ ガードはスパニング ツリーで認識されているポートを使用します。ループ ガードは、Port Aggregation Protocol（PAgP; ポート集約プロトコル）が提供する論理ポートを利用できます。ただし、チャネルを形成するには、そのチャネルにグループ化するすべての物理ポートの設定に互換性がなければなりません。チャネルを形成するために、PAgP はすべての物理ポート上でルート ガードまたはループ ガードの設定を均一にします。

  ループ ガードに適用される注意事項は、次のとおりです。

  - スパニング ツリーは、BPDU を送信するチャネル内で最初に動作するポートを常に選択します。このリンクが単一方向になった場合、チャネル内の他のリンクが適切に機能している場合でも、ループ ガードはチャネルをブロックします。
  - ループ ガードによってブロックされている一連のポートをグループ化して、チャネルを形成した場合、スパニング ツリーはこれらのポートのステート情報をすべて失い、新しいチャネル ポートは指定された役割を使用してフォワーディング ステートに移行できます。
  - チャネルがループ ガードによってブロックされている場合に、チャネルが切断されると、スパニング ツリーはすべてのステート情報を失います。チャネルを形成する 1 つまたは複数のリンクが単一方向リンクである場合も、各物理ポートは指定された役割を使用して、フォワーディング ステートに移行できます。

（注）　UniDirectional Link Detection（UDLD; 単一方向リンク検出）をイネーブルにして、リンク障害を特定することができます。UDLD が障害を検出するまでループが発生することがありますが、ループ ガードはこのループを検出できません。

- ディセーブル化されたスパニング ツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。

PortFast のイネーブル化

注意　PortFast は、単一のエンド ステーションをレイヤ 2 アクセス ポートに接続する場合に*限って*使用してください。そうしない場合、ネットワーク ループが発生する可能性があります。

レイヤ 2 アクセス ポート上で PortFast をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type[1] slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree portfast`	単一のワークステーションまたはサーバに接続されたレイヤ 2 アクセス ポート上で PortFast をイネーブルにします。
ステップ 3	`Router(config-if)# spanning-tree portfast default`	PortFast をイネーブルにします。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show running interface {type[1] slot/port} | {port-channel port_channel_number}`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット インターフェイス 5/8 上で PortFast をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/8
Router(config-if)# spanning-tree portfast
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show running-config interface fastethernet 5/8
Building configuration...

Current configuration:
!
interface FastEthernet5/8
 no ip address
 switchport
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
end

Router#
```

PortFast のデフォルト設定をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree portfast default`	PortFast をデフォルトに設定します。
ステップ 2	`Router(config)# show spanning-tree summary totals`	グローバル コンフィギュレーションを確認します。
ステップ 3	`Router(config)# show spanning-tree interface` *x* `detail`	特定のポートに対する効果を確認します。
ステップ 4	`Router(config-if)# spanning-tree portfast trunk`	ポート上で PortFast トランクをイネーブルにします。
ステップ 5	`Router# show spanning-tree interface fastEthernet` *x* `detail`	設定を確認します。

次に、PortFast のデフォルト設定をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree portfast default
Router(config)# ^Z

Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
Portfast             is enabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  0        0         0        1          1
VLAN0010                  0        0         0        2          2
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
Router#

Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by default
   Link type is point-to-point by default
   BPDU:sent 10, received 0

Router(config-if)# spanning-tree portfast trunk
%Warning:portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

Router(config-if)# ^Z
```

```
Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   BPDU:sent 30, received 0
Router#
```

PortFast BPDU フィルタリングのイネーブル化

ここでは、PortFast BPDU フィルタリングの設定手順について説明します。

PortFast BPDU フィルタリングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree portfast bpdufilter default`	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します。
ステップ 2	`Router# show spanning-tree summary totals`	設定を確認します。

各ポート上で、BPDU フィルタリングはデフォルトに設定されています。次に、ポート上で PortFast BPDU フィルタリングをイネーブルにして、PVST+ モードで設定を確認する例を示します。

（注）　PVST+ の詳細は、第 20 章「スパニング ツリー プロトコル（STP）および先行標準 IEEE 802.1s MST の設定」を参照してください。

```
Router(config)# spanning-tree portfast bpdufilter default
Router(config)# ^Z

Router# show spanning-tree summary totals
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
Portfast             is enabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
Router#
```

非トランキング ポート上で PortFast BPDU フィルタリングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface fastEthernet 4/4`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# spanning-tree bpdufilter enable`	BPDU フィルタリングをイネーブルにします。
ステップ 3	`Router# show spanning-tree interface fastEthernet 4/4`	設定を確認します。

次に、非トランキング ポート上で PortFast BPDU フィルタリングをイネーブルにする例を示します。

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# ^Z

Router# show spanning-tree interface fastEthernet 4/4

Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0010         Desg FWD 1000      160.196  Edge P2p
Router# show spanning-tree interface fastEthernet 4/4 detail
Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   Bpdu filter is enabled
   BPDU:sent 0, received 0
Router#
```

BPDU ガードのイネーブル化

BPDU ガードをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **spanning-tree portfast bpduguard default** Router(config)# **no 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 ガードをグローバルにディセーブルにします。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show spanning-tree summary totals**	設定を確認します。

次に、BPDU ガードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree portfast bpduguard
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary totals default
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
Portfast             is enabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
Router#
```

UplinkFast のイネーブル化

UplinkFast を使用すると、ブリッジ プライオリティが 49152 に増えるとともに、Catalyst 6500 シリーズ スイッチ上のすべてのレイヤ 2 LAN インターフェイスの STP ポート コストに 3000 が加算されます。その結果、スイッチがルート ブリッジになる確率が低くなります。*max_update_rate* 値は、1 秒間に送信されるマルチキャスト パケット数を表します（デフォルトは 150 パケット/秒です）。ブリッジ プライオリティを設定している VLAN 上では、UplinkFast をイネーブルにすることはできません。ブリッジ プライオリティを設定している VLAN 上で UplinkFast をイネーブルにするには、グローバル コンフィギュレーション モードで **no spanning-tree vlan** *vlan_ID* **priority** コマンドを入力して、VLAN のブリッジ プライオリティをデフォルトに戻します。

（注）　UplinkFast をイネーブルにすると、Catalyst 6500 シリーズ スイッチ上のすべての VLAN に影響します。個々の VLAN について UplinkFast を設定できません。

UplinkFast をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree uplinkfast` `Router(config)# spanning-tree uplinkfast [max-update-rate max_update_rate]`	UplinkFast をイネーブルにします。 UplinkFast をイネーブルにして、アップデート速度を秒単位で指定します。
	`Router(config)# no spanning-tree uplinkfast max-update-rate`	デフォルトのレートに戻します。
	`Router(config)# no spanning-tree uplinkfast`	UplinkFast をディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan vlan_ID`	UplinkFast がイネーブルになっていることを確認します。

次に、UplinkFast をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast
Router(config)# exit
Router#
```

次に、UplinkFast をイネーブルにして、アップデート速度を 400 パケット/秒に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast
Router(config)# spanning-tree uplinkfast max-update-rate 400
Router(config)# exit
Router#
```

次に、UplinkFast がイネーブルになっていることを確認する例を示します。

```
Router# show spanning-tree uplinkfast
UplinkFast is enabled
Router#
```

BackboneFast のイネーブル化

（注）　BackboneFast が適切に動作するのは、ネットワーク内のすべてのネットワーク装置上でイネーブルになっている場合だけです。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は、サードパーティ製のネットワーク装置と組み合わせて使用することができます。

BackboneFast をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree backbonefast`	BackboneFast をイネーブルにします。
	`Router(config)# no spanning-tree backbonefast`	BackboneFast をディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree vlan` *vlan_ID*	BackboneFast がイネーブルになっていることを確認します。

次に、BackboneFast をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree backbonefast
Router(config)# end
Router#
```

次に、BackboneFast がイネーブルになっていることを確認する例を示します。

```
Router# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)     : 0
Number of RLQ request PDUs received (all VLANs)   : 0
Number of RLQ response PDUs received (all VLANs)  : 0
Number of RLQ request PDUs sent (all VLANs)       : 0
Number of RLQ response PDUs sent (all VLANs)      : 0
Router#
```

EtherChannel ガードのイネーブル化

EtherChannel ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# spanning-tree etherchannel guard misconfig`	EtherChannel ガードをイネーブルにします。
	`Router(config)# no spanning-tree etherchannel guard misconfig`	EtherChannel ガードをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show spanning-tree summary | include EtherChannel`	EtherChannel ガードがイネーブルになっていることを確認します。

次に、EtherChannel ガードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# spanning-tree etherchannel guard misconfig
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree summary | include EtherChannel
EtherChannel misconfiguration guard is enabled
```

errdisable ステートのインターフェイスを表示するには、**show interface status err-disable** コマンドを入力します。

誤っている設定が解消されると、errdisable ステートのインターフェイスは自動的に回復します。ポートを手動で動作状態に戻すには、**shutdown** コマンドを入力してから、該当するインターフェイスに対して **no shutdown** コマンドを入力します。

ルート ガードのイネーブル化

ルート ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type[1] slot/port} | {port-channel port_channel_number}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# spanning-tree guard root`	ルート ガードをイネーブルにします。
	`Router(config-if)# no spanning-tree guard root`	ルート ガードをディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show spanning-tree` `Router# show running interface {type[1] slot/port} | {port-channel port_channel_number}`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ルートとして一貫性のないステートになっているポートを表示するには、**show spanning-tree inconsistentports** コマンドを入力します。

ループ ガードのイネーブル化

スイッチ上でループ ガードをグローバルにイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router(config)# **spanning-tree loopguard default**	スイッチ上でループ ガードをグローバルにイネーブルにします。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show spanning-tree interface 4/4 detail**	この設定がポートに作用していることを確認します。

次に、ループ ガードをグローバルにイネーブルにする例を示します。

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree loopguard default
Router(config)# ^Z

Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   Bpdu filter is enabled
   Loop guard is enabled by default on the port
   BPDU:sent 0, received 0
```

特定のポート上でループ ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {*type*[1] *slot/port*} | {**port-channel** *port_channel_number*}	設定するポートを選択します。
ステップ 2	Router(config-if)# **spanning-tree guard loop**	ループ ガードを設定します。
ステップ 3	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show spanning-tree interface 4/4 detail**	この設定がポートに作用していることを確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ループ ガードをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree guard loop
Router(config-if)# ^Z
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   Bpdu filter is enabled
   Loop guard is enabled on the port
   BPDU:sent 0, received 0
Router#
```

CHAPTER 22

レイヤ 3 インターフェイスの設定

この章では、Catalyst 6500 シリーズ スイッチにレイヤ 3 インターフェイスを設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

この章で説明する内容は、次のとおりです。

レイヤ 3 インターフェイス設定時の注意事項および制約事項

レイヤ 3 インターフェイスを設定する際に、以下の注意事項と制約事項に従ってください。

- 設定するレイヤ 3 VLAN インターフェイスは 2,000 個までにすることを推奨します。
- Release12.2(18)SXE 以降のリリースでは、レイヤ 3 VLAN インターフェイスで **ip unnumbered** コマンドがサポートされます。
- Release12.2(18)SXE 以降のリリースでは、[**no**] **ip dhcp route** [**connected** | **static**] コマンドがサポートされます。
- VLAN インターフェイスをサポートするには、VLAN を作成および設定し、レイヤ 2 LAN ポートに VLAN メンバシップを割り当てます。詳細については、第 14 章「仮想 LAN（VLAN）の設定」およびを参照してください。第 13 章「VLAN トランキング プロトコル（VTP）の設定」
- Catalyst 6500 シリーズ スイッチは、以下をサポートしません。
  - Integrated Routing and Bridging（IRB）
  - Concurrent Routing and Bridging（CRB）
  - Remote Source-Route Bridging（RSRB; リモート ソースルート ブリッジング）
- VLAN インターフェイスでブリッジ グループ（代替ブリッジングともいう）を使用して、ルーティングされないプロトコルをブリッジします。VLAN インターフェイスのブリッジ グループは、MSFC のソフトウェアでサポートされます。
- Catalyst 6500 シリーズ スイッチは、ブリッジ グループの IEEE ブリッジング プロトコルをサポートしません。VLAN ブリッジまたは DEC スパニング ツリー プロトコルを使用してブリッジ グループを設定します。

レイヤ 3 インターフェイスのサブインターフェイスの設定

レイヤ 3 サブインターフェイスを設定する際に、以下の注意事項と制約事項に従ってください。

- PFC3 を持つ Release12.2(18)SXE 以降のリリースでは、LAN ポート サブインターフェイスで以下の機能をサポートします。
  - MPLS VPN を含む IPv4 ユニキャスト フォワーディング
  - MPLS VPN を含む IPv4 マルチキャスト フォワーディング
  - 6PE
  - EoMPLS
  - 番号付けされていない Ipv4
  - MIBS 内の **show vlans** コマンドを使用したサブインターフェイス用カウンタ
  - iBGP および eBGP
  - OSPF
  - EIGRP
  - RIPv1/v2
  - RIPv2
  - ISIS
  - スタティック ルーティング
  - UniDirectional Link Routing（UDLR; 単一方向リンク ルーティング）

  - IGMPv1、IGMPv2、IGMPv3
  - PIMv1、PIMv2
  - SSM IGMPv3lite および URD
  - スタブ IP マルチキャスト ルーティング
  - IGMP Join
  - IGMP スタティック グループ
  - Multicast Routing Monitor（MRM）
  - Multicast Source Discovery Protocol（MSDP）
  - SSM
  - IPv4 ping
  - Ipv6 ping
- これらの制約事項は、Release 12.2(18)SXE よりも前のリリースに適用されます。
  - サブインターフェイスは、MPLS をサポートするためだけに設定してください。
  - Inter-Switch Link（ISL; スイッチ間リンク）カプセル化を設定しないでください。
- VLAN ID が IEEE 802.1Q ネイティブ VLAN の ID の場合、**native** キーワードを必ず使用してください。**native** キーワードを使用せずに、IEEE 802.1Q トランクのネイティブ VLAN でカプセル化を設定しないでください。
- VLAN ID はスイッチに対してグローバルであるため、サブインターフェイス上、またはレイヤ 3 VLAN インターフェイスに関して VLAN を内部的に使用することができます。
  - サブインターフェイスまたはレイヤ 3 VLAN インターフェイスで、内部 VLAN を設定することはできません。
  - レイヤ 3 VLAN インターフェイスで、サブインターフェイス VLAN を設定することはできません。
  - サブインターフェイス上では、レイヤ 3 VLAN インターフェイスとともに使用される VLAN を設定することはできません。

（注） 1 つのインターフェイス、別のインターフェイスのサブインターフェイス、またはサブインターフェイスで使用されている VLAN を設定することはできません。

- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）透過モードでは、任意の標準範囲または拡張範囲の VLAN ID を使用して、サブインターフェイスを設定することができます。VLAN ID 1 ～ 1005 は、VTP ドメインでグローバルであり、VTP ドメイン内の他のネットワーク装置上で定義することができるため、VTP クライアント/サーバ モードでは、拡張範囲 VLAN のみをサブインターフェイスとともに使用することができます。VTP クライアント/サーバ モードでは、標準範囲 VLAN がサブインターフェイスから除外されます。

（注） サブインターフェイス上で標準範囲 VLAN を設定する場合、VTP モードを透過から変更できません。

サブインターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> enable`	イネーブル EXEC モードを開始します。
ステップ 2	`Router# configure terminal`	グローバル 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	`Router(config)# interface {{type[1] slot/port.subinterface} | {port-channel port_channel_number.subinterface}}`	インターフェイスを選択して、サブインターフェイス 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	`Router(config-subif)# encapsulation dot1q vlan_ID [native]`	サブインターフェイスの 802.1Q カプセル化を設定します。
ステップ 5	`Router(config-if)# 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。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、または **ge-wan**

IPv4 ルーティングおよびアドレスの設定

詳しい説明および設定手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html
- 次の URL にある『*Cisco IOS IP and IP Routing Command Reference*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
  http://www.cisco.com/en/US/docs/ios/12_2/iproute/command/reference/fiprrp_r.html

IPv4 ルーティングおよびアドレスを設定する際に、以下の注意事項と制約事項に従ってください。

- **maximum paths** コマンドの詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。
- Policy Feature Card（PFC; ポリシー フィーチャ カード）および Distributed Feature Card（DFC）は、**match ip address**、**set ip next-hop**、**ip default next-hop** Policy-Based Routing（PBR; ポリシーベース ルーティング）キーワードを使用するルート マップ シーケンス用の PBR をハードウェアでサポートします。

  PBR を設定する際に、以下の注意事項と制約事項に従ってください。

  - PFC はトンネル インターフェイスに設定されている PBR のハードウェア サポートを提供します。
  - PFC は、ネクスト ホップがトンネル インターフェイスである場合に **set ip next-hop** キーワードで設定されている PBR のハードウェア サポートを提供しません。
  - MSFC アドレスが PBR ACL（アクセス制御リスト）範囲内にある場合、MSFC にアドレス指定されたトラフィックは MSFC に転送されずに、ハードウェアでポリシー ルーティングされます。MSFC にアドレス指定されたトラフィックをポリシー ルーティングしないようにするには、MSFC にアドレス指定されたトラフィックを拒否するように PBR ACL を設定します。
  - Cisco IOS ACL のオプションの中で、MSFC に送信されソフトウェアでスイッチングされるフローが発生するような PBR ルート マップでのフィルタリングを実行するものは無視されます。たとえば、PBR ルート マップでのフィルタリングを行う Cisco IOS ACL の ACE で、ロギングはサポートされていません。

- PBR が設定されているスイッチング モジュール ポートを通過する PBR トラフィックは、スイッチング モジュールがリセットされる場合にソフトウェアでルーティングされます（CSCee92191）。
- **permit** ルートマップ シーケンスに **set** ステートメントを指定しないと、一致したトラフィックは MSFC によって処理されます。
- Cisco IOS Release 12.2(33)SXF16 以降のリリースでは、複数の PBR シーケンス（または複数の ACL を持つ単一の PBR シーケンス）を設定する（つまり、複数の PBR ACL が DENY エントリを含む）場合は、ハードウェア リソースを効率的に使用するために、グローバル コンフィギュレーション モードで **platform ipv4 pbr optimize tcam** コマンドを入力してください。それよりも前のリリースでは、このタイプのコンフィギュレーションは避けるように推奨しています（CSCsr45495）。
- Cisco IOS Release 12.2(33)SXH4 以降のリリースでは、BOOTP/DHCP トラフィックは、明示的に許可されていない限り廃棄されます。Cisco IOS Release 12.2(18)SXF では、BOOTP/DHCP パケットは入力インターフェイス内で設定されている PBR の対象にはならず、BOOTP/DHCP パケットは BOOTP/DHCP サーバに転送されます。ただし、これは明示的に許可されてはいません。

PBR の設定については、次の URL にある『*Cisco IOS Quality of Service Solutions Configuration Guide*』Release 12.2 の「Classification」、「Configuring Policy-Based Routing」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html

レイヤ 3 インターフェイスに IPv4 ルーティングおよび IPv4 アドレスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip routing`	IPv4 ルーティングをイネーブルにします（IPv4 ルーティングがディセーブルになっている場合のみ必須）。
ステップ 2	`Router(config)# router ip_routing_protocol`	IPv4 ルーティング プロトコルを指定します。
ステップ 3	`Router(config-router)# ip_routing_protocol_commands`	IPv4 ルーティング プロトコルを設定します。
ステップ 4	`Router(config-router)# exit`	IPv4 ルーティング プロトコルのコンフィギュレーション モードを終了します。
ステップ 5	`Router(config)# interface {vlan vlan_ID} | {type[1] slot/port} | {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 6	`Router(config-if)# ip address ip_address subnet_mask`	IPv4 アドレスおよび IPv4 サブネットを設定します。
ステップ 7	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 8	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

ステップ 9	`Router# show interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show ip interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show running-config interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
		設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、または **ge-wan**

次に、IPv4 Routing Information Protocol（RIP）ルーティングをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# end
Router#
```

次に、ファスト イーサネット ポート 5/4 に IPv4 アドレスを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/4
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

次に、**show interfaces** コマンドを使用して、ファスト イーサネット ポート 5/4 のインターフェイス IPv4 アドレスの設定およびステータスを表示する例を示します。

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
  Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
  Internet address is 172.20.52.106/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7 packets input, 871 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     8 packets output, 1658 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

次に、**show ip interface** コマンドを使用して、ファスト イーサネット ポート 5/4 の詳細な設定およびステータスを表示する例を示します。

```
Router# show ip interface fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
  Internet address is 172.20.52.106/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
  IP mls switching is enabled
Router#
```

次に、**show running-config** コマンドを使用して、ファスト イーサネット ポート 5/4 のインターフェイス IPv4 アドレスの設定を表示する例を示します。

```
Router# show running-config interfaces fastethernet 5/4
Building configuration...

Current configuration:
!
interface FastEthernet5/4
 description "Router port"
 ip address 172.20.52.106 255.255.255.248
 no ip directed-broadcast
!
```

IPX ルーティングおよびネットワーク番号の設定

（注） Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）は、高速スイッチングで Internetwork Packet Exchange（IPX）をサポートしています。

詳しい説明および設定手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS AppleTalk and Novell IPX Configuration Guide*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/atipx/configuration/guide/fatipx_c.html
- 次の URL にある『*Cisco IOS AppleTalk and Novell IPX Command Reference*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/atipx/command/reference/fatipx_r.html

IPX ルーティングを設定し、レイヤ 3 インターフェイスに IPX を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ipx routing`	IPX ルーティングをイネーブルにします。
ステップ 2	`Router(config)# router ipx_routing_protocol`	IP ルーティング プロトコルを指定します。このステップでは、他のコマンド（ルーティングするネットワークを指定する **network** コマンドなど）を使用する場合があります。
ステップ 3	`Router(config)# interface {vlan vlan_ID} | {type[1] slot/port} | {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 4	`Router(config-if)# ipx network [network | unnumbered] encapsulation encapsulation_type`	IPX ネットワーク番号を設定します。このステップにより、インターフェイス上で IPX ルーティングがイネーブルになります。インターフェイス上で IPX ルーティングをイネーブルにするとき、カプセル化タイプも指定できます。
ステップ 5	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 6	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

ステップ 7	`Router# show interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show ipx interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show running-config interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
		設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**、または **ge-wan**

次に、IPX ルーティングをイネーブルにし、インターフェイス VLAN100 に IPX ネットワーク アドレスを割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipx routing
Router(config)# ipx router rip
Router(config-ipx-router)# network all
Router(config-ipx-router)# interface vlan 100
Router(config-if)# ipx network 100 encapsulation snap
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

AppleTalk ルーティング、ケーブルの範囲、およびゾーンの設定

詳しい説明および設定手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS AppleTalk and Novell IPX Configuration Guide*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/atipx/configuration/guide/fatipx_c.html
- 次の URL にある『*Cisco IOS AppleTalk and Novell IPX Command Reference*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/atipx/command/reference/fatipx_r.html

AppleTalk ルーティングを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# appletalk routing`	AppleTalk ルーティングをイネーブルにします。
ステップ 2	`Router(config)# interface {vlan vlan_ID} | {type[1] slot/port} | {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	`Router(config-if)# appletalk cable-range cable_range`	インターフェイスにケーブル範囲を割り当てます。
ステップ 4	`Router(config-if)# appletalk zone zone_name`	インターフェイスにゾーン名を割り当てます。
ステップ 5	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 6	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

ステップ 7	`Router# show interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show appletalk interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
	`Router# show running-config interfaces [{vlan vlan_ID} | {type[1] slot/port} | {port-channel port_channel_number}]`
		設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**、または **ge-wan**

次に、AppleTalk ルーティングをイネーブルにして、インターフェイス VLAN 100 に AppleTalk ケーブルの範囲およびゾーン名を割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# appletalk routing
Router(config)# interface vlan 100
Router(config-if)# appletalk cable-range 100-100
Router(config-if)# appletalk zone Engineering
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

レイヤ 3 インターフェイス上でのその他のプロトコルの設定

レイヤ 3 インターフェイスにその他のプロトコルを設定する手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Configuration Guide*』Release12.2

  http://www.cisco.com/en/US/docs/ios/12_2/apollo/configuration/guide/fapolo_c.html

- 次の URL にある『*Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Command Reference*』Release12.2

  http://www.cisco.com/en/US/docs/ios/12_2/apollo/command/reference/fapolo_r.html

CHAPTER 23

単一方向イーサネット（UDE）および単一方向リンク ルーティング（UDLR）の設定

この章では、Catalyst 6500 シリーズ スイッチの Unidirectional Ethernet（UDE; 単一方向イーサネット）および Unidirectional Link Routing（UDLR; 単一方向リンク ルーティング）を設定する手順について説明します。Release 12.2(18)SXF 以降のリリースで、UDE と UDLR がサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

ここでは、UDE および UDLR の概要について説明します。

UDE および UDLR の概要

ここでは、UDE および UDLR の概要について説明します。

UDE と UDLR の概要

ルーティング プロトコルが単一方向リンクをサポートするのは、単一方向リンクが双方向リンクをエミュレートしている場合だけです。これは、同じインターフェイス上でルーティング プロトコルがトラフィックの送受信をするためです。

単一方向リンクが便利なのは、大容量の全二重双方向リンクで確認応答を受けずに大量の単一方向トラフィックを送信する場合（ビデオ ブロードキャスト ストリームなど）、送信元から宛先までのリンクと、宛先から送信元へほとんど確認応答を送らない「バック チャネル」と呼ばれる大容量の逆方向リンクの両方を同じように使用するためです。

UDE および UDLR を使用すると、バック チャネルに同程度の大容量リンクを消費せずに、大量のトラフィックに対して大容量単一方向リンクをサポートできます。UDE は大容量の単一方向リンクを提供します。UDLR は、標準的な容量のリンクにバック チャネルとしてトンネルを提供します。また、UDLR は、バック チャネルが大容量単一方向リンクと同じインターフェイスにあるかのように透過的に見せることによって、双方向リンクのエミュレーションも行います。

サポートされるハードウェア

Catalyst 6500 シリーズ スイッチの場合、次のスイッチング モジュールのインターフェイスで UDE と UDLR がサポートされています。

- WS-X6704-10GE 4 ポート 10 ギガビット イーサネット
- WS-X6816-GBIC 16 ポート ギガビット イーサネット
- WS-X6516A-GBIC 16 ポート ギガビット イーサネット
- WS-X6516-GBIC 16 ポート ギガビット イーサネット

UDE の概要

ここでは UDE について説明します。

UDE の概要

Catalyst 6500 シリーズ スイッチの場合、ハードウェアまたはソフトウェアを使用して UDE を実装できます。ハードウェア ベース UDE およびソフトウェア ベース UDE では、双方向トラフィックで必要とされる 2 本のファイバケーブルの代わりに 1 本だけを使用します。

ハードウェア ベース UDE が受信専用と送信専用のどちらであるかは、双方向トランシーバが判断します。ソフトウェア ベース UDE は、送信専用または受信専用のどちらにも設定できます。

ハードウェア ベース UDE を実装するポートに、ソフトウェア ベース UDE を設定する必要はありません。

（注）　ハードウェア ベース UDE およびソフトウェア ベース UDE をサポートするインターフェイスを搭載したモジュールの詳細については、「サポートされるハードウェア」（P.23-2）を参照してください。

ハードウェア ベース UDE の概要

単一方向トランシーバを使用すると、単一方向リンクを構築できます。単一方向トランシーバは、双方向トランシーバより安価です。Release 12.2(18)SXE 以降のリリースでは、単一方向トランシーバがサポートされています。

- 受信専用 WDM GBIC（WDM-GBIC-REC=）
- 受信専用 XENPAK（WDM-XENPAK-REC=）

ソフトウェア ベース UDE の概要

双方向トランシーバを搭載したポートでトラフィックの単一方向の送受信を設定すると、単一方向リンクを構築できます。適切な単一方向トランシーバが入手できない場合は、ソフトウェア ベース UDE を使用できます。たとえば、送信専用トランシーバがサポートされていない場合、ソフトウェア ベース UDE を使用して送信専用リンクを設定する必要があります。

UDLR の概要

UDLR は、大容量の単一方向リンクのバック チャネルとして単一方向トンネルを提供し、ユニキャストおよびマルチキャストのトラフィック用に 1 つの双方向リンクを透過的にエミュレートします。

UDLR は、送信の必要のあるパケットを受信専用インターフェイスで代行受信し、UDLR バック チャネル トンネルで送信します。ルータが UDLR バック チャネル トンネルからパケットを受信すると、UDLR によってパケットは送信専用インターフェイスで受信されたかのように扱われます。

UDLR バック チャネル トンネルは、次の IPv4 機能をサポートしています。

- Address Resolution Protocol（ARP; アドレス解決プロトコル）
- Next Hop Resolution Protocol（NHRP）
- すべての IPv4 トラフィック用の双方向リンクのエミュレーション（ブロードキャストおよびマルチキャスト専用制御トラフィックとは逆）
- 受信専用トンネルでの IPv4 GRE マルチポイント

（注） UDLR バック チャネル トンネルは、IPv6 または Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）をサポートしていません。

UDE および UDLR の設定

ここでは、UDE および UDLR の設定手順について説明します。

（注）　この注意事項は、UDLR をサポートしているリリースに対応しています。近接 ISIS ルータは、UDLR トポロジを介して認識されません（CSCee56596）。

UDE の設定

ここでは、UDE の設定手順について説明します。

UDE 設定時の注意事項

UDE を設定する際に、以下の注意事項に従ってください。

- UDE は、Supervisor Engine 720 でサポートされています。UDE は、Supervisor Engine 2 でサポートされていません。
- Spanning Tree Protocol（STP; スパニング ツリー プロトコル）では、単一リンクを備えたトポロジでレイヤ 2 ループの発生を防止できません。
- 送信専用ポートでは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信できないため、必ず STP フォワーディング ステートに移行します。
- 受信専用ポートは BPDU を送信できません。
- 単一方向ポートは、リンクの反対側のポートとの間でネゴシエーションを必要とする次の機能またはプロトコルをサポートしていません。
  - 速度およびデュプレックス モードの自動ネゴシエーション
  - リンク ネゴシエーション
  - Institute of Electrical and Electronic Engineers（IEEE; 米国電気電子学会）802.3Z フロー制御
  - Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）

  通常はレイヤ 2 プロトコルで制御されるパラメータは、手動で設定する必要があります。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）サーバが VTP フレームを VTP ドメインにある全スイッチに送信できる場合に、単一方向リンクを含むトポロジは VTP だけをサポートします。
- VTP プルーニングは情報の双方向交換によって異なるため、送信専用ポートを備えたスイッチで VTP プルーニングをディセーブルにします。
- 単一方向 EtherChannel は、Port Aggregation Protocol（PAgP; ポート集約プロトコル）または Link Aggregation Control Protocol（LACP）をサポートできません。単一方向 EtherChannel を作成するには、on モードで EtherChannel を作成する必要があります。

- ソフトウェア ベース UDE は、EtherChannel の物理ポートに設定できます。ソフトウェア ベース UDE は、非物理インターフェイス（ポート チャネル インターフェイスなど）には設定できません。
- ポートにハードウェア ベース UDE またはソフトウェア ベース UDE を実装すると、Unidirectional Link Detection（UDLD; 単一方向リンク検出）は自動的にディセーブルになります。
- Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）は、送信専用ポートから CDP フレームを送信し、受信専用ポートで CDP フレームを受信します。つまり、単一方向リンクの送信専用側のスイッチは CDP 情報を受信しません。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）では、単一方向ポートの設定が送信先または宛先として制限されることはありません。
  - SPAN の宛先を送信専用ポートにすることができます。
  - SPAN の送信元を受信専用ポートにすることができます。
- 単一方向ポートは、IEEE 802.1X ポートベースの認証をサポートしていません。
- Internet Group Management Protocol（IGMP）スヌーピングは、スイッチとホストとの間にマルチキャスト トラフィックを受信する単一方向リンクがあるトポロジをサポートしていません。
- スイッチ上の IGMP スヌーピングとマルチキャスト ルータ間の単一方向リンクでの通信をサポートするように、UDLR を UDE で設定します。
- 単一方向リンクは ARP をサポートしていません。

ハードウェア ベース UDE の設定

ハードウェア ベース UDE をサポートするために必要なソフトウェアの設定手順はありません。単一方向トランシーバを取り付けて、ハードウェア ベース UDE を実装します。

ポート上でハードウェア ベース UDE を確認するには、次の作業を行います。

コマンド	目的
Router# **show interfaces** [{**gigabitethernet** | **tengigabitethernet**} *slot/interface*}] **status**	設定を確認します。

次に、ギガビット イーサネット ポート 1/1 の設定を確認する例を示します。

```
Router# show interfaces gigabitethernet 1/1 status

Port    Name               Status       Vlan       Duplex  Speed Type
Gi1/1                      notconnect   1            full   1000 WDM-RXONLY
```

ソフトウェア ベース UDE の設定

ポート上でソフトウェア ベース UDE を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**gigabitethernet** | **tengigabitethernet**} *slot/interface*}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **unidirectional** {**send-only** | **receive-only**}	ソフトウェア ベース UDE を設定します。
	Router(config-if)# **no unidirectional**	ソフトウェア ベース UDE の設定を削除します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show interface** {{**gigabitethernet** | **tengigabitethernet**} *slot/interface*} **unidirectional**	設定を確認します。

次に、10 ギガビット イーサネット ポート 1/1 を UDE 送信専用ポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/1
Router(config-if)# unidirectional send-only
Router(config-if)# end

Warning!

Enable port unidirectional mode will automatically disable port udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable l3 port unidirectional mode will automatically disable ip routing on the port. You
must manually configure static ip route and arp entry in order to route ip traffic.
```

次に、10 ギガビット イーサネット ポート 1/2 を UDE 受信専用ポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/2
Router(config-if)# unidirectional receive-only
Router(config-if)# end

Warning!

Enable port unidirectional mode will automatically disable port udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable l3 port unidirectional mode will automatically disable ip routing on the port. You
must manually configure static ip route and arp entry in order to route ip traffic.
```

次に、設定を確認する例を示します。

```
Router> show interface tengigabitethernet 1/1 unidirectional
  Unidirectional configuration mode: send only
  CDP neighbour unidirectional configuration mode: receive only
```

次に、10 ギガビット イーサネット インターフェイス 1/1 の設定をディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 1/1
Router(config-if)# no unidirectional
Router(config-if)# end
```

次に、単一方向イーサネットをサポートしていないポートに対する **show interface** コマンドの実行結果を示します。

```
Router# show interface fastethernet 6/1 unidirectional
Unidirectional Ethernet is not supported on FastEthernet6/1
```

UDLR の設定

ここでは、UDLR を設定する手順について説明します。

- 「UDLR バック チャネル トンネル設定時の注意事項」（P.23-7）
- 「UDE 送信専用ポートでの受信専用トンネル インターフェイスの設定」（P.23-8）
- 「UDE 受信専用ポートでの送信専用トンネル インターフェイスの設定」（P.23-8）

UDLR バック チャネル トンネル設定時の注意事項

UDE バック チャネル トンネルを設定する際に、以下の注意事項に従ってください。

- Policy Feature Card（PFC; ポリシー フィーチャ カード）3 は、ハードウェアでは UDLR バック チャネル トンネルをサポートしていません。Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）3 は、UDLR バック チャネル トンネルをソフトウェアでサポートしています。
- 単一方向リンクに UDLR バック チャネル トンネルを設定します。
- UDE 送信専用インターフェイスで、受信ができるように UDLR バック チャネル トンネル インターフェイスを設定します。
- UDE 受信専用インターフェイスで、送信ができるように UDLR バック チャネル トンネル インターフェイスを設定します。
- UDLR バック チャネル トンネル インターフェイスでは IPv4 アドレスを設定する必要があります。
- UDLR バック チャネル トンネル インターフェイスで、送信元および宛先の IPv4 アドレスを設定する必要があります。
- UDLR バック チャネル トンネルのデフォルト モードは GRE です。
- UDLR バック チャネル トンネルは、IPv6 または MPLS をサポートしていません。

UDE 送信専用ポートでの受信専用トンネル インターフェイスの設定

UDE 送信専用ポートに受信専用トンネル インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tunnel number`	トンネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# tunnel udlr receive-only ude_send_only_port`	トンネルの受信専用インターフェイスを UDE 送信専用ポートと関連付けます。
ステップ 3	`Router(config-if)# ip address ipv4_address`	トンネル IPv4 アドレスを設定します。
ステップ 4	`Router(config-if)# tunnel source {ipv4_address | type number}`	トンネルの送信元を設定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ipv4_address}`	トンネルの宛先を設定します。

UDE 受信専用ポートでの送信専用トンネル インターフェイスの設定

UDE 受信専用ポートに送信専用トンネル インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tunnel number`	トンネル インターフェイスを選択します。
ステップ 2	`Router(config-if)# tunnel udlr send-only ude_receive_only_port`	トンネルの送信専用インターフェイスを UDE 受信専用ポートと関連付けます。
ステップ 3	`Router(config-if)# ip address ipv4_address`	トンネル IPv4 アドレスを設定します。
ステップ 4	`Router(config-if)# tunnel source {ipv4_address | type number}`	トンネルの送信元を設定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ipv4_address}`	トンネルの宛先を設定します。
ステップ 6	`Router(config-if)# tunnel udlr address-resolution`	ARP および NHRP をイネーブルにします。

次に、UDE および UDLR の設定例を示します。

- ルータ A の場合
  - Open Shortest Path First（OSPF）および Protocol Independent Multicast（PIM）が設定されています。
  - 10 ギガビット イーサネット ポート 1/1 が送信専用 UDE ポートになります。
  - UDLR バック チャネル トンネルが受信専用として設定され、10 ギガビット イーサネット ポート 1/1 に関連付けられます。
- ルータ B の場合
  - OSPF および PIM が設定されます。
  - 10 ギガビット イーサネット ポート 1/2 が受信専用 UDE ポートになります。
  - UDLR バック チャネル トンネルが送信専用として設定され、10 ギガビット イーサネット ポート 1/2 に関連付けられます。
  - ARP および NHRP がイネーブルになります。

ルータ A の設定

```
ip multicast-routing
!
! tengigabitethernet 1/1 is send-only
!
interface tengigabitethernet 1/1
 unidirectional send-only
 ip address 10.1.0.1 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as receive-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 11.0.0.1
 tunnel destination 11.0.0.2
 tunnel udlr receive-only tengigabitethernet 1/1
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

ルータ B の設定

```
ip multicast-routing
!
! tengigabitethernet 1/2 is receive-only
!
interface tengigabitethernet 1/2
 unidirectional receive-only
 ip address 10.1.0.2 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as send-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 11.0.0.2
 tunnel destination 11.0.0.1
 tunnel udlr send-only tengigabitethernet 1/2
 tunnel udlr address-resolution
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

CHAPTER 24

ポリシー フィーチャ カード（PFC）3BXL および PFC3B モード マルチプロトコル ラベル スイッチング（MPLS）の設定

この章では、Catalyst 6500 シリーズ スイッチに Policy Feature Card（PFC; ポリシー フィーチャ カード）3BXL および PFC3B モード Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を設定する方法について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

PFC3BXL および PFC3B モード MPLS ラベル スイッチングの設定

ここでは、PFC3BXL および PFC3B モード MPLS ラベル スイッチングについて説明します。

MPLS の概要

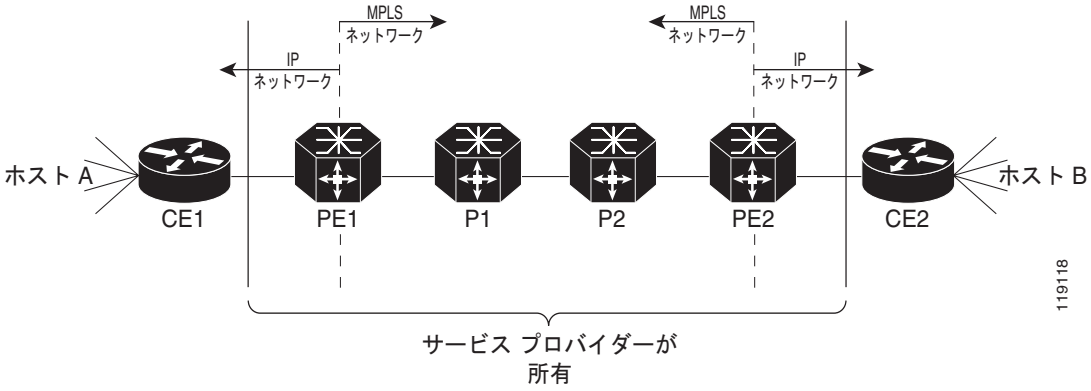
MPLS はラベル スイッチングを使用して、Packet-over-SONET（POS）、フレーム リレー、Asynchronous Transfer Mode（ATM; 非同期転送モード）、イーサネットなどのさまざまなリンク レベル テクノロジーを介してパケットを転送します。ラベルはグループ化または Forwarding Equivalence Class（FEC）に基づいて、パケットに割り当てられます。ラベルはレイヤ 2 ヘッダーとレイヤ 3 ヘッダーの間に追加されます。

MPLS ネットワークでは、Label Edge Router（LER; ラベル エッジ ルータ）が着信ラベルのラベル検索を実行し、着信ラベルを発信ラベルに切り替えて、パケットを Label Switch Router（LSR; ラベル スイッチ ルータ）のネクストホップに送信します。パケットに対してラベルがインポーズ（プッシュ）されるのは、MPLS ネットワークの入力エッジ上に限ります。出力エッジでは、ラベルが削除（ポップ）されます。コア ネットワーク LSR（プロバイダーまたは P ルータ）はラベルを読み取り、適切なサービスを適用し、ラベルに基づいてパケットを転送します。

着信ラベルには集約または非集約の 2 つのタイプがあります。集約ラベルの場合、ネクストホップおよび発信インターフェイスを検出するときに、IP 検索によって着信 MPLS パケットをスイッチングする必要があります。非集約ラベルの場合、パケットに IP ネクストホップ情報が格納されます。

図 24-1 に、カスタマー ネットワークの 2 つのサイトを接続する、サービス プロバイダーの MPLS ネットワークを示します。

図 24-1　　MPLS ネットワーク



MPLS の詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagov.htm

PFC3BXL および PFC3B モード MPLS ラベル スイッチングの概要

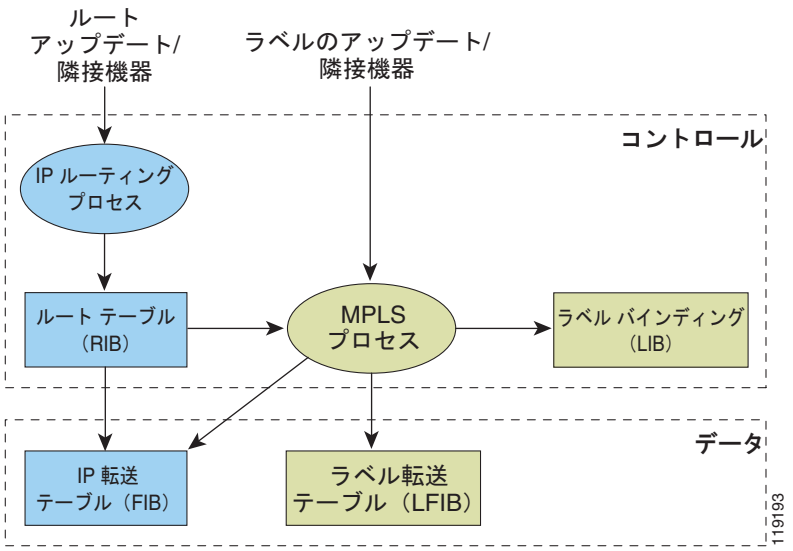
PFC3BXL または PFC3B モードは、レイヤ 3 MPLS Virtual Private Network（VPN; バーチャル プライベート ネットワーク）やレイヤ 2 Ethernet over MPLS（EoMPLS）をサポートし、Quality of Service（QoS; サービス品質）やセキュリティに対応しています。

スーパーバイザ エンジン上の Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）は、アドレス解決やルーティング プロトコルなどのレイヤ 3 コントロール プレーン機能を実行します。MSFC はルーティング プロトコルおよび Label Distribution Protocol（LDP; ラベル配布プロトコル）からの情報を処理し、IP 転送（Forwarding Information Base（FIB; 転送情報ベース））テーブルおよびラベル転送（Label Forwarding Information Base（LFIB; ラベル転送情報ベース））テーブルを構築します。MSFC は両方のテーブルの情報を PFC3BXL または PFC3B に配布します。

PFC3BXL または PFC3B は情報を取得し、FIB および LFIB テーブルのコピーを独自に作成します。また、これらのテーブルを組み合わせて FIB TCAM を作成します。DFC は Forwarding Information Base（FIB; 転送情報ベース）Ternary Content Addressable Memory（TCAM; Ternary CAM）テーブル内で、着信 IP パケットおよびラベル付きパケットを検索します。検索結果は、特定の隣接エントリへのポインタとして示されます。この隣接エントリには、ラベルのプッシュ（IP/MPLS パスの場合）、ラベルのスワップ（MPLS/MPLS パスの場合）、ラベルのポップ（MPLS/IP パスの場合）、カプセル化に関する適切な情報が含まれます。

図 24-2 に、PFC3BXL および PFC3B モード MPLS ラベル スイッチングをサポートする各機能ブロックを示します。ルーティング プロトコルは、IP および MPLS データ パケットの転送に使用する Routing Information Base（RIB）を生成します。Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の場合、必要なルーティング情報が RIB から抽出されて、転送情報ベース（FIB）に構築されます。ラベル配布プロトコル（LDP）は RIB からルートを取得して、ラベル スイッチ パスを介してラベルを配布し、各 LSR および LER 内にラベル転送情報ベース（LFIB）を構築します。

図 24-2　　MPLS 転送、制御、データ プレーン



IP/MPLS

PFC3BXL または PFC3B は MPLS ネットワークへの入口で IP パケットを調べて、FIB TCAM 内でルートを検索します。検索結果は、特定の隣接エントリへのポインタとして示されます。隣接エントリには、ラベルのプッシュ（IP/MPLS パスの場合）およびカプセル化に関する適切な情報が含まれます。PFC3BXL または PFC3B は、MPLS パケットのスイッチングに必要なインポジション ラベルを含めた結果を生成します。

（注）　MPLS 負荷分散が設定されている場合、隣接は負荷分散パスを指すことがあります。「基本的な MPLS ロード バランシング」（P.24-9）を参照してください。

MPLS/MPLS

PFC3BXL または PFC3B は MPLS ネットワークのコアで最上位ラベルを使用して、FIB TCAM 内で検索を実行します。正常な検索結果が指す隣接は、パケット内の最上位ラベルを、ダウンストリーム ラベル スイッチ ルータ（LSR）によってアドバタイズされた新しいラベルで置き換えます。ルータが直前ホップ LSR ルータ（出力 LER の次のアップストリーム LSR）である場合、隣接は PFCBXL に最上位ラベルをポップするように指示します。これにより、VPN または Any Transport over MPLS（AToM）で使用するラベルが残っている MPLS パケット、またはネイティブ IP パケットが作成されます。

MPLS/IP

MPLS ネットワークの出口での処理には複数の方法があります。

ネイティブ IP パケットの場合（直前ルータがラベルをポップした場合）、PFC3BXL または PFC3B は FIB TCAM 内でルートを検索します。

MPLS VPN パケットの場合、Interior Gateway Protocol（IGP）ラベルが直前ルータでポップされたあとに、VPN ラベルが残ります。PFC3BXL または PFC3B が実行する処理は、VPN ラベル タイプによって異なります。集約ラベルを伝送するパケットでは、集約ラベルをポップしたあとに、IP ヘッダーに基づいてさらに検索する必要があります。非集約ラベルの場合、PFC3BXL または PFC3B は FIB TCAM 内でルートを検索し、IP ネクストホップ情報を取得します。

IGP ラベルおよび VPN ラベルが添付されたパケットの場合、Penultimate Hop Popping（PHP）が発生しなければ、パケットは VPN ラベルの上部で明示的 Null ラベルを伝送します。PFC3BXL または PFC3B は FIB TCAM 内で最上位ラベルを検索し、パケットを再循環させます。それから、PFC3BXL または PFC3B は上記段落の説明に従い、集約ラベルであるか非集約ラベルであるかに応じて残りのラベルを処理します。

EoMPLS、MPLS、MPLS VPN の場合、明示的 Null ラベルが添付されたパケットについて、MPLS は同様に処理されます。

MPLS VPN 転送

VPN ラベルには、直接接続されたネットワークまたは集約ルート用の集約ラベルと、非集約ラベルの 2 種類があります。集約ラベルを伝送するパケットでは、集約ラベルをポップしたあとに、IP ヘッダーに基づいてさらに検索する必要があります。VPN 情報（VPN-IPv4 アドレス、拡張コミュニティ、ラベル）は Multiprotocol Border Gateway Protocol（MBGP）によって配布されます。

再循環

場合によって、PFC3BXL または PFC3B はパケットの再循環機能を提供します。再循環を使用すると、Access Control List（ACL; アクセス制御リスト）または QoS TCAM、NetFlow テーブル、または FIB TCAM テーブル内で追加検索を実行できます。再循環は次の場合に必須です。

- 4 つ以上のラベルをインポジションにプッシュする場合
- 3 つ以上のラベルをディスポジションにポップする場合
- 最上位の明示的 Null ラベルをポップする場合
- VPN Routing and Forwarding（VRF; VPN ルーティング/転送）番号が 511 を超える場合
- 出力インターフェイスの IP ACL の場合（非集約（プレフィクス単位）ラベル専用）

パケット再循環が発生するのは、特定のパケット フローに対してのみです。その他のパケット フローには影響しません。パケットの書き換えはモジュールで行われます。書き換えられたパケットは PFC3BXL または PFC3B に転送されて、さらに処理されます。

サポートされるハードウェア機能

次のハードウェア機能がサポートされています。

- ラベル処理 - 任意の個数のラベルをプッシュまたはポップできます。ただし、最適な結果を得るために、同じ処理内でプッシュするラベル数を最大 3 つ、ポップするラベル数を最大 2 つにしてください。
- IP/MPLS パス - IP パケットを受信して、MPLS パスに送信できます。
- MPLS/IP パス - ラベル付きパケットを受信して、IP パスに送信できます。
- MPLS/MPLS パス - ラベル付きパケットを受信して、そのラベル パスに送信できます。
- MPLS Traffic Engineering（MPLS TE）- MPLS バックボーンは、レイヤ 2 Asynchronous Transfer Mode（ATM; 非同期転送モード）およびフレーム リレー ネットワークのトラフィック エンジニアリング機能を反復および拡張できます。
- Time to Live（TTL; 存続可能時間）処理 - MPLS ネットワークの入口では、MPLS フレーム ヘッダーの TTL 値を、IP パケット ヘッダーの TTL フィールド、または隣接エントリのユーザ設定値から取得できます。MPLS ネットワークの出口では、最終 TTL はラベル TTL と IP TTL のいずれか小さい方の値から 1 を引いた値になります。

（注） 均一モードでは、TTL は IP TTL から取得されます。パイプ モードでは、ハードウェア レジスタから取得した値 255 が発信ラベルに使用されます。

- QoS - IP パケットから取得した Differentiated Services（DiffServ; 差別化したサービス）および Type of Service（ToS; サービス タイプ）に関する情報を、MPLS EXP フィールドにマッピングできます。
- MPLS/VPN サポート - 最大 1024 個の VRF をサポートできます（VRF が 511 個を超える場合、再循環する必要があります）。
- Ethernet over MPLS - MPLS ドメインの入口でイーサネット フレームをカプセル化し、出口でカプセル開放できます。
- パケット再循環 - PFC3BXL または PFC3B にはパケット再循環機能があります （「再循環」（P.24-5）を参照）。
- MPLS スイッチング設定は、**mpls ip** コマンドを使用した VLAN インターフェイスでサポートされます。

サポートされる Cisco IOS 機能

PFC3BXL または PFC3B モードでは、次の Cisco IOS ソフトウェア機能がサポートされています。

（注）　Customer Edge（CE; カスタマー エッジ）ルータ（VRF Lite）の Multi-VPN Routing and Forwarding（Multi-VRF）は、VRF インターフェイス間の IPv4 転送、IPv4 ACL、および IPv4 Hot Standby Router Protocol（HSRP）機能とともにサポートされています。IPv4 マルチキャストはサポートされていません。

- CE ルータ（VRF Lite）の Multi-VRF - VRF Lite は、サービス プロバイダーが複数の VPN をサポートして（VRF ベース IPv4 のみを使用）、IP アドレスを重複使用できるようにするための機能です。次のマニュアルを参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html

- シスコ製ルータ上の MPLS - この機能は、ラベル エッジ ルータ（LER）で IP パケットのラベルをインポーズしたり削除したり、ラベル スイッチ ルータ（LSR）でラベルをスイッチングするための、基本的な MPLS サポートを提供します。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st21/fs_rtr.htm

- MPLS TE - MPLS トラフィック エンジニアリング ソフトウェアにより、MPLS バックボーンはレイヤ 2 ATM およびフレーム リレー ネットワークのトラフィック エンジニアリング機能を反復および拡張できます。したがって、MPLS トラフィック処理により従来のレイヤ 2 機能をレイヤ 3 トラフィック フローでも利用できます。詳細については、以下のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm

  http://www.cisco.com/warp/public/105/mplsteisis.html

  http://www.cisco.com/warp/public/105/mpls_te_ospf.html

- MPLS TE DiffServ 認識（DS-TE）- この機能は、MPLS TE に対する拡張を提供し、これを DiffServ 認識にして、保証されたトラフィックの制約に基づくルーティングを可能にします。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsdserv3.htm

- MPLS TE 転送隣接 - この機能により、ネットワーク管理者はトラフィック エンジニアリングである Label-Switched Path（LSP; ラベル スイッチド パス）トンネルを、Shortest Path First（SPF）アルゴリズムに基づいた Interior Gateway Protocol（IGP）ネットワーク内のリンクとして処理できます。Intermediate System-to-Intermediate System（IS-IS）を用いた転送隣接の詳細については、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fstefa_3.htm

- MPLS TE Interarea トンネル - この機能により、ルータは複数の Interior Gateway Protocol（IGP）領域およびレベルにまたがる MPLS TE トンネルを確立して、トンネルの最初と最後のルータを同じ領域におく必要がある制約事項を削除できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/fsiarea3.htm

- MPLS バーチャル プライベート ネットワーク（VPN）- この機能を使用すると、Cisco IOS ネットワーク上に容易に拡張できる IPv4 レイヤ 3 VPN バックボーン サービスを導入することが可能です。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st21/fs_vpn.htm

- MPLS VPN Carrier Supporting Carrier（CSC）- この機能を使用すると、MPLS VPN ベース サービス プロバイダーは、バックボーン ネットワークのセグメントの使用を他のサービス プロバイダーに許可できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftcsc8.htm

- MPLS VPN Supporting Carrier IPv4 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ラベル配布 - この機能を使用すると、ボーダー ゲートウェイ プロトコル（BGP）がバックボーン キャリア Provider Edge（PE; プロバイダー エッジ）ルータとカスタマー キャリア カスタマー エッジ（CE）ルータ間でルートおよび MPLS ラベルを送信できるように、ご使用の CSC ネットワークを設定できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftcscl13.htm

- MPLS VPN Interautonomous System（InterAS）のサポート - この機能を使用すると、MPLS VPN をサービス プロバイダーおよび Autonomous System（AS; 自律システム）に拡張できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/fsias24.htm

- MPLS VPN InterAS IPv4 BGP ラベル配布 - この機能を使用すると、Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）が IPv4 ルートを PE ルータの MPLS ラベルと交換できるように、VPN サービス プロバイダー ネットワークを設定できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftiasl13.htm

- MPLS VPN Hot Standby Router Protocol（HSRP）のサポート - この機能を使用すると、グローバル ルーティング テーブルではなく、正しい IP ルーティング テーブルに、HSRP 仮想 IP アドレスが追加されます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_hsmp.htm

- MPLS VPN の Open Shortest Path First（OSPF）模造リンク サポート - この機能を使用すると、模造リンクを使用して、Open Shortest Path First（OSPF）プロトコルが稼動する VPN クライアント サイトに接続し、MPLS VPN コンフィギュレーション内で OSPF リンクを共有できます。次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ospfshmk.htm

- Any Transport over MPLS（AToM）- MPLS バックボーン上でレイヤ 2 パケットを送信します（「Any Transport over MPLS（AtoM）」（P.24-15）を参照）。

MPLS の注意事項および制約事項

PFC3BXL または PFC3B MPLS を設定する場合、次の注意事項および制約事項に注意してください。

- PFC3BXL または PFC3B モードでは、最大 8 個の負荷分散パスをサポートできます。他のプラットフォーム用の Cisco IOS リリースでサポートできる負荷分散パスは、8 個のみです。
- PFC3BXL または PFC3B モードは、Maximum Transmission Unit（MTU; 最大伝送ユニット）のチェックおよびフラグメンテーションをサポートします。

（注）　フラグメンテーションは（IP/MPLS パスの）ソフトウェアでサポートされます。『*Cisco IOS Master Command List*, Release 12.2SX』の **mtu** コマンドを参照してください。

（注）　その他の制限および制約事項については、「MPLS VPN の注意事項および制約事項」（P.24-12）および「EoMPLS の注意事項および制約事項」（P.24-16）を参照してください。

PFC3BXL および PFC3B モード MPLS でサポートされるコマンド

PFC3BXL および PFC3B モード MPLS では、次のコマンドがサポートされます。

- **mpls ip default route**
- **mpls ip propagate-ttl**
- **mpls ip ttl-expiration pop**
- **mpls label protocol**
- **mpls label range**
- **mpls ip**
- **mpls label protocol**
- **mpls mtu**

詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r/index.htm

MPLS の設定

MPLS の設定手順については、次の URL にある『*Multiprotocol Label Switching on Cisco Routers*』のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm

MPLS のラベル単位ロード バランシング

ここでは、基本的な MPLS、MLPS レイヤ 2 VPN、MPLS レイヤ 3 VPN ロード バランシングの情報について説明します。

基本的な MPLS ロード バランシング

ロード バランシング パスの最大数は 8 です。PFC3BXL または PFC3B は、明示的に設定されていない場合でも MPLS ラベルの付けられたパケットを転送します。パケットに添付されたラベルが 3 つ以下で、基礎となるパケットが IPv4 の場合、PFC3BXL または PFC3B は送信元および宛先 IPv4 アドレスを使用します。基礎となるパケットが IPv4 でなく、4 つ以上のラベルが存在する場合、PFC3BXL または PFC3B は 5 番目または最下位ラベルまでを解析して、ハッシュに使用します。

MPLS レイヤ 2 VPN ロード バランシング

カスタマー イーサネット フレームの Media Access Control（メディア アクセス制御）アドレスの最初のニブルが 4 以外の場合、ロード バランシングは MPLS コアの Virtual Circuit（VC; バーチャル サーキット）ラベルに基づきます。

（注）　レイヤ 2 VPN の場合、入力 PE ではロード バランシングはサポートされません。

MPLS レイヤ 3 VPN ロード バランシング

MPLS レイヤ 3 VPN ロード バランシングは、基本的な MPLS ロード バランシングと類似しています。詳細については、「基本的な MPLS ロード バランシング」（P.24-9）を参照してください。

MPLS の設定例

次に、MPLS の基本設定の例を示します。

```
*****
Basic MPLS
*****


IP ingress interface:

Router# mpls label protocol ldp

interface GigabitEthernet6/2
 ip address 75.0.77.1 255.255.255.0
 media-type rj45
 speed 1000
end

Label egress interface:

interface GigabitEthernet7/15
 mtu 9216
 ip address 75.0.67.2 255.255.255.0
 logging event link-status
 mpls ip
```

```
Router# show ip route 188.0.0.0
Routing entry for 188.0.0.0/24, 1 known subnets

O IA    188.0.0.0 [110/1] via 75.0.77.2, 00:00:10, GigabitEthernet6/2


Router#sh ip ro 88.0.0.0
Routing entry for 88.0.0.0/24, 1 known subnets

O E2    88.0.0.0 [110/0] via 75.0.67.1, 00:00:24, GigabitEthernet7/15
                 [110/0] via 75.0.21.2, 00:00:24, GigabitEthernet7/16
Router#


Router# show mpls forwarding-table 88.0.0.0
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
30     50          88.0.0.0/24       0          Gi7/15     75.0.67.1
       50          88.0.0.0/24       0          Gi7/16     75.0.21.2


Router# show mls cef 88.0.0.0 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(3223   ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3223   ): 8 | 1 0    0 0 0 0   88.0.0.0           (A:344105 ,P:1,D:0,m:1 ,B:0 )
M(3223   ): E | 1 FFF  0 0 0 255.255.255.0
V(3223   ): 9 | 1 0    0 0 0 88.0.0.0 (V0:0    ,C0:0 ,V1:0    ,C1:0 ,RVTEN:0 ,RVTSEL:0  )
Router# show mls cef adj ent 344105

Index: 344105  smac: 0005.9a39.a480, dmac: 000a.8ad8.2340
               mtu: 9234, vlan: 1031, dindex: 0x0, l3rw_vld: 1
               packets: 109478260, bytes: 7006608640

Router# show mls cef adj ent 344105 de

Index: 344105  smac: 0005.9a39.a480, dmac: 000a.8ad8.2340
               mtu: 9234, vlan: 1031, dindex: 0x0, l3rw_vld: 1
               format: MPLS, flags: 0x1000008418
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 50, exp: 0, ovr: 0
               op: PUSH_LABEL2
               packets: 112344419, bytes: 7190042816
```

PFC3BXL または PFC3B モード VPN スイッチング

ここでは、PFC3BXL または PFC3B モード VPN スイッチングについて説明します。

PFC3BXL または PFC3B モード VPN スイッチング処理

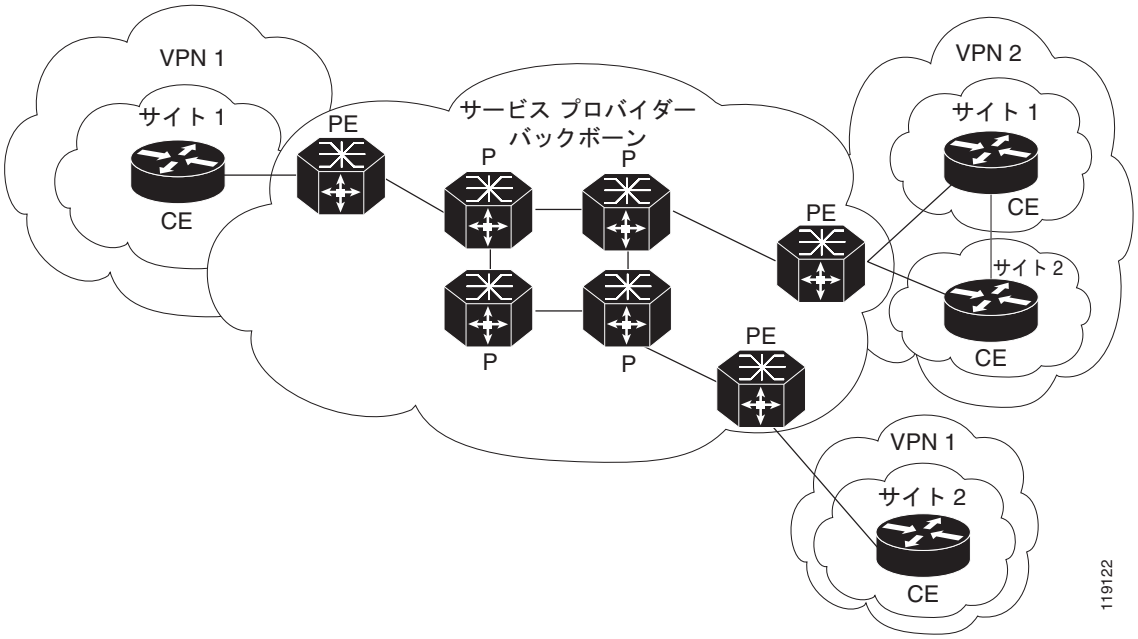
MPLS の IP VPN 機能により Cisco IOS ネットワークは、拡張が容易な IP レイヤ 3 VPN バックボーン サービスを共有インフラストラクチャに配置された複数のサイトに展開し、同時にプライベート ネットワークと同じアクセスまたはセキュリティを提供できます。MPLS テクノロジーに基づいた VPN には、ルーティングの隔離、セキュリティの向上、ルーティングの簡素化、スケーラビリティの向上という利点があります。

MPLS VPN の概要および詳細な設定については、次の URL にある Cisco IOS ソフトウェア マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/index.htm

図 24-3 に、一般的な MPLS VPN ネットワーク トポロジを示します。

図 24-3　　VPN およびサービス プロバイダー バックボーン



PFC3BXL または PFC3B は、入力 PE でパケット ヘッダーに基づいて転送を判断します。PFC3BXL または PFC3B には、VLAN を VPN にマッピングするテーブルが含まれます。Catalyst 6500 シリーズ スイッチ アーキテクチャでは、システム内のすべての物理入力インターフェイスが特定の VPN に関連付けられます。PFC3BXL または PFC3B は CEF テーブル内で IP 宛先アドレスを検索しますが、対象となるのは特定の VPN 内のプレフィクスのみです（テーブル エントリは特定の隣接セットを指します。複数のパラレル パスが存在する場合は、ロード バランシング判断によって特定の隣接が選択されます）。

テーブル エントリには、パケットに必要なレイヤ 2 ヘッダー情報、およびフレームにプッシュされる特定の MPLS ラベルが含まれます。パケット書き換え用のこの情報は、入力ライン カードに送信されて書き換えが行われ、出力ライン インターフェイスに転送されます。

VPN トラフィックはプレフィクス単位のラベルまたは集約ラベルに基づいて、PE からの出口で処理されます。プレフィクス単位のラベルが使用される場合、各 VPN プレフィクスには一意のラベルが関連付けられます。これにより、PE は FIB 内のラベル検索に基づいて、パケットを最終宛先に転送できます。

（注）　PFC3BXL または PFC3B が割り当てるのは、VRF ごとに 1 つの集約ラベルのみです。

出力 PE のディスポジションに集約ラベルが使用される場合、複数のインターフェイスの多数のプレフィクスをこのラベルに関連付けることができます。この場合、PFC3BXL または PFC3B は IP 検索を実行して最終宛先を判別する必要があります。IP 検索では再循環を必要とする場合があります。

MPLS VPN の注意事項および制約事項

MPLS VPN を設定する際に、以下の注意事項と制約事項に従ってください。

- PFC3BXL または PFC3B モードでは、拡張 Optical Services Module（OSM; オプティカル サービス モジュール）を使用してシャーシごとに合計 1024 個の VRF をサポートします。非拡張 OSM を使用すると、システムはデフォルトの VRF 数 511 になります。
- PFC3BXL または PFC3B モードでは、VPN 数が 511 を超えると VPN が再循環されます。

PFC3BXL または PFC3B モード MPLS VPN でサポートされるコマンド

PFC3BXL および PFC3B モード MPLS VPN では、次のコマンドがサポートされます。

- **address-family**
- **exit-address-family**
- **import map**
- **ip route vrf**
- **ip route forwarding**
- **ip vrf**
- **neighbor activate**
- **rd**
- **route-target**

詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r/index.htm

MPLS VPN の設定

MPLS VPN の設定手順については、次の URL にある『*MPLS Virtual Private Networks*』フィーチャ モジュールを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagc.htm#63744

（注）　別の MPLS 装置とのレイヤ 2 ポート ピアリングを使用する MPLS アップリンクとしてレイヤ 3 VLAN インターフェイスを使用した場合、VRF インターフェイスとして別のレイヤ 3 VLAN を使用できます。

MPLS VPN の設定例

次に、LAN、OSM、および FlexWAN CE 方向のインターフェイスのコンフィギュレーション例を示します。PFC3BXL または PFC3B モード MPLS スイッチング コンフィギュレーションは、他のプラットフォームのコンフィギュレーションと同様です。

```
!ip vrf blues
 rd 100:10
 route-target export 100:1
 route-target import 100:1
!
mpls label protocol ldp
mpls ldp logging neighbor-changes
mls mpls tunnel-recir
!
interface Loopback0
 ip address 10.4.4.4 255.255.255.255
!
interface GigabitEthernet4/2
 description Catalyst link to P2
 no ip address
 mls qos trust dscp
!
interface GigabitEthernet4/2.42
 encapsulation dot1Q 42
 ip address 10.0.3.2 255.255.255.0
 tag-switching ip
!
interface GigabitEthernet7/3
 description Catalyst link to CE2
 no ip address
 mls qos trust dscp
!
interface GigabitEthernet7/3.73
 encapsulation dot1Q 73
 ip vrf forwarding blues
 ip address 10.19.7.1 255.255.255.0
!
interface POS8/1
 description OSM link to CE3
 ip vrf forwarding blues
 ip address 10.19.8.1 255.255.255.252
 encapsulation ppp
 mls qos trust dscp
 pos scramble-atm
 pos flag c2 22
```

```
!
interface POS9/0/0
 description FlexWAN link to CE1
 ip vrf forwarding blues
 ip address 10.19.9.1 255.255.255.252
 encapsulation ppp
 pos scramble-atm
 pos flag c2 22
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.4 0.0.0.0 area 0
 network 10.0.0.0 0.0.255.255 area 0
!
router ospf 65000 vrf blues
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 10.19.0.0 0.0.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.3.3.3 remote-as 100
 neighbor 10.3.3.3 description MP-BGP to PE1
 neighbor 10.3.3.3 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.3.3.3 activate
 neighbor 10.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf blues
 redistribute connected
 redistribute ospf 65000 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
!
```

Any Transport over MPLS（AtoM）

Any Transport over MPLS（AtoM）は、MPLS バックボーン上でレイヤ 2 パケットを送信します。AToM はエッジ ルータの間で転送されたラベル配布プロトコル（LDP）セッションを使用して、接続の設定およびメンテナンスを行います。2 つのレベルのラベルを使用して、エッジ ルータ間でスイッチングを行うと、転送が発生します。外部ラベル（トンネル ラベル）は、MPLS バックボーンを介して入力 PE から出力 PE にパケットをルーティングします。VC ラベルは、トンネル エンドポイント（出力 PE の特定の出力インターフェイスおよびイーサネット フレームの VLAN ID）で接続を判別する Demux ラベルです。

AToM は、PFC3BXL または PFC3B モードに関して次の類似したトランスポート タイプをサポートします。

- Ethernet over MPLS（EoMPLS）（VLAN モードおよびポート モード）
- DLCI 間接続による Frame Relay over MPLS（FRoMPLS）
- ATM AAL5 over MPLS
- ATM Cell Relay over MPLS

（注）　その他の AToM タイプが今後のリリースに組み込まれる予定です。

PFC3BXL または PFC3B モードは、ハードウェアベースの EoMPLS および OSM ベース、FlexWAN ベースまたは FlexWAN2 ベースの EoMPLS をサポートします。詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Ethernet_over_MPLS

Supervisor Engine 2 ベースの EoMPLS の要件の詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Supervisor_Engine_2-Based_EoMPLS

その他の AToM 実装（ATM AAL5 over MPLS、ATM Cell Relay over MPLS、Frame Relay over MPLS）については、以下のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Any_Transport_over_MPLS

ここでは、AToM について説明します。

- 「AToM ロード バランシング」（P.24-16）
- 「EoMPLS の概要」（P.24-16）
- 「EoMPLS の注意事項および制約事項」（P.24-16）
- 「EoMPLS の設定」（P.24-18）

AToM ロード バランシング

PFC3BXL または PFC3B モード EoMPLS の場合、トンネル入口ではロード バランシングは行われません。複数の IGP パスを使用できる場合でも、Interior Gateway Protocol（IGP）パスは 1 つのみ選択されますが、MPLS コアではロード バランシングを使用できます。

EoMPLS の概要

EoMPLS は AToM トランスポート タイプの 1 つです。AToM はエッジ ルータの間で転送された LDP セッションを使用して、MPLS バックボーンを介してレイヤ 2 パケットを転送し、接続を設定およびメンテナンスします。2 つのレベルのラベルを使用して、エッジ ルータ間でスイッチングを行うと、転送が発生します。外部ラベル（トンネル ラベル）は、MPLS バックボーンを介して入力 PE から出力 PE にパケットをルーティングします。VC ラベルは、トンネル エンドポイント（出力 PE の特定の出力インターフェイスおよびイーサネット フレームの VLAN ID）で接続を判別する Demux ラベルです。

EoMPLS は MPLS パケットにイーサネット Protocol Data Unit（PDU; プロトコル データ ユニット）をカプセル化し、MPLS ネットワーク上で転送することにより機能します。各 PDU は単一パケットとして送信されます。

（注）　同じ VLAN 上でローカルなレイヤ 2 スイッチングおよび EoMPLS を実行する場合は、OSM ベースの EoMPLS を使用してください。Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）に EoMPLS を設定する必要があります。コア方向のカードは OSM でなければなりません。ローカルなレイヤ 2 スイッチングが不要な場合、サブインターフェイスまたは物理インターフェイスに設定された PFC ベースの EoMPLS を使用してください。

EoMPLS の注意事項および制約事項

EoMPLS を設定する際に、以下の注意事項と制約事項に従ってください。

- 受信された最大のレイヤ 2 VLAN を伝送できるように、エンドポイント間のすべての中間リンクの最大伝送ユニット（MTU）を設定する必要があります。
- EoMPLS は、IEEE 802.1Q 標準に準拠する VLAN パケットをサポートします。802.1Q 仕様は、イーサネット フレームに VLAN メンバシップ情報を挿入する標準方式を確立します。
- QoS がグローバルにディセーブルになっている場合、802.1p および IP precedence ビットは両方とも保護されます。QoS がレイヤ 2 ポートでイネーブルになっている場合、802.1Q P ビットまたは IP precedence ビットのいずれかを、信頼できる設定を使用して保護できます。ただし、デフォルトでは、保護されていないビットは保護されたビットの値によって上書きされます。たとえば、P ビットが保護されている場合、IP precedence ビットは P ビットの値で上書きされます。PFC3BXL または PFC3B モードには、IP precedence ビットを保護しながら、P ビットを信頼できるようにする新しいコマンドが装備されています。IP precedence ビットを保護するには、**no mls qos rewrite ip dscp** コマンドを使用します。

（注）　**no mls qos rewrite ip dscp** コマンドは、MPLS および MPLS VPN 機能と互換性がありません。第 41 章「PFC QoS の設定」を参照してください。

（注）　同じシステム内で PFC ベースの EoMPLS サービスおよび PXF ベースの EoMPLS サービスを使用する場合は、**no mls qos rewrite ip dscp** コマンドを使用しないでください。

- プライベート VLAN では、EoMPLS はサポートされません。
- EoMPLS でトランクを使用する場合は、次の制約事項が適用されます。
  - EoMPLS クラウドでイーサネット 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）をサポートするには、MPLS VLAN 上のイーサネットのスーパーバイザ エンジン スパニング ツリーをディセーブルにする必要があります。これにより、EoMPLS VLAN のカスタマー スイッチへの伝送経路がトランクに限定されます。このようにしないと、BPDU はスーパーバイザ エンジンに転送され、EoMPLS クラウドに転送されません。
  - トランクのネイティブ VLAN を EoMPLS VLAN として設定しないでください。
- PFC3BXL または PFC3B モードでは、すべてのプロトコル（Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）、VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）、BPDU など）は無条件に MPLS クラウドでトンネリングされます。
- EoMPLS パケットを受信するインターフェイスでは、Inter-Switch Link（ISL; スイッチ間リンク）カプセル化はサポートされません。
- インターフェイス間では一意の VLAN が必要です。異なるインターフェイスで同じ VLAN を使用することはできません。
- PE 間のラベル スイッチド パス（LSP）を確保するには、ルーティング テーブルおよび CEF テーブル内の EoMPLS トンネル宛先ルートが / 32 アドレス（マスクが 255.255.255.255 であるホストアドレス）でなければなりません。
- 特定の EoMPLS 接続では、入力 PE の入力 EoMPLS インターフェイスおよび出力 PE の出力 EoMPLS インターフェイスを、dot1Q カプセル化が設定されたサブインターフェイスにする必要があります。このようにしないと、どちらもサブインターフェイスになりません。
- MPLS ネットワークに接続された発信インターフェイスがレイヤ 2 カードのポートである場合、802.1Q-in-802.1Q over EoMPLS がサポートされます。
- MPLS ネットワークに接続された出力インターフェイスがレイヤ 2 LAN ポート（PFC ベース EoMPLS と呼ばれるモード）である場合、EoMPLS トラフィックのシェーピングはサポートされません。
- PFC3BXL または PFC3B に基づいた EoMPLS では、宛先 MAC アドレスがローカルまたはリモート セグメント上にあるかどうかを判別するためのレイヤ 2 検索を実行しません。また、レイヤ 2 アドレス学習も実行しません（従来の LAN ブリッジングが実行します）。この機能（ローカル スイッチング）を使用できるのは、OSM および FlexWAN モジュールをアップリンクとして使用している場合のみです。
- AToM の旧リリースでは、AToM 回路を設定するのに使用するコマンドは **mpls l2 transport route** でした。このコマンドは、**xconnect** コマンドで置き換えられています。**xconnect** コマンドを使用して EoMPLS 回路を設定できます。
- AToM 制御ワードはサポートされていません。
- EoMPLS は、レイヤ 3 VLAN インターフェイスではサポートされません。
- ポイントツーポイント EoMPLS は、物理インターフェイスおよびサブインターフェイスと連動します。

EoMPLS の設定

ここでは、EoMPLS の設定手順について説明します。

前提条件

EoMPLS を設定する前に、ネットワークが次のように設定されていることを確認してください。

- PE ルータが IP 経由で相互に到達できるように、コアに IP ルーティングを設定します。
- PE ルータ間でラベル スイッチド パス（LSP）が存在するように、コアに MPLS を設定します。

EoMPLS は MPLS パケットにイーサネット PDU をカプセル化し、MPLS ネットワーク上で転送することにより機能します。各 PDU は単一パケットとして送信されます。PFC3BXL または PFC3B モードで EoMPLS を設定する場合、次の 2 つの方法を使用できます。

- VLAN モード - MPLS ネットワーク上の単一 VC を介して、送信元 802.1Q VLAN から宛先 802.1Q VLAN にイーサネット トラフィックをトランスポートします。VLAN モードは、デフォルトとして VC タイプ 5（dot1q タグなし）を使用します。リモート PE サブインターフェイス（VLAN）ベースの EoMPLS に対して VC タイプ 5 をサポートしない場合は、VC タイプ 4（トランスポート dot1 タグ）を使用します。
- ポート モード - ポートのすべてのトラフィックが MPLS ネットワーク上の単一 VC を共有できるようにします。ポート モードは VC タイプ 5 を使用します。

（注）

- VLAN モードおよびポート モードのどちらの場合も、ループバック ポートを使用しない限り、PFC3BXL および PFC3B モード EoMPLS はインターフェイス間におけるパケットのローカル スイッチングを許可しません。
- システムでは、OSM または FlexWAN 設定、および PFC3BXL または PFC3B モード設定を同時にイネーブルにできます。シスコはこの設定をサポートしますが、推奨しません。MPLS コアへのアップリンクが OSM または FlexWAN 対応インターフェイスを経由しない場合、OSM または FlexWAN ベースの EoMPLS 接続はアクティブになりません。このため、非 WAN インターフェイスに着信する OSM または FlexWAN ベースの EoMPLS に対応するパケットは廃棄されます。WAN（FlexWAN および OSM）EoMPLS の詳細については、以下のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Ethernet_over_MPLS

PFC3BXL または PFC3B モード は MPLS をサポートします。PFC3BXL または PFC3B モードでは、LAN ポートは OSM または FlexWAN モジュールを使用しなくても、レイヤ 2 トラフィックを受信し、ラベルをインポーズし、フレームを MPLS コアにスイッチングできます。

PFC3BXL または PFC3B モードでは、MPLS ネットワークのコア方向の OSM または FlexWAN モジュールを装備することができます。この場合、OSM 設定または FlexWAN 設定、あるいは PFC3BXL または PFC3B モード設定のいずれかを使用できます。詳細については、以下のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Ethernet_over_MPLS

PFC3BXL および PFC3B モード VLAN ベース EoMPLS の設定

PFC3BXL または PFC3B モード VLAN ベース EoMPLS を設定する場合、次の注意事項および制約事項 に注意してください。

- AToM 制御ワードはサポートされていません。
- ハードウェアレベルの Cyclic Redundancy Check（CRC; 巡回冗長検査）エラー、フレーミング エラー、ラント パケットを含むイーサネット パケットは、入力時に廃棄されます。
- サブインターフェイスに VLAN ベース EoMPLS を設定する必要があります。

PFC3BXL または PFC3B モード VLAN ベース EoMPLS を設定する場合、プロバイダー エッジ（PE）ルータで次の作業を行ってください。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface gigabitethernet`*slot/interface.subinterface*	ギガビット イーサネット サブインターフェイスを指定します。隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。
ステップ 3	`Router(config-if)# encapsulation dot1q` *vlan_id*	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS（EoMPLS）が稼動している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内に存在する必要があります。その他のすべてのサブインターフェイスおよびバックボーン ルータは、同じサブネット内に存在する必要はありません。
ステップ 4	`Router(config-if)# xconnect` *peer_router_id vcid* `encapsulation mpls`	接続回路を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

次に、PFC3BXL または PFC3B モード VLAN ベース EoMPLS 設定の例を示します。

```
!
interface GigabitEthernet7/4.2
encapsulation dot1Q 3
xconnect 13.13.13.13 3 encapsulation mpls
no shut
```

（注） IP アドレスは CE 装置のサブインターフェイス上で設定されます。

設定の確認

MPLS トンネルを介したレイヤ 2 VLAN トランスポートの設定を確認および表示するには、次の作業を行います。

- VLAN ごとの VLAN 名、ステータス、ポートを 1 行で表示するには、**show vlan brief** コマンドを使用します。

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active
2    VLAN0002                         active
3    VLAN0003                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- PE ルータ エンドポイントが相互に検出されたことを確認するには、**show mpls ldp discovery** コマンドを使用します。PE ルータが別の PE ルータから LDP Hello メッセージを受信した場合、そのルータおよび指定されたラベル スペースは「検出された」と見なされます。

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    13.13.13.13:0
    Discovery Sources:
    Interfaces:
        GE-WAN3/3 (ldp): xmit/recv
            LDP Id: 12.12.12.12:0
    Targeted Hellos:
        13.13.13.13 -> 11.11.11.11 (ldp): active/passive, xmit/recv
            LDP Id: 11.11.11.11:0
```

- ラベル配布セッションが確立されたことを確認するには、**show mpls ldp neighbor** コマンドを使用します。出力の 3 行目は、LDP セッションのステートが動作可能であり、メッセージが送受信中であることを示します。

```
Router# show mpls ldp neighbor
    Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 12.12.12.12.646 - 13.13.13.13.11010
        State: Oper; Msgs sent/rcvd: 1649/1640; Downstream
        Up time: 23:42:45
        LDP discovery sources:
          GE-WAN3/3, Src IP addr: 34.0.0.2
        Addresses bound to peer LDP Ident:
          23.2.1.14       37.0.0.2        12.12.12.12     34.0.0.2
          99.0.0.1
    Peer LDP Ident: 11.11.11.11:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 11.11.11.11.646 - 13.13.13.13.11013
        State: Oper; Msgs sent/rcvd: 1650/1653; Downstream
        Up time: 23:42:29
        LDP discovery sources:
          Targeted Hello 13.13.13.13 -> 11.11.11.11, active, passive
        Addresses bound to peer LDP Ident:
          11.11.11.11     37.0.0.1        23.2.1.13
```

- ラベル転送テーブルが正しく構築されたことを確認するには、**show mpls forwarding-table** コマンドを入力して、リモート PE のラベルが学習されたこと、およびこのラベルが正しいインターフェイスから正しいネクストホップに送信されていることを確認します。

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
16     Untagged    223.255.254.254/32   \
                                       0          Gi2/1      23.2.0.1
20     Untagged    l2ckt(2)            133093     Vl2        point2point
21     Untagged    l2ckt(3)            185497     Vl3        point2point
24     Pop tag     37.0.0.0/8          0          GE3/3      34.0.0.2
25     17          11.11.11.11/32      0          GE3/3      34.0.0.2
26     Pop tag     12.12.12.12/32      0          GE3/3      34.0.0.2
Router#
```

  出力では次のデータが表示されます。

  - Local tag - このルータによって割り当てられたラベル
  - Outgoing tag or VC - ネクストホップによって割り当てられたラベル
  - Prefix or Tunnel ID - このラベルが添付されたパケットの送信先アドレスまたはトンネル
  - Bytes tag switched - この着信ラベルによってスイッチングされるバイト数
  - Outgoing interface - このラベルが添付されたパケットが送信されるインターフェイス
  - Next Hop - 発信ラベルに割り当てられたネイバの IP アドレス

- 現在ルーティングされている VC のステートを表示するには、**show mpls l2transport vc** コマンドを入力します。

```
Router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Vl2            Eth VLAN 2           11.11.11.11     2          UP
Vl3            Eth VLAN 3           11.11.11.11     3          UP
```

各 VC の詳細情報を表示するには、**detail** キーワードを追加します。

```
Router# show mpls l2transport vc detail
Local interface: Vl2 up, line protocol up, Eth VLAN 2 up
  Destination address: 11.11.11.11, VC ID: 2, VC status: up
    Tunnel label: 17, next hop 34.0.0.2
    Output interface: GE3/3, imposed label stack {17 18}
  Create time: 01:24:44, last status change time: 00:10:55
  Signaling protocol: LDP, peer 11.11.11.11:0 up
    MPLS VC labels: local 20, remote 18
    Group ID: local 71, remote 89
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 1009, send 1019
    byte totals:   receive 133093, send 138089
    packet drops:  receive 0, send 0

Local interface: Vl3 up, line protocol up, Eth VLAN 3 up
  Destination address: 11.11.11.11, VC ID: 3, VC status: up
    Tunnel label: 17, next hop 34.0.0.2
    Output interface: GE3/3, imposed label stack {17 19}
  Create time: 01:24:38, last status change time: 00:10:55
  Signaling protocol: LDP, peer 11.11.11.11:0 up
    MPLS VC labels: local 21, remote 19
```

```
  Group ID: local 72, remote 90
  MTU: local 1500, remote 1500
  Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 1406, send 1414
  byte totals:   receive 185497, send 191917
  packet drops:  receive 0, send 0
```

PFC3BXL および PFC3B モード ポートベース EoMPLS の設定

PFC3BXL または PFC3B モード ポートベース EoMPLS を設定する場合、次の注意事項および制約事項 に注意してください。

- AToM 制御ワードはサポートされていません。
- ハードウェアレベルの巡回冗長検査（CRC）エラー、フレーミング エラー、ラント パケットを含むイーサネット パケットは、入力時に廃棄されます。
- ポートベース EoMPLS および VLAN ベース EoMPLS は相互に排他的な関係です。メイン インターフェイスでポートツーポート トランスポートをイネーブルにした場合、サブインターフェイスでのコマンドも入力できません。

PFC3BXL または PFC3B モードで EoMPLS による 802.1Q-in-802.1Q トラフィックおよびイーサネット トラフィックをサポートするには、次の作業を行って、ポートベースの EoMPLS を設定します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface gigabitethernet`*slot/interface*	ギガビット イーサネット インターフェイスを指定します。隣接 CE ルータのインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。
ステップ 3	`Router(config-if)# xconnect` *peer_router_id vcid* `encapsulation mpls`	接続回路を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

次に、ポートベースの基本設定の例を示します。

```
!
EoMPLS:

router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa8/48         Ethernet             75.0.78.1       1          UP
Gi7/11.2000    Eth VLAN 2000        75.0.78.1       2000       UP


Port-Based EoMPLS Config:

router# show run interface f8/48
Building configuration...

Current configuration : 86 bytes
!
interface FastEthernet8/48
 no ip address
```

```
 xconnect 75.0.78.1 1 encapsulation mpls
end

Sub-Interface Based Mode:
router# show run interface g7/11
Building configuration...

Current configuration : 118 bytes
!
interface GigabitEthernet7/11
 description Traffic-Generator
 no ip address
 logging event link-status
 speed nonegotiate
end

router# show run int g7/11.2000
Building configuration...

Current configuration : 112 bytes
!
interface GigabitEthernet7/11.2000
 encapsulation dot1Q 2000
 xconnect 75.0.78.1 2000 encapsulation mpls
end

kb7606# show mpls l2transport vc 1 detail
Local interface: Gi7/47 up, line protocol up, Ethernet up
  Destination address: 75.0.80.1, VC ID: 1, VC status: up
    Tunnel label: 5704, next hop 75.0.83.1
    Output interface: Te8/3, imposed label stack {5704 10038}
  Create time: 00:30:33, last status change time: 00:00:43
  Signaling protocol: LDP, peer 75.0.80.1:0 up
    MPLS VC labels: local 10579, remote 10038
    Group ID: local 155, remote 116
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 26, send 0
    byte totals:   receive 13546, send 0
    packet drops:  receive 0, send 0
```

VC タイプを取得するには、次のコマンドを使用します。

```
kb7606# remote command switch show mpls l2transport vc 1 de

Local interface: GigabitEthernet7/47, Ethernet
  Destination address: 75.0.80.1, VC ID: 1
  VC status: receive UP, send DOWN
  VC type: receive 5, send 5
    Tunnel label: not ready, destination not in LFIB
    Output interface: unknown, imposed label stack {}
    MPLS VC label: local 10579, remote 10038
  Linecard VC statistics:
    packet totals:  receive: 0  send: 0
    byte totals:  receive: 0  send: 0
    packet drops:  receive: 0  send: 0
  Control flags:
    receive 1,  send: 31
!
```

設定の確認

MPLS トンネルを介したレイヤ 2 VLAN トランスポートの設定を確認および表示するには、次の作業を行います。

- VLAN ごとの VLAN 名、ステータス、ポートを 1 行で表示するには、**show vlan brief** コマンドを使用します。

```
Router# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    VLAN0002                         active    Gi1/4
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- PE ルータ エンドポイントが相互に検出されたことを確認するには、**show mpls ldp discovery** コマンドを使用します。PE ルータが別の PE ルータから LDP Hello メッセージを受信した場合、そのルータおよび指定されたラベル スペースは「検出された」と見なされます。

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    13.13.13.13:0
    Discovery Sources:
    Interfaces:
        GE-WAN3/3 (ldp): xmit/recv
            LDP Id: 12.12.12.12:0
    Targeted Hellos:
        13.13.13.13 -> 11.11.11.11 (ldp): active/passive, xmit/recv
            LDP Id: 11.11.11.11:0
```

- ラベル配布セッションが確立されたことを確認するには、**show mpls ldp neighbor** コマンドを使用します。出力の 3 行目は、LDP セッションのステートが動作可能であり、メッセージが送受信中であることを示します。

```
Router# show mpls ldp neighbor
    Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 12.12.12.12.646 - 13.13.13.13.11010
        State: Oper; Msgs sent/rcvd: 1715/1706; Downstream
        Up time: 1d00h
        LDP discovery sources:
          GE-WAN3/3, Src IP addr: 34.0.0.2
        Addresses bound to peer LDP Ident:
          23.2.1.14       37.0.0.2        12.12.12.12     34.0.0.2
          99.0.0.1
    Peer LDP Ident: 11.11.11.11:0; Local LDP Ident 13.13.13.13:0
        TCP connection: 11.11.11.11.646 - 13.13.13.13.11013
        State: Oper; Msgs sent/rcvd: 1724/1730; Downstream
        Up time: 1d00h
        LDP discovery sources:
          Targeted Hello 13.13.13.13 -> 11.11.11.11, active, passive
        Addresses bound to peer LDP Ident:
          11.11.11.11     37.0.0.1        23.2.1.13
```

- ラベル転送テーブルが正しく構築されたかを確認するには、**show mpls forwarding-table** コマンドを入力します。

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix              Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        switched   interface
16     Untagged    223.255.254.254/32   \
                                   0          Gi2/1      23.2.0.1
20     Untagged    l2ckt(2)           55146580   Vl2        point2point
24     Pop tag     37.0.0.0/8         0          GE3/3      34.0.0.2
25     17          11.11.11.11/32     0          GE3/3      34.0.0.2
26     Pop tag     12.12.12.12/32     0          GE3/3      34.0.0.2
```

- 出力では次のデータが表示されます。
  - Local tag - このルータによって割り当てられたラベル
  - Outgoing tag or VC - ネクストホップによって割り当てられたラベル
  - Prefix or Tunnel ID - このラベルが添付されたパケットの送信先アドレスまたはトンネル
  - Bytes tag switched - この着信ラベルによってスイッチングされるバイト数
  - Outgoing interface - このラベルが添付されたパケットが送信されるインターフェイス
  - Next Hop - 発信ラベルに割り当てられたネイバの IP アドレス
- 現在ルーティングされている VC のステートを表示するには、**show mpls l2transport vc** コマンドを入力します。

```
Router# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Vl2            Eth VLAN 2           11.11.11.11     2          UP
```

CHAPTER 25

IPv4 マルチキャスト VPN（MVPN）サポートの設定

この章では、Catalyst 6500 シリーズ スイッチに IPv4 Multicast Virtual Private Network（MVPN; マルチキャスト VPN）サポートを設定する手順について説明します。Release12.2(18)SXE 以降のリリースでは、スイッチが Policy Feature Card（PFC; ポリシー フィーチャ カード）3B モードまたは PFC3BXL モードで動作している場合に MVPN がサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

MVPN の機能概要

ここでは MVPN について説明します。

MVPN の概要

MVPN は、標準ベースの機能で、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）クラウド全体に IPv4 マルチキャスト トラフィックを伝送します。Catalyst 6500 シリーズ スイッチの MVPN は、VPN を介してワイヤ速度でマルチキャスト トラフィックを転送するのに、IPv4 マルチキャスト トラフィックに対する既存の PFC ハードウェア サポートを使用します。MVPN は、レイヤ 3 IPv4 VPN を介した IPv4 マルチキャスト トラフィックのサポートを既存の IPv4 ユニキャスト サポートに追加します。

MVPN は、個別の VPN Routing and Forwarding（VRF; VPN ルーティング/転送）インスタンスのマルチキャスト パケットをルーティングし転送するだけでなく、サービス プロバイダー バックボーン全体に VPN トンネルを介してマルチキャスト パケットを伝送します。

MVPN は、IP-in-IP Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルに置き換わるものです。GRE トンネルは、簡単に拡張できるソリューションではなく、提供する粒度にも制限があります。

マルチキャスト ルーティング/転送とマルチキャスト ドメイン

MVPN は、マルチキャスト ルーティング情報を VRF テーブルに追加します。Provider Edge（PE; ）ルータがマルチキャスト データまたは制御パケットを Customer Edge（CE; カスタマー エッジ）ルータから受信すると、Multicast VRF（MVRF; マルチキャスト VRF）内の情報に応じて転送が実行されます。

（注）　MVRF は、Multicast over VRF-Lite とも呼ばれます。

各 MVRF では、特定の VRF インスタンスに必要なルーティング/転送情報を保持しています。MVRF は、マルチキャスト ルーティングがイネーブルになる以外は、既存の VRF と同じ方法で作成、設定されます。

マルチキャスト ドメインは、MPLS ネットワーク内で互いにマルチキャスト トラフィックを送信できるホストのセットを構成します。たとえば、特定のタイプのマルチキャスト トラフィックを全社の従業員に送信したい企業向けのマルチキャスト ドメインは、その企業に関連しているすべての CE ルータで構成されます。

マルチキャスト分散ツリー

MVPN 機能は、各マルチキャスト ドメインに対して少なくとも 1 つの Multicast Distribution Tree（MDT; マルチキャスト分散ツリー）を作成します。MDT は、異なる PE ルータにある同じ MVRF を相互接続するために必要な情報を提供します。

MVPN は、次の 2 種類の MDT をサポートします。

- デフォルト MDT - デフォルト MDT は、Protocol Independent Multicast（PIM）制御メッセージの持続的なチャネルで、特定のマルチキャスト ドメイン内にあるすべての PE ルータ間の低帯域幅ストリームです。デフォルト MDT にあるすべてのマルチキャスト トラフィックは、ドメイン内にあるすべての他の PE ルータに複製されます。各 PE ルータは、ドメイン内にある他のすべての PE ルータから論理的に PIM ネイバ（1 ホップ先）として認識されます。
- データ MDT - データ MDT はオプションです。これをイネーブルにすると、フルモーション動画など、すべての PE ルータに送信する必要のない高帯域幅伝送用の最適パスを提供するように、動的に作成されます。これにより、PE ルータ間で高帯域幅トラフィックのオンデマンド転送が可能になり、作成されるすべての高帯域幅ストリームによってすべての PE ルータがフラッディングしないようにできます。

データ MDT を作成するには、マルチキャスト ストリームを定期的にバックボーンに転送する各 PE ルータが、各デフォルト MDT で送信されるトラフィックを次のように検査します。

1. 各 PE ルータが定期的（ソフトウェア スイッチングで約 10 秒ごと、ハードウェア スイッチングで 90 秒ごと）にマルチキャスト トラフィックをサンプリングして、マルチキャスト ストリームが設定されたスレッシュホールドを超過しているかどうかを判別します （ストリームをサンプリングする時間によっては、最悪の場合、高帯域幅ストリームが検出されるまでに 180 秒かかる可能性があります）。

   （注） データ MDT は、VRF マルチキャスト ルーティング テーブル内の（S, G）マルチキャスト ルート エントリに対してのみ作成されます。これらは、（*, G）エントリに対して作成されません。

2. 特定のマルチキャスト ストリームが定義されたスレッシュホールドを超過した場合、この特定のマルチキャスト トラフィックに対して送信側 PE ルータは動的にデータ MDT を作成します。
3. 次に送信側 PE ルータは DATA-MDT JOIN 要求（ポート 3232 への User Datagram Protocol（UDP; ユーザ データグラム プロトコル）メッセージ）を他の PE ルータに送信し、新しいデータ MDT について通知します。
4. 受信側 PE ルータは、VRF ルーティング テーブルを検査して、このデータ ストリームの受信対象がいるかどうかを判断します。いる場合、受信側 PE ルータは、ストリームを受け入れるために、PIM プロトコルを使用して（グローバル テーブル PIM インスタンス内にある）この特定のデータ MDT グループの PIM JOIN メッセージを伝送します。現在このストリームの対象がいないルータも、あとでこのストリームを要求することがある場合に備えて情報をキャッシュし続けます。
5. DATA-MDT JOIN メッセージを送信してから 3 秒後に、送信側 PE ルータは高帯域幅マルチキャスト ストリームをデフォルト MDT から削除して、新しいデータ MDT の伝送を開始します。
6. 送信側 PE ルータは、マルチキャスト ストリームが定義したスレッシュホールドを超過し続ける間、DATA-MDT JOIN メッセージを 60 秒ごとに送信し続けます。ストリームがスレッシュホールドを 60 秒以上下回った場合、送信側 PE ルータは DATA-MDT JOIN メッセージの送信を停止して、ストリームをデフォルトの MDT に戻します。
7. 受信側ルータは、DATA-MDT JOIN メッセージを 3 分以上受信しなくなると、デフォルト MDT のキャッシュ情報を期限切れにします。

データ MDT は、MPLS VPN コア内で、最適なトラフィック転送を保証しながら VPN 内の高帯域ソースを許可します。

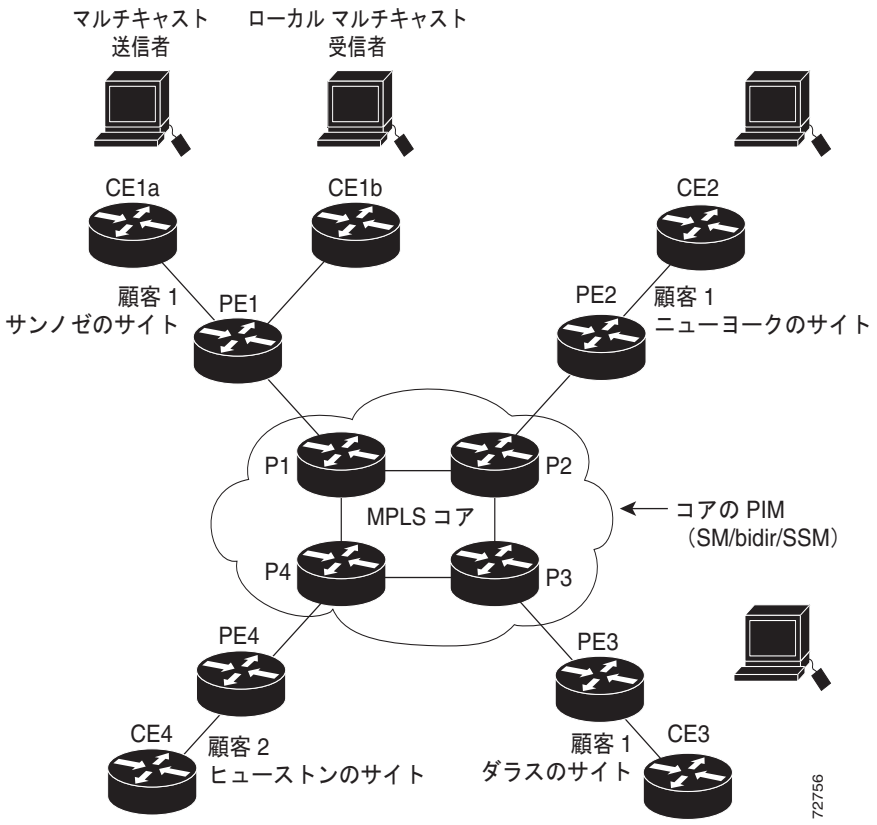
（注）　DATA-MDT JOIN メッセージとその他のデータ MDT 作成および使用法に関する技術情報については、Eric C. Rosen 他によるインターネット ドラフト『*Multicast in MPLS/BGP IP VPNs*』を参照してください。

以下の例では、サービス プロバイダーに San Jose、New York、および Dallas にオフィスを持つマルチキャスト カスタマーがいます。San Jose サイトでは、一方向のマルチキャスト プレゼンテーションを伝送します。サービス プロバイダー ネットワークは、このカスタマーに関連した 3 つのサイトすべてをサポートし、さらに他の企業の Houston サイトもサポートしています。

この企業のデフォルト MDT は、プロバイダー ルータ P1、P2、および P3 と、関連する PE ルータで構成されています。PE4 は MPLS コア内にあるこれらの他のルータと相互接続しています。ただし、PE4 は別のカスタマーに関連し、したがってデフォルト MDT の一部ではありません。

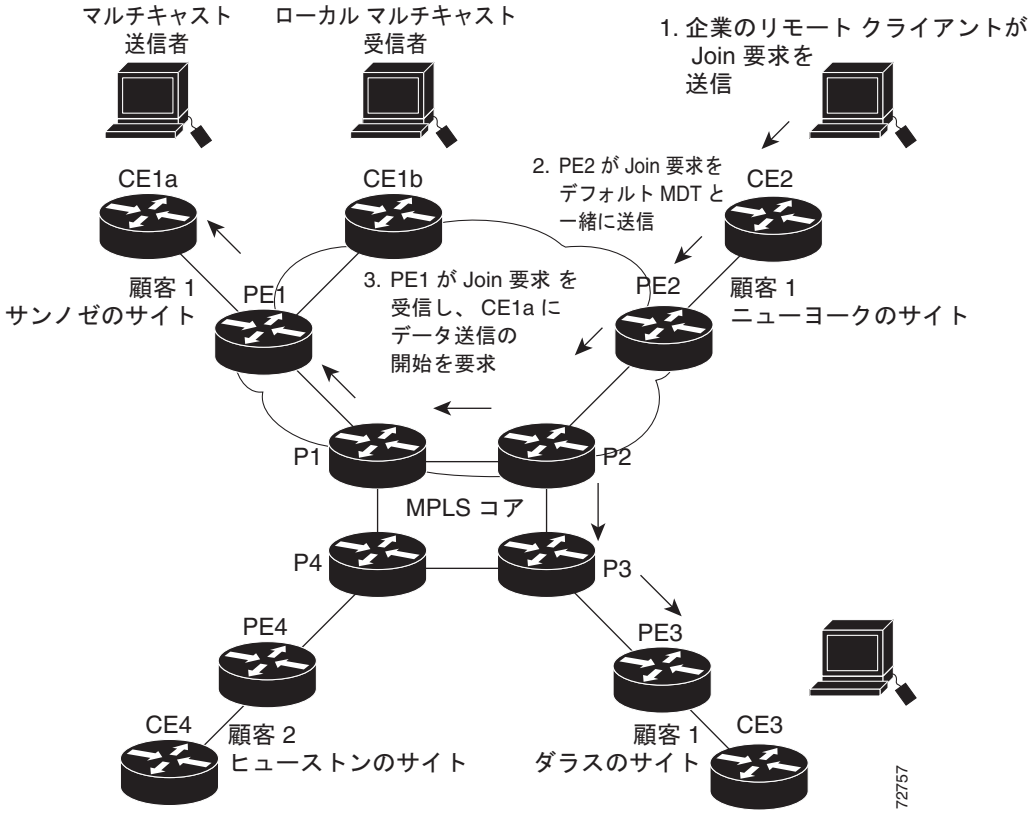
図 25-1 は、San Jose の外側にマルチキャスト ブロードキャストに加わるものがいない場合、つまりデフォルト MDT に沿って流れるデータがない場合の、このネットワークの状況を示します。各 PE ルータは、デフォルト MDT を介して他の PE ルータとの PIM 関係を維持するだけでなく、直接接続された PE ルータと PIM 関係も維持します。

図 25-1　デフォルトのマルチキャスト分散ツリーの概要



New York の従業員がマルチキャスト セッションに加わる場合、New York サイトに関連付けられた PE ルータが Join メッセージを送信し、そのメッセージはマルチキャスト ドメインのデフォルト MDT に流れます。マルチキャスト セッション送信元（PE1）に関連付けられた PE ルータが要求を受信します。図 25-2 に、PE ルータがマルチキャスト送信元（CE1a）に関連付けられた CE ルータに要求を転送する方法を示します。

図 25-2　データ MDT の初期化



CE ルータ（CE1a）が関連付けられている PE ルータ（PE1）へマルチキャスト データの送信を開始し、データ MDT の作成される帯域幅スレッシュホールドを、マルチキャスト データが超過したことを認識します。そこで PE1 はデータ MDT を作成して、すべてのルータにデータ MDT に関する情報が含まれるデフォルト MDT を使用してメッセージを送信します。

約 3 秒後に PE1 は、特定のストリームに対して、データ MDT を使用してマルチキャスト データの送信を開始します。この送信元に関係するレシーバーがあるのは PE2 だけなので、PE2 がデータ MDT に参加して、そのトラフィックを受信します。

マルチキャスト トンネル インターフェイス

PE ルータは、マルチキャスト ドメイン内の各 MVRF に対して Multicast Tunnel Interface（MTI; マルチキャスト トンネル インターフェイス）を作成します。MVRF は、MVRF とグローバル MVRF を接続するコンジットを提供するために、トンネル インターフェイスを使用してマルチキャスト ドメインにアクセスします。

ルータでは、MTI がクラス D マルチキャスト アドレスを持つトンネル インターフェイスです（**interface tunnel** コマンドを使用して作成されます）。この MVRF のデフォルト MDT で設定されているすべての PE ルータは、マルチキャスト ドメイン内にある他のすべての PE ルータに対して、各 PE ルータが PIM ネイバ（1 ホップ先）として認識されるような、論理ネットワークを作成します。この場合、各ルータ間の実際の物理的な距離は関係ありません。

MVRF が設定されると MTI は自動的に作成されます。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ピアリング アドレスは、MTI インターフェイス送信元アドレスとして割り当てられ、PIM プロトコルは自動的に各 MTI でイネーブルになります。

ルータがネットワークのカスタマー側からマルチキャスト パケットを受信すると、着信インターフェイスの VRF を使用してどの MVRF が受信すべきかを判断します。次に、ルータは GRE カプセル化を使用してパケットをカプセル化します。ルータがパケットをカプセル化すると、送信元アドレスをその BGP ピアリング インターフェイスに設定し、宛先アドレスをデフォルト MDT のマルチキャスト アドレス、または設定されている場合にはデータ MDT の送信元アドレスに設定します。次にルータは、適切な数の MTI インターフェイスに転送するために、必要に応じてパケットを複製します。

ルータが MTI インターフェイスでパケットを受信すると、宛先アドレスを使用して適切なデフォルト MDT またはデータ MDT を識別し、その結果適切な MVRF を識別します。ここで、パケットのカプセルを開放してこれを該当するインターフェイスに転送して、必要な分だけ複製します。

（注）

- MVPN MTI は、シスコ製ルータで一般的に使用されている他のトンネル インターフェイスとは違い、ポイントツーポイント インターフェイスではなく LAN インターフェイスとして分類されます。MTI インターフェイスは設定できませんが、**show interface tunnel** コマンドを使用してそのステータスを表示することはできます。
- MTI インターフェイスは、もっぱら VPN トンネルを介したマルチキャスト トラフィックで使用されます。
- トンネルはユニキャスト ルーテッド トラフィックは伝送しません。

MVPN 用の PE ルータ ルーティング テーブルのサポート

MVPN 機能をサポートする各 PE ルータは、VPN および MVPN トラフィックが正常にルーティングされるようにするために、以下のルーティング テーブルを使用します。

- デフォルトのルーティング テーブル - すべてのシスコ製ルータで使用される標準ルーティング テーブル。このテーブルには、バックボーン トラフィックや非 MPLS VPN ユニキャストおよびマルチキャスト トラフィック（Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）マルチキャスト トラフィックなど）で必要なルートが含まれています。
- VPN ルーティング/転送（VRF）テーブル - 各 VRF インスタンスで作成されるルーティング テーブル。MPLS ネットワークにある VPN 間のユニキャスト トラフィックのルーティングに使用されます。
- マルチキャスト VRF（MVRF）テーブル - 各 VRF インスタンス用に作成されたマルチキャスト ルーティング テーブルおよびマルチキャスト ルーティング プロトコル インスタンス。ネットワークのマルチキャスト ドメインにある マルチキャスト トラフィックのルーティングに使用されます。またこのテーブルには、マルチキャスト ドメイン全体で使用されるマルチキャスト トンネル インターフェイスも含まれています。

マルチキャスト分散スイッチングのサポート

MVPN は、インターフェイス単位または VRF 単位でのマルチキャストをサポートする Multicast Distributed Switching（MDS; マルチキャスト分散スイッチング）をサポートしています。MDS を設定する際に、インターフェイス（ループバック インターフェイスを含む）に **no ip mroute-cache** コマンドが設定されていないことを確認する必要があります。

ハードウェア処理の IPv4 マルチキャスト

PFC3BXL または PFC3B モードは、VPN トラフィックを介した IPv4 マルチキャストのハードウェア アクセラレーションをサポートしています。これにより、マルチキャスト トラフィックを MSFC3 CPU の利用率を増やすことなくワイヤ速度で該当する VPN に転送します。

カスタマー VRF では、PFC3BXL または PFC3B モードのハードウェア アクセラレーションは、PIM dence（密）、PIM sparse（疎）、PIM 双方向、PIM Source-Specific Multicast（SSM）モードのマルチキャスト トラフィックをサポートします。

サービス プロバイダー コアでは、PFC3BXL または PFC3B モードのハードウェア アクセラレーションは、PIM sparse（疎）、PIM 双方向、PIM SSM モードのマルチキャスト トラフィックをサポートします。サービス プロバイダー コアでは、PFC3BXL または PFC3B モードのハードウェア アクセラレーションは、PIM dense（密）モードのマルチキャスト トラフィックをサポートしません。

MVPN 設定時の注意事項および制約事項

MVPN を設定する際に、以下の注意事項と制約事項に従ってください。

- Release12.2(18)SXE 以降のリリースでは、スイッチが PFC3B モードまたは PFC3BXL モードで動作している場合に MVPN がサポートされます。Supervisor Engine 2 は、MVPN をサポートしていません。
- マルチキャスト ドメイン内にあるすべての PE ルータは、MVPN 機能をサポートする Cisco IOS ソフトウェア イメージを実行している必要があります。PE ルータおよび CE ルータについては、MVPN サポートの要件はありません。
- IPv4 マルチキャスト トラフィックのサポートは、すべてのバックボーン ルータでイネーブルでなければなりません。
- Border Gateway Protocol（BGP）ルーティング プロトコルは、マルチキャスト トラフィックをサポートするすべてのルータに設定され、動作可能でなければなりません。さらに、ネットワークで MDT を使用できるようにするためには、（**neighbor send-community both** または **neighbor send-community extended** コマンドを使用して）BGP 拡張コミュニティがイネーブルでなければなりません。
- MVPN が設定される場合、入力レプリケーションのみがサポートされます。スイッチが現在出力レプリケーション用に設定されている場合、最初に MVRF が設定されるときに強制的に入力レプリケーションになります。
- スイッチが PE として動作していて、Time to Live（TTL; 存続可能時間）値が 2 のカスタマー ルータからのマルチキャスト パケットを受信した場合、パケットは廃棄され、カプセル化して MVPN リンクに転送されることはありません。そのようなパケットは通常 MVPN リンクのもう一方の端にある PE で廃棄されるため、トラフィック フローには影響しません。
- コア マルチキャスト ルーティングで SSM を使用している場合、データとデフォルトのマルチキャスト分散ツリー（MDT）グループが IPv4 アドレスの SSM 範囲に設定されていなければなりません。
- BGP ピアリングのアップデート送信元インターフェイスは、デフォルト MDT を適切に設定するために、ルータ上にあるすべての BGP ピアリングと同じでなければなりません。BGP ピアリングのループバック アドレスを使用する場合、PIM sparse（疎）モードがループバック アドレスでイネーブルでなければなりません。
- 分散マルチキャスト スイッチングがこれをサポートするプラットフォーム上で機能するために、**ip mroute-cache** コマンドが、BGP ピアリング インターフェイスとして使用されるループバック インターフェイスでイネーブルになっていなければなりません。これらのインターフェイスには、**no ip mroute-cache** コマンドが存在しては*いけません*。
- dense（密）モード マルチキャスト トラフィックのフラッディングおよびプルーニング特性により、データ MDT は定期的にアクティブになり、ティアダウンされるため、VRF PIM dense（密）モード マルチキャスト ストリームに対してデータ MDT は作成されません。
- 送信元情報が利用できないため、VRF PIM 双方向モードに対してデータ MDT は作成されません。
- MVPN は複数の BGP ピアリング アップデート送信元をサポートせず、これを設定すると MVPN Reverse Path Forwarding（RPF）チェック機能が中断する可能性があります。MVPN トンネルの送信元 IPv4 アドレスは、BGP ピアリング アップデート送信元に使用されている最も高い IPv4 アドレスによって決定されます。この IPv4 アドレスが、リモート PE ルータを持つ BGP ピアリング アドレスとして使用されている IPv4 アドレスではない場合、MVPN は適切に機能しません。
- MDT トンネルはユニキャスト トラフィックは伝送しません。
- MVPN が MPLS VPN ネットワークのインフラストラクチャを使用していても、VPN を介したマルチキャスト トラフィックに MPLS タグやラベルは適用できません。

- デフォルト MDT で設定されている各 MVRF は、3 種類の隠し VLAN（カプセル化、カプセル開放、インターフェイス用にそれぞれ 1 つ）に加えて、外部の、ユーザから見える VLAN を使用しています。つまり、最大 1,000 の MVRF が各ルータでサポートされるということです（MDT が設定されていない MVRF が 1 つの内部 VLAN を使用しているので、未使用 MVRF は VLAN 割り当てを節約するために削除されます）。
- MVPN が MPLS を使用しているので、MVPN は Route Processor Redundancy（RPR）と Route Processor Redundancy Plus（RPR+）冗長モードのみをサポートします。Release 12.2(18)SXD およびリビルドでは、MPLS は Nonstop Forwarding（NSF）/Stateful Switchover（SSO）冗長モードと共存できますが、ステートフル MPLS スイッチオーバーのサポートはありません。
- すでに MPLS VPN ネットワークに VRF のネットワークが含まれている場合、MVRF トラフィックをサポートできるようにこれを削除したり再作成したりする必要はありません。代わりに、以下の手順で示しているように、**mdt default** および **mdt data** コマンドを設定して VRF を介したマルチキャスト トラフィックをイネーブルにします。
- BGP は、マルチキャスト トラフィックを送受信するすべてのルータに設定済みで、動作可能である必要があります。さらに、ネットワークで MDT を使用できるようにするためには、（**neighbor send-community both** または **neighbor send-community extended** コマンドを使用して）BGP 拡張コミュニティがイネーブルでなければなりません。
- 特定の VPN 接続をサポートする各 PE ルータに、同じ MVRF が設定されていなければなりません。
- 特定の MVRF をサポートする各 PE ルータは、同じ **mdt default** コマンドで設定されていなければなりません。
- MVPN が設定される場合、スイッチでは入力レプリケーションのみがサポートされます。スイッチが現在出力レプリケーション用に設定されている場合、最初に MVRF が設定されるときに強制的に入力レプリケーションになります。スイッチが現在出力レプリケーション用に設定されている場合、トラフィックの中断が最小限になるように、スケジュールされたメンテナンス期間にのみこのタスクを実行することを推奨します。

MVPN の設定

ここでは、MVPN の設定手順について説明します。

- 「入力マルチキャスト レプリケーション モードへの強制的な変更（任意）」（P.25-10）
- 「マルチキャスト VPN ルーティング/転送インスタンスの設定」（P.25-11）
- 「マルチキャスト VRF ルーティングの設定」（P.25-17）
- 「MVPN をサポートするためのマルチキャスト ルーティング用インターフェイスの設定」（P.25-23）

（注）　これらの設定タスクでは、BGP がマルチキャスト トラフィックを送受信するすべてのルータに設定済みで、動作可能であることを想定しています。さらに、ネットワークで MDT を使用できるようにするためには、（**neighbor send-community both** または **neighbor send-community extended** コマンドを使用して）BGP 拡張コミュニティがイネーブルでなければなりません。

入力マルチキャスト レプリケーション モードへの強制的な変更（任意）

MVPN 機能は入力マルチキャスト レプリケーション モードのみをサポートします。スイッチが現在出力レプリケーション用に設定されている場合、最初に MVRF が設定されるときに強制的に入力レプリケーションになります。このレプリケーション モードの変更によって、ハードウェア内の転送エントリがすべて自動的に削除され、テーブル エントリが再構築されるまでスイッチが一時的にソフトウェア スイッチングに強制的に変更されます。

カスタマー トラフィックが停止しないようにするために、MVRF の設定前には、スイッチがすでに入力マルチキャスト レプリケーション モードになっていることを確認することを推奨します。

次に、現在のマルチキャスト レプリケーション モードを確認する例を示します。

```
Router# show mls ip multicast capability

Current mode of replication is Ingress
auto replication mode detection is ON

 Slot           Multicast replication capability
    2                      Egress
    5                      Egress
    6                      Egress
    8                      Ingress
    9                      Ingress

Router#
```

現在のレプリケーション モードが出力であるか、いずれかのスイッチング モジュールが出力レプリケーション モードに対応している場合、カスタマー トラフィックの停止を最小限にするために、スケジュールされたメンテナンス期間に入力レプリケーション モードを設定します。

入力マルチキャスト レプリケーション モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# mls ip multicast replication-mode ingress`	入力マルチキャスト レプリケーション モードを設定して、（デフォルトでイネーブルの）レプリケーション モードの自動検出をディセーブルにします。
	`Router(config)# no mls ip multicast replication-mode ingress`	レプリケーション モードの自動検出をイネーブルにします。
ステップ 3	`Router(config)# do show mls ip multicast capability | include Current`	設定を確認します。

次に、入力マルチキャスト レプリケーション モードを設定して、その設定を確認する例を示します。

```
Router(config)# mls ip multicast replication-mode ingress
Router(config)# do show mls ip multicast capability | include Current
Current mode of replication is Ingress
```

マルチキャスト VPN ルーティング/転送インスタンスの設定

ここでは、PE ルータの各 VPN 接続に、マルチキャスト VPN ルーティング/転送インスタンス（MVRF）インスタンスを設定する方法を示します。各 PE ルータでは、マルチキャスト トラフィックを送受信するための特定の VPN 接続のトラフィックを処理します。

VRF エントリの設定

VRF エントリを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip vrf vrf_name`	VRF ルーティング テーブル エントリと Cisco Express Forwarding（CEF; シスコ　エクスプレス　フォワーディング）テーブル エントリを設定して、VRF コンフィギュレーション モードを開始します。
	`Router(config)# no ip vrf vrf_name`	VRF エントリを削除します。
ステップ 3	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

次に、blue という名前の VRF を設定して、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# ip vrf blue
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
  blue                              <not set>
```

ルート識別子の設定

ルート識別子を設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router(config-vrf)# rd route_distinguisher`	VPN IPv4 プレフィクスのルート識別子を指定します。
	`Router(config-vrf)# no rd route_distinguisher`	ルート識別子を削除します。
ステップ 2	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

ルート識別子を設定する際に、以下のいずれかの形式でルート識別子を入力します。

- 16 ビット Autonomous System（AS; 自律システム）番号:ユーザの 32 ビットの番号（101:3）
- 32 ビット IPv4 アドレス:ユーザの 16 ビットの番号（192.168.122.15:1）

次に、ルート識別子として 55:1111 を設定して、その設定を確認する例を示します。

```
Router(config-vrf)# rd 55:1111
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
blue                              55:1111
```

ルートターゲット拡張コミュニティの設定

ルートターゲット拡張コミュニティを設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router(config-vrf)# route-target [import | export | both] route_target_ext_community`	VRF のルートターゲット拡張コミュニティを設定します。
	`Router(config-vrf)# no route-target [[import | export | both] route_target_ext_community]`	ルートターゲット拡張コミュニティを削除します。
ステップ 2	`Router(config-vrf)# do show ip vrf detail`	設定を確認します。

ルートターゲット拡張コミュニティを設定する際、次の情報に注意してください。

- **import** - ルーティング情報をターゲット VPN 拡張コミュニティからインポートします。
- **export** - ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
- **both** - インポートとエクスポートの両方を行います。
- *route_target_ext_community* - 48 ビットのルートターゲット拡張コミュニティを VRF に追加します。以下のいずれかの形式で番号を入力します。
  - 16 ビット AS 番号:ユーザの 32 ビットの番号（101:3）
  - 32 ビット IPv4 アドレス:ユーザの 16 ビットの番号（192.168.122.15:1）

次に、インポートおよびエクスポート ルートターゲット拡張コミュニティとして 55:1111 を設定して、その設定を確認する例を示します。

```
Router(config-vrf)# route-target both 55:1111
Router(config-vrf)# do show ip vrf detail
VRF blue; default RD 55:1111; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:55:1111
  Import VPN route-target communities
    RT:55:1111
  No import route-map
  No export route-map
CSC is not configured.
```

デフォルト MDT の設定

デフォルト MDT を設定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config-vrf)# mdt default` *group_address*	デフォルト MDT を設定します。
`Router(config-vrf)# no mdt default`	デフォルト MDT を削除します。

デフォルト MDT を設定する際、次の情報に注意してください。

- *group_address* は、デフォルト MDT グループのマルチキャスト IPv4 アドレスです。すべてのプロバイダー エッジ（PE）ルータが同じグループ アドレスに設定されている場合、それらのルータは同じグループのメンバとなるため、このアドレスは、MVRF コミュニティの識別子としての役割を果たします。これにより、グループ内の他のメンバが送信した PIM 制御メッセージとマルチキャスト トラフィックを受信できます。
- PE ルータをイネーブルにしてこの特定の MVRF のマルチキャスト トラフィックを受信するために、各 PE ルータにはこの同じデフォルト MDT が設定されていなければなりません。

次に、デフォルト MDT として 239.1.1.1 を設定する設定する例を示します。

```
Router(config-vrf)# mdt default 239.1.1.1
```

データ MDT の設定（任意）

任意のデータ MDT を設定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config-vrf)# mdt data group_address wildcard_bits [threshold threshold_value] [list access_list]`	（任意）指定された範囲のマルチキャスト アドレスに対してデータ MDT を設定します。
`Router(config-vrf)# no mdt data`	データ MDT を削除します。

オプションのデータ MDT を設定する際、次の情報に注意してください。

- *group_address1* - マルチキャスト グループ アドレス。アドレスは 224.0.0.1 ～ 239.255.255.255 の範囲で設定可能ですが、デフォルト MDT に割り当てられたアドレスと重複できません。
- *wildcard_bits* - 可能なアドレス範囲を作成するために、マルチキャスト グループ アドレスに適用されるワイルドカード ビットマスク。これにより、各 MVRF がサポートできるデータ MDT の最大数を制限できます。
- **threshold** *threshold_value* -（任意）マルチキャスト トラフィックがデフォルト MDT からデータ MDT に切り替えられるスレッシュホールド値をキロビット単位で定義します。*threshold_value* パラメータは、1 ～ 4294967 キロビットに設定可能です。
- **list** *access_list* -（任意）このトラフィックに適用されるアクセス リスト名または番号を指定します。

次に、データ MDT を設定する例を示します。

```
Router(config-vrf)# mdt data 239.1.2.0 0.0.0.3 threshold 10
```

データ MDT ログ機能のイネーブル化

データ MDT ログ機能をイネーブルにするには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config-vrf)# mdt log-reuse`	（任意）データ MDT が再利用されるたびに Syslog メッセージを生成することで、データ MDT 再利用情報の記録をイネーブルにします。データ MDT を頻繁に再利用する場合、**mdt data** コマンドで使用されるワイルドカード ビットマスクのサイズを増やして、使用可能な MDT の数を増やす必要があります。
`Router(config-vrf)# no log-reuse`	MDT ログ機能をディセーブルにします。

次に、データ MDT ログ機能をイネーブルにする例を示します。

```
Router(config-vrf)# mdt log-reuse
```

コンフィギュレーション例

以下のコンフィギュレーション ファイルからの抜粋は、VRF 範囲の一般的な VRF コンフィギュレーションを示しています。表示を簡略化するために、最初と最後の VRF のみを示しています。

```
!
ip vrf mvpn-cus1
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
...

ip vrf mvpn-cus249
 rd 200:249
 route-target export 200:249
 route-target import 200:249
 mdt default 239.1.1.249
 mdt data 239.1.1.128 0.0.0.7
```

VRF 情報の表示

スイッチで設定されるすべての VRF を表示するには、**show ip vrf** コマンドを使用します。

```
Router# show ip vrf

  Name                             Default RD          Interfaces
  green                            1:52                GigabitEthernet6/1
  red                              200:1               GigabitEthernet1/1
                                                       GigabitEthernet3/16
                                                       Loopback2

Router#
```

すべての MVRF に現在設定されている MDT に関する情報を表示するには、**show ip pim mdt** コマンドを使用します。次に、このコマンドの一般的な出力例を示します。

```
Router# show ip pim mdt

  MDT Group       Interface   Source                VRF
* 227.1.0.1       Tunnel1     Loopback0             BIDIR01
* 227.2.0.1       Tunnel2     Loopback0             BIDIR02
* 228.1.0.1       Tunnel3     Loopback0             SPARSE01
* 228.2.0.1       Tunnel4     Loopback0             SPARSE02
```

（注）　特定のトンネル インターフェイスに関する情報を表示するには、**show interface tunnel** コマンドを使用します。トンネル インターフェイス用の IPv4 アドレスは、MVRF の デフォルト MDT に対するマルチキャスト グループ アドレスです。

MDT の追加情報を表示するには、**show mls ip multicast mdt** コマンドを使用します。次に、このコマンドの一般的な出力例を示します。

```
Router# show mls ip multicast mdt

  State: H - Hardware Installed, I - Install Pending, D - Delete Pending,
       Z - Zombie

                MMLS
  VRF           VPN-ID            MDT INFO                       MDT Type     State
   BIDIR01HWRP       1            (10.10.10.9, 227.1.0.1)        default      H
   BIDIR01SWRP       2            (10.10.10.9, 227.2.0.1)        default      H
  SPARSE01HWRP       3            (10.10.10.9, 228.1.0.1)        default      H
  SPARSE01SWRP       4            (10.10.10.9, 228.2.0.1)        default      H
           red       5               (6.6.6.6, 234.1.1.1)        default      H
           red       5            (131.2.1.2, 228.1.1.75)   data (send)      H
           red       5            (131.2.1.2, 228.1.1.76)   data (send)      H
           red       5            (131.2.1.2, 228.1.1.77)   data (send)      H
           red       5            (131.2.1.2, 228.1.1.78)   data (send)      H

Router#
```

特定の VRF のルーティング情報を表示するには、**show ip route vrf** コマンドを使用します。

```
Router# show ip route vrf red

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback2
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [200/0] via 3.1.1.3, 00:20:09
C    21.0.0.0/8 is directly connected, GigabitEthernet3/16
B    22.0.0.0/8 [200/0] via 3.1.1.3, 00:20:09

Router#
```

特定の MVRF のマルチキャスト ルーティング テーブルとトンネル インターフェイスに関する情報を表示するには、**show ip mroute vrf** コマンドを使用します。次に、BIDIR01 という名前の MVRF の一般的な出力例を示します。

```
Router# show ip mroute vrf BIDIR01

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.1.0.1), 00:16:25/stopped, RP 10.10.10.12, flags: SJCF
  Incoming interface: Tunnel1, RPF nbr 10.10.10.12, Partial-SC
  Outgoing interface list:
    GigabitEthernet3/1.3001, Forward/Sparse-Dense, 00:16:25/00:02:49, H
(6.9.0.100, 228.1.0.1), 00:14:13/00:03:29, flags: FT
  Incoming interface: GigabitEthernet3/1.3001, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Tunnel1, Forward/Sparse-Dense, 00:14:13/00:02:46, H

Router#
```

（注）　この例では、**show ip mroute vrf** コマンドは、この VRF で使用されている Tunnel1 が MDT トンネル インターフェイス（MTI）であることを示しています。

マルチキャスト VRF ルーティングの設定

ここでは、MVPN をサポートするためのマルチキャスト ルーティングの設定手順について説明します。

- 「IPv4 マルチキャスト ルーティングのグローバルなイネーブル化」（P.25-18）
- 「IPv4 マルチキャスト VRF ルーティングのイネーブル化」（P.25-18）
- 「PIM VRF レジスタ メッセージの送信元アドレスの設定」（P.25-19）
- 「PIM VRF ランデブー ポイント（RP）アドレスの指定」（P.25-19）
- 「Multicast Source Discovery Protocol（MSDP）ピアの設定」（P.25-20）
- 「IPv4 マルチキャスト ヘッダー ストレージのイネーブル化」（P.25-20）
- 「マルチキャスト ルートの最大数の設定」（P.25-21）
- 「コンフィギュレーション例」（P.25-22）
- 「IPv4 マルチキャスト VRF ルーティング情報の表示」（P.25-22）

（注）　BGP は、マルチキャスト トラフィックを送受信するすべてのルータに設定済みで、動作可能である必要があります。さらに、ネットワークで MDT を使用できるようにするためには、（**neighbor send-community both** または **neighbor send-community extended** コマンドを使用して）BGP 拡張コミュニティがイネーブルでなければなりません。

IPv4 マルチキャスト ルーティングのグローバルなイネーブル化

IPv4 マルチキャスト ルーティングをグローバルにイネーブルにするには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip multicast-routing`	IPv4 マルチキャスト ルーティングをグローバルにイネーブルにします。
	`Router(config)# no ip multicast-routing`	IPv4 マルチキャスト ルーティングをグローバルにディセーブルにします。

次に、IPv4 マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing
```

IPv4 マルチキャスト VRF ルーティングのイネーブル化

IPv4 マルチキャスト VRF ルーティングをイネーブルにするには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip multicast-routing vrf` *vrf_name* `[distributed]`	IPv4 マルチキャスト VRF ルーティングをイネーブルにします。
`Router(config)# no ip multicast-routing`	IPv4 マルチキャスト VRF ルーティングをディセーブルにします。

IPv4 マルチキャスト VRF ルーティングをイネーブルにする際、次の情報に注意してください。

- *vrf_name* - マルチキャスト ルーティング用に 特定の VRF を指定します。*vrf_name* は、「マルチキャスト VPN ルーティング/転送インスタンスの設定」（P.25-11）で示しているように、前に作成された VRF を参照するようにします。
- **distributed** - （任意）マルチキャスト分散スイッチング（MDS）をイネーブルにします。

次に、IPv4 マルチキャスト VRF ルーティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing vrf blue
```

PIM VRF レジスタ メッセージの送信元アドレスの設定

PIM VRF レジスタ メッセージの送信元アドレスを設定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip pim vrf vrf_name register-source interface_type interface_number`	（任意）PIM VRF レジスタ メッセージの送信元アドレスを設定します。ループバック インターフェイスをレジスタ メッセージの送信元として設定できます。
`Router(config)# no ip pim vrf vrf_name register-source`	IPv4 マルチキャスト VRF ルーティングをディセーブルにします。

次に、PIM VRF レジスタ メッセージの送信元アドレスを設定する例を示します。

```
Router(config)# ip pim vrf blue register-source loopback 3
```

PIM VRF ランデブー ポイント（RP）アドレスの指定

PIM VRF Rendezvous Point（RP; ランデブー ポイント）アドレスを指定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip pim vrf vrf_name rp-address rp_address [access_list] [override] [bidir]`	sparse（疎）PIM ネットワークに必要な PIM RP IPv4 アドレスを指定します。
`Router(config)# no ip pim vrf vrf_name rp-address rp_address`	PIM RP IPv4 アドレスをクリアします。

PIM VRF RP アドレスを指定する際、次の情報に注意してください。

- **vrf** *vrf_name* -（任意）使用する特定の VRF インスタンスを指定します。
- *rp_address* - PIM RP ルータのユニキャスト IP アドレス
- *access_list* -（任意）RP のマルチキャスト グループを定義するアクセス リストの番号または名前
- **override** -（任意）RP アドレスが矛盾している場合、この特定の RP を Auto-RP を通じて学習した RP に上書きします。
- **bidir** -（任意）*access_list* 引数で指定されたマルチキャスト グループが双方向モードで動作するように指定します。このオプションが指定されていない場合、グループは PIM sparse（疎）モードで動作します。
- スケーラビリティ向上のため、可能な限り双方向モードを使用してください。

次に、PIM VRF RP アドレスを指定する例を示します。

```
Router(config)# ip pim vrf blue rp-address 198.196.100.33
```

Multicast Source Discovery Protocol（MSDP）ピアの設定

Multicast Source Discovery Protocol（MSDP）ピアを設定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip msdp vrf vrf_name peer {peer_name | peer_address} [connect-source interface_type interface_number] [remote-as ASN]`	（任意）MSDP ピアを設定します。
`Router(config)# no ip msdp vrf vrf_name peer {peer_name | peer_address} [connect-source interface_type interface_number] [remote-as ASN]`	PIM RP IPv4 アドレスをクリアします。

MSDP ピアを設定する際、次の情報に注意してください。

- **vrf** *vrf_name* - 使用する特定の VRF インスタンスを指定します。
- {*peer_name* | *peer_address*} - MSDP ピア ルータの Domain Name System（DNS; ドメイン ネーム システム）名または IP アドレス
- **connect-source** *interface_type interface_number* - プライマリ アドレスが TCP 接続の送信元 IP アドレスとして使用されいているインターフェイスのインターフェイス名と番号
- **remote-as** *ASN* -（任意）MSDP ピアの自律システム番号。これは、表示するためだけのものです。

次に、MSDP ピアの設定例を示します。

```
Router(config)# ip msdp peer router.cisco.com connect-source fastethernet 1/1 remote-as 109
```

IPv4 マルチキャスト ヘッダー ストレージのイネーブル化

IPv4 マルチキャスト ヘッダー ストレージをイネーブルにするには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip multicast vrf vrf_name cache-headers [rtp]`	（任意）IPv4 マルチキャスト パケット ヘッダーを保存する循環バッファをイネーブルにします。
`Router(config)# no ip multicast vrf vrf_name cache-headers [rtp]`	IPv4 マルチキャスト ヘッダー ストレージをディセーブルにします。

IPv4 マルチキャスト ヘッダー ストレージをイネーブルにする際、次の情報に注意してください。

- **vrf** *vrf_name* - 指定 VRF のバッファを割り当てます。
- **rtp** -（任意）Real-Time Transport Protocol（RTP; リアルタイム トランスポート プロトコル）ヘッダーもキャッシュします。
- バッファは **show ip mpacket** コマンドとともに表示できます。

次に、IPv4 マルチキャスト ヘッダー ストレージをイネーブルにする例を示します。

```
Router(config)# ip multicast vrf blue cache-headers
```

マルチキャスト ルートの最大数の設定

マルチキャスト ルートの最大数を設定するには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip multicast vrf vrf_name route-limit limit [threshold]`	（任意）マルチキャスト トラフィックに追加できるマルチキャスト ルートの最大数を設定します。
`Router(config)# no ip multicast vrf vrf_name route-limit limit [threshold]`	設定されているマルチキャスト ルートの最大数をクリアします。

最大ルート数を設定する際、次の情報に注意してください。

- **vrf** *vrf_name* - 指定 VRF のルート制限をイネーブルにします。
- *limit* - 追加できるマルチキャスト数。指定できる範囲は 1 ～ 2147483647 です。デフォルトは 2147483647 です。
- *threshold* - （任意）警告メッセージが発生するまで追加できるマルチキャスト ルート数。有効な範囲は 1 から *limit* パラメータの値までです。

次に、マルチキャスト ルートの最大数を設定する例を示します。

```
Router(config)# ip multicast vrf blue route-limit 200000 20000
```

IPv4 マルチキャスト ルート フィルタリングの設定

IPv4 マルチキャスト ルート フィルタリングを設定にするには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config)# ip multicast mrinfo-filter access_list`	（任意）アクセス リストを使用して IPv4 マルチキャスト ルート フィルタリングを設定します。*access_list* パラメータにはアクセス リストの名前または番号を指定できます。
`Router(config)# no ip multicast mrinfo-filter`	設定されているマルチキャスト ルートの最大数をクリアします。

次に、IPv4 マルチキャスト ルート フィルタリングを設定する例を示します。

```
Router(config)# ip multicast mrinfo-filter 101
```

コンフィギュレーション例

以下のコンフィギュレーション ファイルからの抜粋は、VRF 範囲のマルチキャスト ルーティングをサポートするのに必要な最小コンフィギュレーションを示しています。表示を簡略化するために、最初と最後の VRF のみを示しています。

```
!
ip multicast-routing
ip multicast-routing vrf lite
ip multicast-routing vrf vpn201
ip multicast-routing vrf vpn202

...

ip multicast-routing vrf vpn249
ip multicast-routing vrf vpn250
ip multicast cache-headers


...

ip pim rp-address 192.0.1.1
ip pim vrf lite rp-address 104.1.1.2
ip pim vrf vpn201 rp-address 192.200.1.1
ip pim vrf vpn202 rp-address 192.200.2.1

...

ip pim vrf vpn249 rp-address 192.200.49.6
ip pim vrf vpn250 rp-address 192.200.50.6
...
```

IPv4 マルチキャスト VRF ルーティング情報の表示

特定の MVRF に対する既知の PIM ネイバを表示するには、**show ip pim vrf neighbor** コマンドを使用します。

```
Router# show ip pim vrf 98 neighbor

PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
40.60.0.11        Tunnel96                00:00:31/00:01:13 v2    1 / S
40.50.0.11        Tunnel96                00:00:54/00:00:50 v2    1 / S

Router#
```

MVPN をサポートするためのマルチキャスト ルーティング用インターフェイスの設定

ここでは、MVPN をサポートするためのマルチキャスト ルーティング用インターフェイスの設定手順について説明します。

マルチキャスト ルーティングの設定の概要

Protocol Independent Multicast（PIM）は、IPv4 マルチキャスト トラフィックに使用されるすべてのインターフェイスで設定されていなければなりません。VPN マルチキャスト環境では、少なくとも以下のすべてのインターフェイスで PIM をイネーブルにする必要があります。

- バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
- BGP ピアリングで使用されるループバック インターフェイス
- sparse（疎）PIM ランデブー ポイント（RP）ルータ アドレスの送信元として使用されるループバック インターフェイス

さらに、マルチキャスト トラフィックを転送しようとしているこれらのインターフェイスと MVRF を関連付ける必要があります。

BGP は、マルチキャスト トラフィックを送受信するすべてのルータに設定済みで、動作可能である必要があります。さらに、ネットワークで MDT を使用できるようにするためには、（**neighbor send-community both** または **neighbor send-community extended** コマンドを使用して）BGP 拡張コミュニティがイネーブルでなければなりません。

インターフェイスでの PIM の設定

インターフェイスで PIM を設定するには、次の作業を行います。

	コマンドまたはアクション	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface` *type* {*slot/port* | *number*}	特定のインターフェイスのインターフェイス 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	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	インターフェイスで PIM をイネーブルにします。
	`Router(config)# no ip pim [dense-mode | sparse-mode | sparse-dense-mode]`	PIM をディセーブルにします。

インターフェイスで PIM を設定する際、次の情報に注意してください。

- 次のインターフェイス タイプのいずれかを使用できます。
  - バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
  - BGP ピアリングで使用されるループバック インターフェイス
  - sparse（疎）PIM ネットワーク ランデブー ポイント（RP）アドレスの送信元として使用されるループバック インターフェイス
- PIM モードには以下のものがあります。
  - **dense-mode** - 動作の dense（密）モードをイネーブルにします。
  - **sparse-mode** - 動作の sparse（疎）モードをイネーブルにします。
  - **sparse-dense-mode** - マルチキャスト グループに RP ルータが定義されている場合は sparse（疎）モードをイネーブルにし、RP ルータが定義されていない場合は dense（密）モードをイネーブルにします。
- バックボーンに接続されたすべての PE ルータの物理インターフェイスに対して、または BGP ピアリングまたは RP アドレッシングの送信元として使用されるすべてのループバック インターフェイスで、**sparse-mode** を使用します。

次に、物理インターフェイスに PIM sparse（疎）モードを設定にする例を示します。

```
Router# configure terminal
interface gigabitethernet 10/1
Router(config-if)# ip pim sparse-mode
```

次に、ループバック インターフェイスに PIM sparse（疎）モードを設定する例を示します。

```
Router# configure terminal
Router(config)# interface loopback 2
Router(config-if)# ip pim sparse-mode
```

IPv4 VRF 転送用インターフェイスの設定

IPv4 VRF 転送用インターフェイスを設定にするには、次の作業を行います。

コマンドまたはアクション	目的
`Router(config-if)# ip vrf forwarding vrf_name`	（任意）指定した VRF ルーティング / 転送テーブルをインターフェイスと関連付けます。これが指定されていない場合、インターフェイスはデフォルトでグローバル ルーティング テーブルを使用します。 **（注）** インターフェイスでこのコマンドを入力すると IP アドレスが削除されるので、IP アドレスを再設定します。
`Router(config-if)# no ip vrf forwarding [vrf_name]`	IPv4 VRF 転送をディセーブルにします。

次に、インターフェイスに VRF bule 転送を設定する例を示します。

```
Router(config-if)# ip vrf forwarding blue
```

コンフィギュレーション例

以下のコンフィギュレーション ファイルからの抜粋は、単一の MVRF を介したマルチキャスト トラフィックをイネーブルにするためのインターフェイス コンフィギュレーションを、関連する MVRF コンフィギュレーションと共に示しています。

```
ip multicast-routing vrf blue
ip multicast-routing

ip vrf blue
 rd 100:27
 route-target export 100:27
 route-target import 100:27
 mdt default 239.192.10.2

interface GigabitEthernet1/1
 description blue connection
 ip vrf forwarding blue
 ip address 192.168.2.26 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet1/15
 description Backbone connection
 ip address 10.8.4.2 255.255.255.0
 ip pim sparse-mode

ip pim vrf blue rp-address 192.7.25.1
ip pim rp-address 10.1.1.1
```

MVPN のコンフィギュレーション例

ここでは、MVPN 機能のコンフィギュレーション例を示します。

- 「デフォルト MDT のみを使用した MVPN コンフィギュレーション」（P.25-26）
- 「デフォルト MDT とデータ MDT を使用した MVPN コンフィギュレーション」（P.25-28）

デフォルト MDT のみを使用した MVPN コンフィギュレーション

以下のコンフィギュレーション ファイルからの抜粋は、3 つの MVRF の MVPN コンフィギュレーションに関連した行を示しています（必要な BGP コンフィギュレーションは省略しています）。

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname MVPN Router
!
boot system flash slot0:
logging snmp-authfail
!
ip subnet-zero
!
!
no ip domain-lookup
ip host tftp 223.255.254.238
!
ip vrf mvpn-cus1
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
ip multicast-routing
ip multicast-routing vrf mvpn-cus1
ip multicast-routing vrf mvpn-cus2
ip multicast-routing vrf mvpn-cus3
ip multicast multipath
frame-relay switching
mpls label range 4112 262143
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp explicit-null
mpls traffic-eng tunnels
tag-switching tdp discovery directed-hello accept from 1
tag-switching tdp router-id Loopback0 force
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
mls ip multicast bidir gm-scan-interval 10
mls flow ip destination
no mls flow ipv6
mls rate-limit unicast cef glean 10 10
mls qos
mls cef error action freeze
```

```
...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 2001-2101,3501-3700,4001,4051-4080,4093
!
!
!
interface Loopback0
 ip address 201.252.1.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback1
 ip address 209.255.255.14 255.255.255.255
!
interface Loopback10
 ip vrf forwarding mvpn-cus1
 ip address 210.101.255.14 255.255.255.255
!
interface Loopback11
 ip vrf forwarding mvpn-cus1
 ip address 210.111.255.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback12
 ip vrf forwarding mvpn-cus1
 ip address 210.112.255.14 255.255.255.255

...

!
interface GigabitEthernet3/3
 mtu 9216
 ip vrf forwarding mvpn-cus3
 ip address 172.10.14.1 255.255.255.0
 ip pim sparse-dense-mode
!

...

!
interface GigabitEthernet3/19
 ip vrf forwarding mvpn-cus2
 ip address 192.16.4.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 229.1.1.1
 ip igmp static-group 229.1.1.2
 ip igmp static-group 229.1.1.4
!
interface GigabitEthernet3/20
 ip vrf forwarding mvpn-cus1
 ip address 192.16.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
...
```

デフォルト MDT とデータ MDT を使用した MVPN コンフィギュレーション

次のコンフィギュレーション例には、デフォルト MDT とデータ MDT の両方が設定された 3 つの MVRF が含まれています。MVPN コンフィギュレーションに関連したコンフィギュレーションのみを示しています。

```
...
!
ip vrf v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 226.1.1.1
 mdt data 226.1.1.128 0.0.0.7 threshold 1
!
ip vrf v2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 mdt default 226.2.2.1
 mdt data 226.2.2.128 0.0.0.7
!
ip vrf v3
 rd 3:3
 route-target export 3:3
 route-target import 3:3
 mdt default 226.3.3.1
 mdt data 226.3.3.128 0.0.0.7
!
ip vrf v4
 rd 155.255.255.1:4
 route-target export 155.255.255.1:4
 route-target import 155.255.255.1:4
 mdt default 226.4.4.1
 mdt data 226.4.4.128 0.0.0.7
!
ip multicast-routing
ip multicast-routing vrf v1
ip multicast-routing vrf v2
ip multicast-routing vrf v3
ip multicast-routing vrf v4
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching tdp router-id Loopback1
mls ip multicast replication-mode ingress
mls ip multicast bidir gm-scan-interval 10
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
!
!
!

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
```

```
interface Loopback1
 ip address 155.255.255.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback4
 ip vrf forwarding v4
 ip address 155.255.4.4 255.255.255.255
 ip pim sparse-mode
!
interface Loopback11
 ip vrf forwarding v1
 ip address 155.255.255.11 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback22
 ip vrf forwarding v2
 ip address 155.255.255.22 255.255.255.255
 ip pim sparse-mode
!
interface Loopback33
 ip vrf forwarding v3
 ip address 155.255.255.33 255.255.255.255
 ip pim sparse-mode
!
interface Loopback44
 no ip address
!
interface Loopback111
 ip vrf forwarding v1
 ip address 1.1.1.1 255.255.255.252
 ip pim sparse-dense-mode
 ip ospf network point-to-point
!
interface GigabitEthernet1/1
 description Gi1/1 - 155.50.1.155 255.255.255.0 - peer dut50 - mpls
 mtu 9216
 ip address 155.50.1.155 255.255.255.0
 ip pim sparse-mode
 tag-switching ip
!
interface GigabitEthernet1/2
 ip vrf forwarding v1
 ip address 155.1.2.254 255.255.255.0
 ip pim sparse-mode
!
interface GigabitEthernet1/3
 description Gi1/3 - 185.155.1.155/24 - vrf v1 stub peer 185.Gi1/3
 ip vrf forwarding v1
 ip address 185.155.1.155 255.255.255.0
 ip pim sparse-mode
!

...

!
interface GigabitEthernet1/48
 ip vrf forwarding v1
 ip address 157.155.1.155 255.255.255.0
 ip pim bsr-border
 ip pim sparse-dense-mode
!
interface GigabitEthernet6/1
 no ip address
 shutdown
```

```
!
interface GigabitEthernet6/2
 ip address 9.1.10.155 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 11 vrf v1
 router-id 155.255.255.11
 log-adjacency-changes
 redistribute connected subnets tag 155
 redistribute bgp 1 subnets tag 155
 network 1.1.1.0 0.0.0.3 area 155
 network 155.255.255.11 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 22 vrf v2
 router-id 155.255.255.22
 log-adjacency-changes
 network 155.255.255.22 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 33 vrf v3
 router-id 155.255.255.33
 log-adjacency-changes
 network 155.255.255.33 0.0.0.0 area 155
!
router ospf 1
 log-adjacency-changes
 network 155.50.1.0 0.0.0.255 area 0
 network 155.255.255.1 0.0.0.0 area 155
!
router bgp 1
 bgp router-id 155.255.255.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 175.255.255.1 remote-as 1
 neighbor 175.255.255.1 update-source Loopback1
 neighbor 185.255.255.1 remote-as 1
 neighbor 185.255.255.1 update-source Loopback1
 !
 address-family vpnv4
 neighbor 175.255.255.1 activate
 neighbor 175.255.255.1 send-community extended
 neighbor 185.255.255.1 activate
 neighbor 185.255.255.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf v4
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v3
 redistribute ospf 33
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v2
```

```
 redistribute ospf 22
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v1
 redistribute ospf 11
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route 9.255.254.1 255.255.255.255 9.1.10.254
no ip http server
ip pim bidir-enable
ip pim rp-address 50.255.2.2 MCAST.MVPN.MDT.v2 override bidir
ip pim rp-address 50.255.3.3 MCAST.MVPN.MDT.v3 override bidir
ip pim rp-address 50.255.1.1 MCAST.MVPN.MDT.v1 override bidir
ip pim vrf v1 spt-threshold infinity
ip pim vrf v1 send-rp-announce Loopback11 scope 16 group-list MCAST.GROUP.BIDIR bidir
ip pim vrf v1 send-rp-discovery Loopback11 scope 16
ip pim vrf v1 bsr-candidate Loopback111 0
ip msdp vrf v1 peer 185.255.255.11 connect-source Loopback11
ip msdp vrf v1 cache-sa-state
!
!
ip access-list standard MCAST.ANYCAST.CE
 permit 2.2.2.2
ip access-list standard MCAST.ANYCAST.PE
 permit 1.1.1.1
ip access-list standard MCAST.BOUNDARY.VRF.v1
 deny   226.192.1.1
 permit any
ip access-list standard MCAST.GROUP.BIDIR
 permit 226.192.0.0 0.0.255.255
ip access-list standard MCAST.GROUP.SPARSE
 permit 226.193.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.BOUNDARY.DATA.MDT
 deny   226.1.1.128
 permit any
ip access-list standard MCAST.MVPN.MDT.v1
 permit 226.1.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v2
 permit 226.2.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v3
 permit 226.3.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.RP.v4
 permit 227.0.0.0 0.255.255.255
!
access-list 1 permit 226.1.1.1
access-list 2 deny   226.1.1.1
access-list 2 permit any
...
```

CHAPTER 26

IP ユニキャスト レイヤ 3 スイッチングの設定

この章では、Catalyst 6500 シリーズ スイッチに IP ユニキャスト レイヤ 3 スイッチングを設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

（注）

- IPX トラフィックは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）で高速スイッチングされます。詳細については、次の URL を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_c/index.htm
- IP マルチキャスト レイヤ 3 スイッチングについては、第 28 章「IPv4 マルチキャスト レイヤ 3 スイッチングの設定」を参照してください。

レイヤ 3 スイッチングの機能概要

ここではレイヤ 3 スイッチングについて説明します。

ハードウェア レイヤ 3 スイッチングの概要

ハードウェア レイヤ 3 スイッチングを使用すると、サブネット間における IP ユニキャスト トラフィックの転送を、MSFC ではなく Policy Feature Card（PFC; ポリシー フィーチャ カード）および Distributed Feature Card（DFC）で行うことができます。ハードウェア レイヤ 3 スイッチングは、MSFC 上のソフトウェアを使用せずに、PFC および DFC 上でワイヤ速度による転送機能を提供します。ハードウェア レイヤ 3 スイッチングの実行には、MSFC からの最低限のサポートが必要です。ハードウェア レイヤ 3 スイッチングが不可能なトラフィックは、MSFC がルーティングします。

ハードウェア レイヤ 3 スイッチングは、MSFC に設定されているルーティング プロトコルをサポートします。ハードウェア レイヤ 3 スイッチングは、MSFC に設定されているルーティング プロトコルに代わるものではありません。

各モジュールに IP ユニキャスト レイヤ 3 スイッチングをローカルで提供するために、ハードウェア レイヤ 3 スイッチングは、PFC および DFC 上で等しく稼動します。ハードウェア レイヤ 3 スイッチングでは、次の機能を提供します。

- Policy-Based Routing（PBR; ポリシー ベース ルーティング）用のハードウェア Access Control List（ACL; アクセス制御リスト）スイッチング
- TCP インターセプトのハードウェア NetFlow スイッチング、再帰 ACL 転送判断
- その他のすべての IP ユニキャスト トラフィック用のハードウェア Cisco Express Forwarding（CEF）スイッチング

PFC 上のハードウェア レイヤ 3 スイッチングは、DFC を装備していないモジュールをサポートします。レイヤ 3 スイッチングが不可能なトラフィックは、MSFC が転送します。

トラフィックはアクセス リストおよび Quality of Service（QoS; サービス品質）によって処理されたあとで、ハードウェア レイヤ 3 スイッチングされます。

ハードウェア レイヤ 3 スイッチングは、入力ポート モジュール上でローカルに各パケットの転送先を決定し、出力ポートに各パケットの書き換え情報を送信します。出力ポート上でパケットが Catalyst 6500 シリーズ スイッチから送信されるときに、書き換えが行われます。

ハードウェア レイヤ 3 スイッチングにより、レイヤ 3 スイッチド トラフィックのフロー統計情報が生成されます。ハードウェア レイヤ 3 フロー統計情報は NetFlow Data Export（NDE; NetFlow データ エクスポート）に使用できます（第 51 章「NetFlow データ エクスポート（NDE）の設定」を参照）。

レイヤ 3 スイッチド パケットの書き換え

特定のサブネット上の送信元から別のサブネット上の宛先へパケットをレイヤ 3 スイッチングするとき、Catalyst 6500 シリーズ スイッチは MSFC から学習した情報に基づいて、出力ポートでパケットの書き換えを行います。この書き換えにより、パケットは MSFC がルーティングしたように表示されます。

パケットの書き換えによって変更されるフィールドは、次の 5 つです。

- レイヤ 2（Media Access Control（MAC; メディア アクセス制御））宛先アドレス
- レイヤ 2（MAC）送信元アドレス
- レイヤ 3 IP Time to Live（TTL）
- レイヤ 3 チェックサム
- レイヤ 2（MAC）チェックサム（別名フレーム チェックサムまたは FCS）

（注） パケットは、ネクストホップのサブネットに適したカプセル化を使用して書き換えられます。

送信元 A と宛先 B が異なるサブネットに属し、送信元 A が MSFC にパケットを送信して宛先 B へルーティングされる場合、スイッチはそのパケットが MSFC のレイヤ 2（MAC）アドレスに送信されたと認識します。

レイヤ 3 スイッチングを実行するため、スイッチはレイヤ 2 フレーム ヘッダーを書き換え、レイヤ 2 宛先アドレスを宛先 B のレイヤ 2 アドレスに変更し、レイヤ 2 送信元アドレスを MSFC のレイヤ 2 アドレスに変更します。レイヤ 3 アドレスは変更されません。

IP ユニキャストおよび IP マルチキャスト トラフィックの場合、スイッチはレイヤ 3 TTL 値を 1 減らし、レイヤ 3 パケット チェックサムを再計算します。スイッチはレイヤ 2 フレーム チェックサムを再計算し、書き換えたパケットを宛先 B のサブネットに転送します（または、マルチキャスト パケットの場合、必要に応じて複製します）。

受信 IP ユニキャスト パケットの形式は（概念的には）、次のとおりです。

レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
MSFC MAC	*送信元 A MAC*	*宛先 B IP*	*送信元 A IP*	*n*	*計算 1*		

スイッチが IP ユニキャスト パケットの書き換えを行ったあとの形式は（概念的には）、次のとおりです。

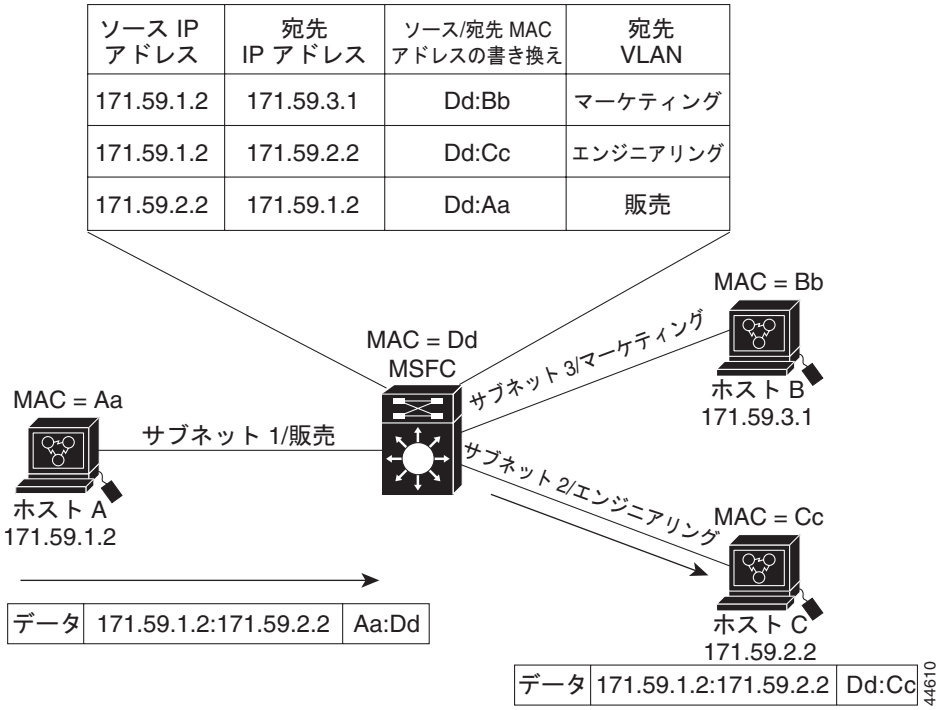
レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
宛先 B MAC	*MSFC MAC*	*宛先 B IP*	*送信元 A IP*	*n-1*	*計算 2*		

ハードウェア レイヤ 3 スイッチングの例

図 26-1（P.26-4）に、単純なネットワーク トポロジを示します。この例では、ホスト A は販売部門の VLAN（IP サブネット 171.59.1.0）、ホスト B はマーケティング部門の VLAN（IP サブネット 171.59.3.0）、ホスト C はエンジニアリング部門の VLAN（IP サブネット 171.59.2.0）にあります。

ホスト A がホスト C に対して HTTP ファイル転送を開始すると、ハードウェア レイヤ 3 スイッチングはローカル Forwarding Information Base（FIB; 転送情報ベース）および隣接テーブルの情報を使用して、ホスト A からホスト C にパケットを転送します。

図 26-1　ハードウェア レイヤ 3 スイッチングのトポロジ例



ハードウェア レイヤ 3 スイッチングのデフォルト設定

表 26-1 に、ハードウェア レイヤ 3 スイッチングのデフォルト設定を示します。

表 26-1　ハードウェア レイヤ 3 スイッチングのデフォルト設定

機能	デフォルト値
ハードウェア レイヤ 3 スイッチングのイネーブル ステート	イネーブル（ディセーブルにはできません）
MSFC 上の Cisco IOS CEF イネーブル ステート	イネーブル（ディセーブルにはできません）
MSFC 上の Cisco IOS dCEF[1] イネーブル ステート	イネーブル（ディセーブルにはできません）

1. dCEF = Distributed Cisco Express Forwarding

設定時の注意事項および制約事項

ハードウェア レイヤ 3 スイッチングを設定する場合、次の注意事項および制約事項に注意してください。

- ハードウェア レイヤ 3 スイッチングは、次の入力および出力カプセル化をサポートします。
  - イーサネット V2.0（ARPA）
  - 1 バイト コントロールを使用する 802.2 対応の 802.3（SAP1）
  - 802.2 対応の 802.3 および Subnetwork Access Protocol（SNAP）

ハードウェア レイヤ 3 スイッチングの設定

（注）　MSFC 上のユニキャスト ルーティングの設定手順については、第 22 章「レイヤ 3 インターフェイスの設定」を参照してください。

ハードウェア レイヤ 3 スイッチングは、永続的にイネーブルになります。したがって設定作業は不要です。

レイヤ 3 スイッチド トラフィックに関する情報を表示するには、次の作業を行います。

コマンド	目的
`Router# show interface {{type[1] slot/port} | {port-channel number}} | begin L3`	レイヤ 3 スイッチド トラフィックの要約を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 3/3 上のハードウェア レイヤ 3 スイッチド トラフィックに関する情報を表示する例を示します。

```
Router# show interface fastethernet 3/3 | begin L3
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 12 pkt, 778 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
     4046399 packets input, 349370039 bytes, 0 no buffer
     Received 3795255 broadcasts, 2 runts, 0 giants, 0 throttles
<...output truncated...>
Router#
```

（注）　レイヤ 3 スイッチング パケット カウントは、約 5 秒間隔で更新されます。

Cisco IOS CEF および dCEF は、永続的にイネーブルになります。ハードウェア レイヤ 3 スイッチングをサポートするための設定作業は不要です。

PFC を（存在する場合は DFC も）利用して、ハードウェア レイヤ 3 スイッチングは、フローごとのロード バランシングを IP の送信元および宛先のアドレスに基づいて使用します。フローごとのロード バランシングは、パケットごとのロード バランシングでは必要となるパケットの再配列を行いません。どのようなフローに対しても、PFC や DFC を装備したすべてのスイッチが、まったく同じロード バランシングの判断を行うので、結果としてロード バランシングがランダムにならない場合があります。

MSFC 上の Cisco IOS CEF **ip load-sharing per-packet**、**ip cef accounting per-prefix**、および **ip cef accounting non-recursive** コマンドは、MSFC 上のソフトウェアで CEF スイッチングされるトラフィックだけに適用されます。これらのコマンドは、PFC 上または DFC を搭載したスイッチング モジュール上でハードウェア レイヤ 3 スイッチングされるトラフィックには影響しません。

MSFC 上の Cisco IOS CEF および dCEF の詳細については、次のマニュアルを参照してください。

- 次の URL にある「Cisco Express Forwarding」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt1/index.htm
- 次の URL にある『*Cisco IOS Switching Services Command Reference*』
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_r/index.htm

ハードウェア レイヤ 3 スイッチング統計情報の表示

ハードウェア レイヤ 3 スイッチング統計情報は、VLAN 単位で収集されます。

ハードウェア レイヤ 3 スイッチング統計情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show interfaces** {{*type*[1] *slot/port*} | {**port-channel** *number*}}	ハードウェア レイヤ 3 スイッチング統計情報を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ハードウェア レイヤ 3 スイッチング統計情報を表示する例を示します。

```
Router# show interfaces gigabitethernet 9/5 | include Switched
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

隣接テーブルの情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show adjacency** [{{*type*[1] *slot/port*} | {**port-channel** *number*}} | **detail** | **internal** | **summary**]	隣接テーブルの情報を表示します。オプションの **detail** キーワードを指定すると、レイヤ 2 情報を含む詳細な隣接情報が表示されます。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、隣接統計情報を表示する例を示します。

```
Router# show adjacency gigabitethernet 9/5 detail
Protocol Interface                 Address
IP       GigabitEthernet9/5        172.20.53.206(11)
                                   504 packets, 6110 bytes
                                   00605C865B82
                                   000164F83FA50800
                                   ARP        03:49:31
```

（注）　隣接統計情報は、約 60 秒間隔で更新されます。

CHAPTER 27

IPv6 マルチキャスト PFC3 および DFC3 レイヤ 3 スイッチングの設定

Release 12.2(18)SXE 以降のリリースの場合、PFC3 および DFC3 は IPv6 マルチキャスト トラフィックをハードウェアでサポートしています。Catalyst 6500 シリーズ スイッチで IPv6 マルチキャストを設定する場合、次のマニュアルを使用してください。

- 『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Multicast」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm
- 『*Cisco IOS IPv6 Command Reference*』
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_r/index.htm

ここでは、Catalyst 6500 シリーズ スイッチでの IPv6 マルチキャスト サポートに関する追加情報を説明します。

IPv6 マルチキャストをサポートする機能

これらの機能は IPv6 マルチキャストをサポートします。

- RPR および RPR+ 冗長モード - 第 8 章「Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定」を参照してください。
- Multicast Listener Discovery version 2（MLDv2）スヌーピング - 第 29 章「IPv6 マルチキャスト トラフィック用の Multcast Listener Discovery version 2（MLDv2）スヌーピングの設定」を参照してください。

（注）　MLDv1 スヌーピングはサポートされていません。

- IPv6 マルチキャスト レート リミッタ - 第 36 章「サービス拒絶（DoS）からの保護の設定」を参照してください。
- IPv6 マルチキャストの Bootstrap Router（BSR; ブートストラップ ルータ）- 『*Cisco IOS IPv6 Configuration Library*』および『*Cisco IOS IPv6 Command Reference*』の BSR 情報を参照してください。
- IPv6 アクセス サービス - 次の URL にある「DHCPv6 Prefix Delegation」を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm
- IPv6 用 SSM マッピング - 次の資料を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6_vgf.htm

IPv6 マルチキャストに関する注意事項および制約事項

次の注意事項と制約事項は、Catalyst 6500 シリーズ スイッチの IPv6 マルチキャスト サポートに適用されます。

- Release 12.2(18)SXE 以降のリリースの場合、PFC3 および DFC3 は以下についてハードウェアでサポートしています。
  - 完全にスイッチングされている IPv6 マルチキャスト フロー
  - IPv6 PIM Sparse（疎）モード（PIM-SM）（S,G）転送
  - NetFlow テーブルを使用する IPv6 PIM-SM（S,G）トラフィックのマルチキャスト RPF チェック
  - マルチキャスト RPF チェックに失敗する IPv6 PIM-SM（S,G）トラフィックのレート制限
  - スタティック IPv6 マルチキャスト ルート
  - IPv6 用 SSM マッピング（PIM-SSM）
  - NetFlow テーブルを使用する IPv6 Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）
  - NetFlow テーブルを使用する IPv6 distributed MFIB（dMFIB; 分散 MFIB）
  - リンクローカルおよびリンクグローバル IPv6 マルチキャスト スコープ
  - **ipv6 mfib hardware-switching** コマンドを使用した出力マルチキャスト レプリケーション
  - マルチキャスト ルート用入力インターフェイス統計（出力インターフェイス統計はありません）

  - RPR および RPR+ 冗長モード -（第 8 章「Route Processor Redundancy（RPR）および Route Processor Redundancy plus（RPR+）スーパーバイザ エンジンの冗長構成の設定」を参照）
  - 入力および出力 PFC QoS（第 41 章「PFC QoS の設定」を参照）
  - 入力および出力 Cisco Access Control List（ACL; アクセス制御リスト）
- PFC3 と DFC3 は、次のものに対してはハードウェアでのサポートをしていません。
  - 部分的にスイッチングされている IPv6 マルチキャスト フロー
  - PIM-SM（*,G）転送
  - PIM-SM（*,G）トラフィックのマルチキャスト RPF チェック
  - マルチキャスト ヘルパー マップ
  - サイトローカル マルチキャスト スコープ
  - 手動で設定した IPv6 over IPv4 トンネル
  - IPv6 マルチキャスト 6to4 トンネル
  - IPv6 マルチキャスト自動化トンネル
  - IPv6 over GRE トンネル
  - IPv6-in-IPv6 PIM レジスタ トンネル
  - IPv6 マルチキャスト基本 ISATAP トンネル
  - 組み込み 6to4 トンネルのある ISATAP トンネル

新規または変更された IPv6 マルチキャスト コマンド

Release 12.2(18)SXE の新規または変更された IPv6 マルチキャスト コマンドの詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

- **ipv6 mfib hardware-switching**
- **mls rate-limit multicast ipv6**（第 36 章「サービス拒絶（DoS）からの保護の設定」を参照）
- **show ipv6 mfib**
- **show mls rate-limit**（第 36 章「サービス拒絶（DoS）からの保護の設定」を参照）
- **show platform software ipv6-multicast**
- **show tcam interface**

IPv6 マルチキャスト レイヤ 3 スイッチングの設定

IPv6 マルチキャスト レイヤ 3 スイッチングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ipv6 unicast-routing`	すべてのレイヤ 3 インターフェイス上でユニキャスト ルーティングをイネーブルにします。
ステップ 2	`Router(config)# ipv6 multicast-routing`	すべてのレイヤ 3 インターフェイス上で PIM-SM をイネーブルにします。
ステップ 3	`Router(config)# ipv6 mfib hardware-switching`	MFIB ハードウェア スイッチングをグローバルにイネーブルにします。

IPv6 マルチキャスト レイヤ 3 スイッチングを確認するための show コマンドの使用

ここでは、IPv6 マルチキャスト レイヤ 3 スイッチングを確認するための **show** コマンドの使用方法について説明します。

（注）　以下のセクションにある **show** コマンドは、スロット 1 に DFC3 を搭載したスイッチング モジュールのあるスイッチと、スロット 6 に PFC3 を搭載した Supervisor Engine 720 用に使用します。

MFIB クライアントの確認

次に、**show ipv6 mrib client** コマンドの完全な出力例を示します。

```
Router# show ipv6 mrib client
IP MRIB client-connections
mfib ipv6:81    (connection id 0)
igmp:124        (connection id 1)
pim:281 (connection id 2)
slot 1  mfib ipv6 rp agent:15   (connection id 3)
slot 6  mfib ipv6 rp agent:15   (connection id 4)
```

次に、MSFC で動作する MFIB クライアントを表示する例を示します。

```
Router# show ipv6 mrib client | include ^mfib ipv6
mfib ipv6:81    (connection id 0)
```

次に、PFC3 および DFC3 で動作する MFIB クライアントを表示する例を示します。

```
Router# show ipv6 mrib client | include slot
slot 1  mfib ipv6 rp agent:15   (connection id 3)
slot 6  mfib ipv6 rp agent:15   (connection id 4)
```

スイッチング能力の表示

次に、**show platform software ipv6-multicast capability** コマンドの完全な出力例を示します。

```
Router# show platform software ipv6-multicast capability

 Hardware switching for IPv6 is enabled
 (S,G) forwarding for IPv6 supported using Netflow
 (*,G) bridging for IPv6 is supported using FIB
 Directly-connected entries for IPv6 is supported using ACL-TCAM.

Current System HW Replication Mode : Ingress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   1 Ingress                Ingress
   2 Egress                 Ingress
   6 Egress                 Ingress
   8 Ingress                Ingress
```

（S,G）転送能力の確認

次に、（S,G）転送を確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include (S,G)
 (S,G) forwarding for IPv6 supported using Netflow
```

（*,G）転送能力の確認

次に、（*,G）転送を確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include (\*,G)
 (*,G) bridging for IPv6 is supported using FIB
```

サブネット エントリのサポート ステータスの確認

次に、サブネット エントリのサポート ステータスを確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include entries
 Directly-connected entries for IPv6 is supported using ACL-TCAM.
```

現在のレプリケーション モードの確認

次に、現在のレプリケーション モードを確認する例を示します。

```
Router# show platform software ipv6-multicast capability | include Current
Current System HW Replication Mode : Ingress
```

（注）　レプリケーション モード自動検出をイネーブルにするには、**no ipv6 mfib hardware-switching replication-mode ingress** を入力します。

レプリケーション モード自動検出ステータスの表示

次に、レプリケーション モード自動検出ステータスを表示する例を示します。

```
Router# show platform software ipv6-multicast capability | include detection
Auto-detection of Replication Mode : ON
```

レプリケーション モード能力の表示

次に、インストールされているモジュールのレプリケーション モード能力を表示する例を示します。

```
Router# show platform software ipv6-multicast capability | begin ^Slot
Slot Replication-Capability Replication-Mode
   1 Ingress                Ingress
   2 Egress                 Ingress
   6 Egress                 Ingress
   8 Ingress                Ingress
```

サブネット エントリの表示

次に、サブネット エントリを表示する例を示します。

```
Router# show platform software ipv6-multicast connected
IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception
Interface: Vlan20 [ H ]
         S:20::1 G:FF00::
Interface: Vlan10 [ H ]
         S:10::1 G:FF00::
```

（注）　この例では、VLAN 10 および VLAN 20 のサブネット エントリがあります。

IPv6 マルチキャスト要約情報の表示

次に、IPv6 マルチキャスト要約情報を表示する例を示します。

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[1]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      100
(*, G)                      0
IPv6 Multicast FIB SC summary on Slot[1]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47

IPv6 Multicast Netflow SC summary on Slot[6]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      100
(*, G)                      0
IPv6 Multicast FIB SC summary on Slot[6]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47
```

NetFlow ハードウェア転送カウントの表示

次に、NetFlow ハードウェア転送カウントを表示する例を示します。

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[1]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      100
(*, G)                      0

<...Output deleted...>

IPv6 Multicast Netflow SC summary on Slot[6]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      100
(*, G)                      0
<...Output truncated...>
```

（注） PIM-SM（*, G）転送が MSFC3 のソフトウェアでサポートされているので、NetFlow（*, G）カウントは、常にゼロです。

FIB ハードウェア ブリッジングおよび廃棄カウントの表示

次に、FIB ハードウェア ブリッジングおよび廃棄ハードウェア カウントを表示する例を示します。

```
Router# show platform software ipv6-multicast summary | begin FIB
IPv6 Multicast FIB SC summary on Slot[1]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47

<...Output deleted...>

IPv6 Multicast FIB SC summary on Slot[6]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  10
(*, G/m)                    47
```

（注）
- （*, G/128）値は、ハードウェア ブリッジ エントリ カウントです。
- （*, G/m）値は、ハードウェア ブリッジ/廃棄エントリ カウントです。

共有および well-known ハードウェア隣接カウンタの表示

show platform software ipv6-multicast shared-adjacencies コマンドは、FIB および ACL-TCAM 内のエントリが IPv6 マルチキャストに使用する共有および well-known ハードウェア隣接カウンタを表示します。

```
Router# show platform software ipv6-multicast shared-adjacencies

---- SLOT [1] ----

Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------- ------------------
Subnet bridge adjacency       0x7F802  0             0
Control bridge adjacency      0x7      0             0
StarG_M bridge adjacency      0x8      0             0
S_G bridge adjacency          0x9      0             0
Default drop adjacency        0xA      0             0
StarG (spt == INF) adjacency  0xB      0             0
StarG (spt != INF) adjacency  0xC      0             0

---- SLOT [6] ----

Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------- ------------------
Subnet bridge adjacency       0x7F802  0             0
Control bridge adjacency      0x7      0             0
StarG_M bridge adjacency      0x8      0             0
S_G bridge adjacency          0x9      0             0
Default drop adjacency        0xA      28237         3146058
StarG (spt == INF) adjacency  0xB      0             0
StarG (spt != INF) adjacency  0xC      0             0
```

CHAPTER 28

IPv4 マルチキャスト レイヤ 3 スイッチングの設定

この章では、Catalyst 6500 シリーズ スイッチに IPv4 マルチキャスト レイヤ 3 スイッチングを設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

IPv4 マルチキャスト レイヤ 3 スイッチングの機能概要

ここでは、IPv4 マルチキャスト レイヤ 3 スイッチングの機能について説明します。

IPv4 マルチキャスト レイヤ 3 スイッチングの概要

Policy Feature Card（PFC; ポリシー フィーチャ カード）は、ハードウェア レプリケーション テーブルおよびハードウェア Cisco Express Forwarding（CEF）（PFC の Forwarding Information Base（FIB; 転送情報ベース）および隣接テーブルを使用）を使用して、IP マルチキャスト フローのレイヤ 3 スイッチング機能を提供します。Distributed Forwarding Card（DFC）を装備したシステムでは、IP マルチキャスト フローは、Multicast Distributed Hardware Switching（MDHS）を使用してローカルにレイヤ 3 スイッチングされます。MDHS は、各 DFC 上のローカルなハードウェア CEF テーブルおよびレプリケーション テーブルを使用して、DFC を装備した各スイッチング モジュール上で、レイヤ 3 スイッチングおよび Reverse Path Forwarding（RPF）障害のレート制限をローカルに実行します。

PFC および DFC は、（*,G）ステート フローのハードウェア スイッチングをサポートします。PFC および DFC は、非 RPF トラフィックのレート制限をサポートします。

マルチキャスト レイヤ 3 スイッチングは、高度な Application-Specific Integrated Circuit（ASIC; 特定用途向け IC）スイッチング ハードウェアを使用して、IP サブネット間で IP マルチキャスト データ パケット フローを転送します。その結果、プロセッサを集中的に使用するマルチキャスト転送および複製といったネットワーク ルータの負荷を軽減します。

ハードウェア スイッチングが不可能なレイヤ 3 フローは、引き続きルータによってソフトウェアで転送されます。ルートの決定には、Protocol Independent Multicast（PIM）が使用されます。

PFC および DFC はいずれも、レイヤ 2 マルチキャスト転送テーブルを使用して、レイヤ 2 マルチキャスト トラフィックを転送するポート（ある場合）を判別します。マルチキャスト転送テーブル エントリは、Internet Group Management Protocol（IGMP）スヌーピングとともに読み込まれます（第 30 章「IPv4 マルチキャスト トラフィック用インターネット グループ管理プロトコル（IGMP）スヌーピングの設定」を参照）。

マルチキャスト レイヤ 3 スイッチング キャッシュ

ここでは、PFC および DFC がハードウェア テーブルにレイヤ 3 スイッチング情報を保持する方法について説明します。

PFC および DFC は、適切なマスクを使用して（S,G）または（*,G）フローをハードウェア FIB テーブルに読み込みます。たとえば、(S/32, G/32）および（*/0, G/32）などです。RPF インターフェイスおよび隣接ポインタ情報も、各エントリに保存されます。隣接テーブルには、書き換え情報およびレプリケーション エントリへのポインタが含まれます。フローが FIB エントリと一致した場合、RPF チェックによって着信インターフェイス/VLAN がエントリと比較されます。一致しない場合は RPF 障害であり、レート制限機能がイネーブルになっている場合はレート制限の対象になります。

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）は新しいフローのトラフィックを受信するたびに、自身のマルチキャスト ルーティング テーブルを更新し、新しい情報を PFC に転送します。さらに、MSFC 上のマルチキャスト ルーティング テーブルのエントリが期限切れになると、MSFC はそのエントリを削除し、更新された情報を PFC に転送します。DFC を装備したシステムでは、すべての DFC および PFC に対称的にフローが読み込まれます。

レイヤ 3 スイッチング キャッシュには、すべてのアクティブなレイヤ 3 スイッチド フローに関する情報が含まれます。スイッチング キャッシュが読み込まれたあと、既存のフローに属することが識別されたマルチキャスト パケットは、そのフローに対応するキャッシュ エントリに基づいて、レイヤ 3 スイッチングされます。PFC はキャッシュ エントリごとに、IP マルチキャスト グループに対応する出力インターフェイスのリストを維持します。PFC はこのリストを使用して、特定のマルチキャスト フローからのトラフィックをどの VLAN に複製しなければならないかを識別します。

レイヤ 3 スイッチング キャッシュ エントリに有効なコマンドは、次のとおりです。

- **clear ip mroute** コマンドを使用してマルチキャスト ルーティング テーブルを消去すると、マルチキャスト レイヤ 3 スイッチング キャッシュ エントリがすべて消去されます。
- **no ip multicast-routing** コマンドを使用して MSFC 上の IP マルチキャスト ルーティングをディセーブルにすると、PFC 上のマルチキャスト レイヤ 3 スイッチング キャッシュ エントリがすべて消去されます。
- **no mls ip multicast** コマンドを使用してインターフェイス単位でマルチキャスト レイヤ 3 スイッチングをディセーブルにすると、そのインターフェイスを RPF インターフェイスとして使用するフローが、ソフトウェア上で MSFC によってのみルーティングされます。

レイヤ 3 スイッチド マルチキャスト パケットの書き換え

マルチキャスト送信元から宛先マルチキャスト グループへマルチキャスト パケットがレイヤ 3 スイッチングされる場合、PFC および DFC は、MSFC から得た情報とその隣接テーブルに保存されている情報に基づき、パケットの書き換えを実行します。

たとえば、サーバ A が IP マルチキャスト グループ G1 を宛先とするマルチキャスト パケットを送信するとします。送信元 VLAN 以外の VLAN 上にグループ G1 のメンバが存在する場合、PFC は他の VLAN にトラフィックを複製するとき、パケットの書き換えを実行しなければなりません（スイッチはさらに、送信元 VLAN 内でパケットをブリッジします）。

PFC がマルチキャスト パケットを受信した時点でのパケットの形式は（概念的には）、次のとおりです。

レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
グループ G1 MAC[1]	*送信元 A MAC*	*グループ G1 IP*	*送信元 A IP*	*n*	*計算 1*		

1. この例では、宛先 B はグループ G1 のメンバです。

PFC は、パケットを次のように書き換えます。

- レイヤ 2 フレーム ヘッダーの送信元 MAC（メディア アクセス制御）アドレスを、ホストの MAC アドレスから MSFC の MAC アドレスに変更します（システムに組み込まれている MAC アドレスです。この MAC アドレスは、すべての出力インターフェイスの場合と同じで変更できません。この MAC アドレスを表示するには、**show mls multicast statistics** コマンドを使用します。）
- IP ヘッダーの Time to Live（TTL）を 1 だけ減らし、IP ヘッダー チェックサムを再計算します。

その結果、表示される書き換えられた IP マルチキャスト パケットは、ルーティングされていることになります。PFC は書き換えたパケットを該当する宛先 VLAN に複製し、パケットはその VLAN 上で IP マルチキャスト グループ G1 のメンバに転送されます。

PFC がパケットの書き換えを行ったあとの形式は（概念的には）、次のとおりです。

フレーム ヘッダー		IP ヘッダー				データ	FCS
宛先	送信元	宛先	送信元	TTL	チェックサム		
グループ G1 MAC	*MSFC MAC*	*グループ G1 IP*	*送信元 A IP*	*n–1*	*計算 2*		

フローの部分的なスイッチングおよび完全なスイッチング

特定のフローで、1 つまたは複数の出力レイヤ 3 インターフェイスがマルチレイヤ スイッチングされ、1 つまたは複数の出力インターフェイスがマルチレイヤ スイッチングされない場合、そのフローは部分的にスイッチングされていると見なされます。部分的にスイッチングされるフローが作成されると、そのフローに属するすべてのマルチキャスト トラフィックが MSFC に到達し、マルチレイヤ スイッチングされない出力インターフェイス上でソフトウェアによって転送されます。

ここでは、フローの部分的なスイッチングおよび完全なスイッチングについて説明します。

- 「フローの部分的スイッチング」（P.28-4）
- 「フローの完全スイッチング」（P.28-5）

フローの部分的スイッチング

次の状況で、フローは完全にスイッチングされずに部分的にスイッチングされる可能性があります。

- マルチキャスト送信元の RPF インターフェイスで、スイッチが IP マルチキャスト グループのメンバとして設定されている場合（**ip igmp join-group** コマンドを使用）
- 登録ステートの間 PIM sparse（疎）モードで、スイッチが送信元への最初のホップ ルータである場合（この場合、スイッチは Rendezvous Point（RP; ランデブー ポイント）に PIM 登録メッセージを送信しなければなりません）
- フローの出力インターフェイスで、マルチキャスト TTL スレッシュホールドが設定されている場合（**ip multicast ttl-threshold** コマンドを使用）
- フローの RPF インターフェイスにマルチキャスト ヘルパーが設定されていて、マルチキャストからブロードキャストへの変換が必要な場合
- PFC2 で、出力インターフェイスが Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル インターフェイスの場合
- PFC3 で Release 12.2(18)SXE よりも前のバージョンのときに、出力インターフェイスが GRE トンネル インターフェイスの場合

- 出力インターフェイスが Distance Vector Multicast Routing Protocol（DVMRP）トンネル インターフェイスの場合
- インターフェイスに Network Address Translation（NAT; ネットワーク アドレス変換）が設定されていて、出力インターフェイス用に送信元アドレスの変換が必要な場合
- 出力インターフェイスが特定のフローでレイヤ 3 スイッチングされない場合、フローは部分的にスイッチングされます

次の状況で、(S,G）フローは完全にスイッチングされずに部分的にスイッチングされます。

- (S,G）エントリに RPT ビット（R ビット）が設定されている場合、(S,G）フローは部分的にスイッチングされます。
- (S,G）エントリに Shortest-Path-Tree（SPT）ビット（T フラグ）およびプルーニング ビット（P フラグ）が設定されていない場合、(S,G）フローは部分的にスイッチングされます。

次の状況で、(*,G）フローは完全にスイッチングされずに部分的にスイッチングされます。

- 共有ツリーから SPT へのスレッシュホールドが無限に等しくならない場合、(*,G）フローは最後のホップ リーフ ルータ上で部分的にスイッチングされます。これによって、フローは SPT から移行できます。
- 少なくとも 1 つの（S,G）エントリに（*,G）エントリと同じ RPF があるが、いずれも真の場合、(*,G）フローは部分的にスイッチングされます。
  - RPT フラグ（R ビット）は設定されません。
  - SPT フラグ（T ビット）は設定されません。
  - プルーニング フラグ（P ビット）は設定されません。
- DVMRP ネイバが（*,G）エントリの入力インターフェイスで検出された場合、(*,G）フローは部分的にスイッチングされます。
- インターフェイス/マスク エントリが、(*,G）エントリの RPF インターフェイスにインストールされておらず、RPF インターフェイスがポイントツーポイント インターフェイスではない場合、(*,G）フローは部分的にスイッチングされます。

フローの完全スイッチング

特定のフローで、すべての出力インターフェイスがレイヤ 3 スイッチングされ、かつフローに上記の状況がいずれも該当しない場合、そのフローは完全にスイッチングされていると見なされます。完全にスイッチングされるフローが作成されると、PFC は、送信元 VLAN 上でそのフロー用にブリッジされているマルチキャスト トラフィックが VLAN の MSFC インターフェイスに到達できないようにして、そのフローの転送および複製など MSFC の負荷を軽減します。

フローが完全にスイッチングされると、そのフローに関してはパケット単位でのマルチキャスト統計情報を記録できません。そのため、PFC はすべての完全にスイッチングされたフローに関するマルチキャスト パケットおよびバイト カウント統計情報を、定期的に MSFC に送信します。MSFC は対応するマルチキャスト ルーティング テーブル エントリを更新し、そのマルチキャスト ルートに対応する期限タイマーをリセットします。

（注）　PIM-RP または PIM-dense（密）モードでは（*,G）ステートが作成されますが、フローの転送には使用されず、これらのフローについてはレイヤ 3 スイッチング エントリは作成されません。

非 RPF トラフィックの処理

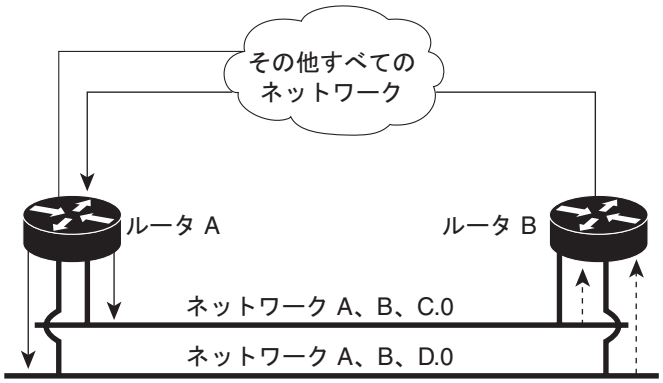
ここでは、非 RPF トラフィックの処理について説明します。

非 RPF トラフィックの概要

複数のルータが同一 LAN セグメントに接続する冗長構成では、1 台のルータだけが、出力インターフェイス上でマルチキャスト トラフィックを送信元から受信側まで転送します（図 28-1 を参照）。このようなトポロジでは、PIM Designated Router（PIM DR; PIM 指定ルータ）だけが共通の VLAN 内でデータを転送し、非 PIM DR は転送されたマルチキャスト トラフィックを受信します。このトラフィックは、誤ったインターフェイスに着信して RPF チェックに失敗するため、冗長ルータ（非 PIM DR）はこのトラフィックを廃棄しなければなりません。このように RPF チェックに失敗するトラフィックを、「非 RPF トラフィック」といいます。

Catalyst 6500 シリーズ スイッチは、PFC のハードウェアで、非 RPF トラフィックをフィルタリング（廃棄）するか、またはレート制限することによって処理します。

図 28-1　スタブ ネットワークにおける冗長マルチキャスト ルータの構成



— マルチキャスト トラフィック
--- 非 RPF トラフィック

スタブ ネットワークのための RPF 障害のフィルタリング

PFC および DFC は、sparse（疎）モードのスタブ ネットワーク用に、RPF 障害の Access Control List（ACL; アクセス制御リスト）ベースのフィルタリング機能をサポートしています。冗長ルータ上で **mls ip multicast stub** コマンドを入力して、ACL ベースの方式による RPF 障害のフィルタリングをイネーブルにすると、次の ACL が自動的に PFC にダウンロードされ、指定するインターフェイスに適用されます。

```
access-list 100 permit ip A.B.C.0 0.0.0.255 any
access-list 100 permit ip A.B.D.0 0.0.0.255 any
access-list 100 permit ip any 224.0.0.0 0.0.0.255
access-list 100 permit ip any 224.0.1.0 0.0.0.255
access-list 100 deny ip any 224.0.0.0 15.255.255.255
```

ACL によって、ハードウェアで RPF 障害がフィルタリングおよび廃棄されるため、ルータに転送されなくなります。

ACL ベースの RPF 障害フィルタリング機能は、ダウンストリーム ルータの存在しない、sparse（疎）モードのスタブ ネットワークに限って使用してください。dense（密）モード グループの場合は、PIM アサート メカニズムを正常に動作させるために、ルータ上で RPF 障害パケットを認識する必要があります。dense（密）モードのネットワーク、および sparse（疎）モードの中継ネットワークでは、CEF ベースまたは NetFlow ベースのレート制限を使用して、RPF 障害のレートを制限してください。

RPF 障害に対する ACL ベースのフィルタリングについての詳細は、「RPF 障害に対する ACL ベースのフィルタリングの設定」（P.28-19）を参照してください。

RPF 障害トラフィックのレート制限

RPF チェックに失敗するパケット（非 RPF パケット）のレート制限を行うと、ほとんどの非 RPF パケットがハードウェアで廃棄されます。マルチキャスト プロトコルの仕様に従って、PIM アサート メカニズムが正しく機能するには、ルータが非 RPF パケットを受信する必要があるので、すべての非 RPF パケットをハードウェアで廃棄することはできません。

非 RPF パケットを受信すると、NetFlow エントリが 非 RPF フローごとに作成されます。

非 RPF パケットが到着すると、PFC はパケットを MSFC およびブリッジド ポートへブリッジし、送信元、グループ、入力インターフェイス情報を含む NetFlow エントリを作成します。NetFlow エントリでは、その送信元およびグループのパケットがすべて処理されあと、パケットを MSFC ではなくブリッジド ポートへのみ送信されます。

PIM アサート メカニズムをサポートするために、PFC は非 RPF フロー パケットの一部を MSFC に定期的に転送します。

PIM sparse（疎）モードで直接接続された送信元の最初のパケットはレートが制限され、CPU により処理されます。

RPF 障害のレート制限は、デフォルトでディセーブルに設定されています。

マルチキャスト境界

マルチキャスト境界機能は、マルチキャスト グループ アドレスの管理境界を設定することを可能にします。マルチキャスト データ パケットのフローを制限することにより、同じマルチキャスト グループ アドレスを異なる管理ドメイン内で再利用することができます。

マルチキャスト境界は、インターフェイス上に設定します。マルチキャスト データ パケットは、パケットのマルチキャスト グループ アドレスがマルチキャスト境界機能に関連付けられているアクセス制御リスト（ACL）に一致すると、インターフェイスを越えての伝送がブロックされます。

マルチキャスト境界 ACL は、ハードウェアの場合には PFC、Distributed Forwarding Card（DFC）で、ソフトウェアの場合には MSFC で処理できます。マルチキャスト境界 ACL は、パケットの宛先アドレスに一致するようにプログラムされます。この ACL は、インターフェイス上の両方向（入力と出力）のトラフィックに適用されます。

マルチキャスト境界 ACL をハードウェアでサポートするために、スイッチは、新しい ACL TCAM エントリを作成するか、または既存の ACL TCAM エントリに変更を加えます（ACL ベースの他の機能がそのインターフェイス上でアクティブになっている場合）。TCAM リソース利用率を確認するには、**show tcam counts ip** コマンドを入力します。

filter-autorp キーワードを設定すると、管理境界で自動 RP 検出メッセージと通知メッセージも調べられ、境界 ACL によって拒否される自動 RP パケットの自動 RP グループ範囲の通知はすべて削除されます。

IPv4 双方向 PIM の機能概要

PFC3 では、IPv4 双方向 PIM グループのハードウェア転送をサポートします。IPv4 双方向 PIM グループをサポートするために、PFC3 は Designated Forwarder（DF）モードという新しいモードを実行します。DF は、IPv4 双方向 PIM グループのセグメントへ、またセグメントからパケットを転送するよう選定されたルータです。DF モードでは、スーパーバイザ エンジンは RPF および DF インターフェイスからパケットを受け入れます。

スーパーバイザ エンジンが IPv4 双方向 PIM グループを転送するとき、RPF インターフェイスは常に（*,G）エントリの出力インターフェイス リストに含まれ、DF インターフェイスが含まれるエントリは IGMP/PIM Join に応じて決まります。

RP へのルートが使用できない場合、グループは dense（密）モードに変更されます。RP への RPF リンクが使用できなくなると、IPv4 双方向 PIM フローはハードウェア FIB から削除されます。

IPv4 双方向 PIM の設定手順については、「IPv4 双方向 PIM の設定」（P.28-26）を参照してください。

IPv4 マルチキャスト レイヤ 3 スイッチングのデフォルト設定

表 28-1 に、IP マルチキャスト レイヤ 3 スイッチングのデフォルト設定を示します。

表 28-1　IP マルチキャスト レイヤ 3 スイッチングのデフォルト設定

機能	デフォルト値
スタブ ネットワーク用の ACL	全インターフェイスでディセーブル
直接接続されたサブネット エントリのインストール	グローバルにイネーブル
マルチキャスト ルーティング	グローバルにディセーブル
PIM ルーティング	全インターフェイスでディセーブル
IP マルチキャスト レイヤ 3 スイッチング	マルチキャスト ルーティングがイネーブルで、インターフェイス上で PIM がイネーブルになっている場合はイネーブル
ショートカット整合性検査	イネーブル

IGMP スヌーピングは、すべての VLAN 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 IGMP スヌーピングをディセーブルにしても、マルチキャスト レイヤ 3 フローは引き続きハードウェアによりスイッチングされます。IGMP スヌーピングをディセーブルに設定したインターフェイス上でフローをブリッジすると、VLAN のすべての転送インターフェイスにフラッディングが発生します。IGMP スヌーピングの設定については、第 30 章「IPv4 マルチキャスト トラフィック用インターネット グループ管理プロトコル（IGMP）スヌーピングの設定」を参照してください。

IPv4 マルチキャスト レイヤ 3 スイッチング設定時の注意事項および制約事項

ここでは、IP マルチキャスト レイヤ 3 スイッチングの設定に関する制約事項について説明します。

制約事項

次のような場合に、IP マルチキャスト レイヤ 3 スイッチングは IP マルチキャスト フローに提供されません。

- 224.0.0.*（* は 0 ～ 255）の範囲の IP マルチキャスト グループ。これらのグループは、ルーティング プロトコルが使用します。レイヤ 3 スイッチングは、225.0.0.* ～ 239.0.0.*、および 224.128.0.* ～ 239.128.0.* のグループでサポートされます。

（注）　224.0.0.* の範囲のグループはルーティング コントロール パケット専用で、VLAN のすべての転送ポートにフラッディングする必要があります。これらのアドレスは、マルチキャスト MAC アドレス範囲 01-00-5E-00-00-*xx*（*xx* は 0 ～ 0xFF）に対応します。

- PIM 自動 RP マルチキャスト グループ（IP マルチキャスト グループ アドレス 224.0.1.39 および 224.0.1.40）
- IP オプションを指定されたパケット。ただし、IP オプションを指定されていないフロー内でのパケットは、ハードウェア スイッチングされます。
- トンネル インターフェイスで受信する送信元トラフィック（MBONE トラフィックなど）
- sparse（疎）モードの（S,G）エントリに、SPT ビット、RPT ビット、またはプルーニング フラグが設定されていない場合
- 1 つ以上の（S,G）エントリに（*,G）エントリの RPF とは異なる RPF があり、（S,G）がハードウェアでスイッチングされない場合、（*,G）エントリはハードウェアでスイッチングされません。
- （S,G）または（*,G）エントリの入力インターフェイスがヌルの場合。（*,G）エントリが IPv4 双方向 PIM エントリでスイッチがグループの RP である場合を除く。
- DF インターフェイスまたは RPF インターフェイスがトンネルの場合の IPv4 双方向 PIM エントリ
- PFC2 の場合、マルチキャスト パケットの NAT 変換はソフトウェアで処理されます。
- PFC2 の場合、マルチキャスト パケットの GRE トンネル カプセル化および非カプセル化は、ソフトウェアで処理されます。
- PFC3 および Release 12.2(18)SXE よりも前のリリースの場合、マルチキャスト パケットの GRE トンネル カプセル化および非カプセル化は、ソフトウェアで処理されます。
- Supervisor Engine 32 は、出力マルチキャスト レプリケーションをサポートせず、マルチキャスト レプリケーション モードを検出できません。

サポートされない機能

IP マルチキャスト レイヤ 3 スイッチングをイネーブルにした場合、レイヤ 3 インターフェイスに関する IP アカウンティングでは、正確な値が報告されません。**show ip accounting** コマンドはサポートされません。

IPv4 マルチキャスト レイヤ 3 スイッチングの設定

ここでは、IP マルチキャスト レイヤ 3 スイッチングの設定手順について説明します。

（注）　コンフィギュレーション モードで EXEC モード レベルのコマンドを入力するには、コマンドの前に **do** キーワードを入力します。

IGMPv3、IGMP v3lite、および URD を使用した Source-Specific Multicast

IGMPv3、IGMP v3lite、および URL Rendezvous Directory（URD）を使用した Source-Specific Multicast（SSM）の詳細および手順については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfssm.htm

IPv4 マルチキャスト ルーティングのグローバルなイネーブル化

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにするには、事前に IP マルチキャスト ルーティングをグローバルにイネーブルにする必要があります。

詳しい説明および設定手順については、次のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』Release 12.2
  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html
- 次の URL にある『*Cisco IOS IP and IP Routing Command Reference*』Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm

IP マルチキャスト ルーティングをグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをグローバルにイネーブルにします。
`Router(config)# no ip multicast-routing`	IP マルチキャスト ルーティングをグローバルにディセーブルにします。

次に、マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router(config)# ip multicast-routing
Router(config)#
```

レイヤ 3 インターフェイス上での IPv4 PIM のイネーブル化

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングを動作させるには、事前にレイヤ 3 インターフェイス上で PIM をイネーブルにする必要があります。

レイヤ 3 インターフェイス上で IP PIM をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	レイヤ 3 インターフェイス上で IP PIM をイネーブルにします。
	`Router(config-if)# no ip pim [dense-mode | sparse-mode | sparse-dense-mode]`	レイヤ 3 インターフェイス上で IP PIM をディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス上でデフォルト モード（**sparse-dense-mode**）を使用して PIM をイネーブルにする例を示します。

```
Router(config-if)# ip pim
Router(config-if)#
```

次に、インターフェイス上で PIM sparse（疎）モードをイネーブルにする例を示します。

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#
```

IP マルチキャスト レイヤ 3 スイッチングのグローバルなイネーブル化

システム上でマルチキャスト ルートのハードウェア スイッチングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls ip multicast`	マルチキャスト ルートのハードウェア スイッチングをグローバルにイネーブルにします。
ステップ 2	`Router# show mls ip multicast`	MLS IP マルチキャスト設定を表示します。

次に、マルチキャスト ルートのハードウェア スイッチングをグローバルにイネーブルにする例を示します。

```
Router(config)# mls ip multicast
Router(config)#
```

レイヤ 3 インターフェイス上での IP マルチキャスト レイヤ 3 スイッチングのイネーブル化

レイヤ 3 インターフェイス上で PIM をイネーブルにすると、インターフェイス上では IP マルチキャスト レイヤ 3 スイッチングがデフォルトでイネーブルになります。次の作業は、インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをディセーブルにしたあと、再びイネーブルにする場合にのみ行います。

PIM は、VLAN インターフェイスも含めて、任意のレイヤ 3 インターフェイス上でイネーブルに設定できます。

（注） IP マルチキャスト レイヤ 3 スイッチングを動作させるには、事前に関与するすべてのレイヤ 3 インターフェイス上で PIM をイネーブルにする必要があります。レイヤ 3 インターフェイス上での PIM の設定手順については、「レイヤ 3 インターフェイス上での IPv4 PIM のイネーブル化」（P.28-12）を参照してください。

レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan` *vlan_ID*`} | {`*type*[1] *slot/port*`}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls ip multicast`	レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにします。
ステップ 3	`Router(config-if)# no mls ip multicast`	レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、レイヤ 3 インターフェイス上で IP マルチキャスト レイヤ 3 スイッチングをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

レプリケーション モードの設定

（注） Supervisor Engine 32 および Supervisor Engine 2 は、入力レプリケーション モードのみをサポートします。

Supervisor Engine 720 の場合、Release12.2(18)SXF 以降のリリースで、**egress** キーワードがサポートされます。**egress** キーワードのサポートは、リリース ノートおよび Feature Navigator で「マルチキャスト拡張機能 - レプリケーション モード検出」と呼ばれます。

デフォルトでは、Supervisor Engine 720 はシステムにインストールされたモジュール タイプに基づいてレプリケーション モードを自動的に検出します。すべてのモジュールが出力レプリケーションに対応している場合、システムは出力レプリケーション モードを使用します。スーパーバイザ エンジンが、出力レプリケーションに対応していないモジュールを検出した場合、レプリケーション モードは自動的に入力レプリケーションに切り替わります。出力レプリケーションをサポートしないファブリック対応モジュール（Optical Services Module （OSM; オプティカル サービス モジュール）など）がインストールされている場合でも、引き続きシステムを出力レプリケーション モードで動作させるには、**mls ip multicast replication-mode egress** コマンドを入力することで、この動作を上書きできます。また、入力レプリケーション モードでのみ動作するようにシステムを設定することもできます。

システムが自動検出モードで動作中に、出力レプリケーションを実行できないモジュールをインストールする場合、次のことが発生します。

- システムが入力モードに戻る
- システム ログが生成される
- システム リロードが発生し、古い設定に戻る

システムが強制出力モードで動作する場合、出力レプリケーション モードに対応していないモジュールの存在を表示するシステム ログが作成されます。

（注） 出力レプリケーションに対応しないファブリック対応モジュールのあるシステムで強制出力モードを設定した場合、これらのモジュールがマルチキャスト トラフィックを送受信しないことを確認する必要があります。

（注） 出力モードは、QoS とも SPAN とも互換性がありません。QoS を設定すると、出力レプリケーションで正しくない COS または DSCP マーキングのパケットが発生する可能性があります。SPAN を設定すると、出力レプリケーションで SPAN 宛先ポートに送信されないマルチキャスト パケットが発生する可能性があります。QoS または SPAN を使用していて、スイッチング モジュールが出力レプリケーションできる場合は、**mls ip multicast replication-mode ingress** コマンドを入力して出力レプリケーションを強制してください。

出力レプリケーション モードから入力レプリケーション モードに変わる間、ショートカットが消去され再インストールされるので、トラフィックが中断する場合があります。トラフィック転送の中断を避けるには、グローバル コンフィギュレーション モードで **mls ip multicast replication-mode ingress** コマンドを入力します。このコマンドは、強制的に入力レプリケーションモードで動作するようにシステムを設定します。

mls ip multicast replication-mode ingress コマンドの **no** 形式により、システムは自動検出モードに戻ります。

IP マルチキャスト レイヤ 3 スイッチングをイネーブルするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls ip multicast replication-mode** [**egress** | **ingress**]	レプリケーション モードを指定します。 （注）　Release12.2(18)SXF 以降のリリースでは、**egress** キーワードがサポートされます。
ステップ 2	Router# **show mls ip multicast capability**	設定されているレプリケーション モードを表示します。
ステップ 3	Router# **show mls ip multicast summary**	レプリケーション モードおよび自動検出がイネーブルかディセーブルかを表示します。

次に、レプリケーション モードをイネーブルにする例を示します。

```
Router (config)# mls ip multicast replication-mode egress
Router# show mlp ip multicast capability
Current mode of replication is Ingress
Configured replication mode is Egress

 Slot           Multicast replication capability
    2                        Egress
    3                        Egress
    4                       Ingress
    5                        Egress
    6                        Egress

Router# show mls ip multicast summary
4 MMLS entries using 656 bytes of memory
Number of partial hardware-switched flows:2
Number of complete hardware-switched flows:2

Directly connected subnet entry install is enabled
Current mode of replication is Ingress
Auto-detection of replication mode is enabled
Consistency checker is enabled
Router (config)#
```

ローカル出力レプリケーションのイネーブル化

（注） Supervisor Engine 32 および Supervisor Engine 2 は、入力レプリケーション モードのみをサポートします。

Supervisor Engone 720 の場合、Release12.2(18)SXF 以降のリリースで、ローカル出力レプリケーションを無条件にイネーブルにできます。この機能は、リリース ノートおよび Feature Navigator で「マルチキャスト拡張機能 - 出力レプリケーション パフォーマンス改善」と呼ばれます。

デュアル スイッチ ファブリック接続の DFC 搭載モジュールは、ファブリック接続ごとに 1 つずつ、合計 2 つのパケット レプリケーション エンジンをホストします。各レプリケーション エンジンは、スイッチ ファブリック接続に関連付けられたインターフェイスとの間で送受信されるパケットの転送を受け持ちます。スイッチ ファブリック接続に関連付けられたインターフェイスは、パケット レプリケーション エンジンから「ローカル」と見なされます。

Release 12.2(18)SXF 以降のリリースでは、スイッチ ファブリック接続上のマルチキャスト パケットの重複レプリケーションを行わないようにできます。このようにするには、レプリケーション エンジンがサポートするスイッチ ファブリック接続に関連付けられたローカル インターフェイスにのみパケットを転送するように、これらのモジュールに搭載された 2 つのレプリケーション エンジンに対して指示するコマンドを入力します。

この機能をイネーブルにすると、各レプリケーション エンジンの Multicast Expansion Table（MET; マルチキャスト拡張テーブル）には、ローカル レイヤ 3 インターフェイスだけが読み込まれます。この動作により、レプリケーション エンジンでサポートされていないインターフェイス（非ローカル インターフェイス）でレプリケーションが実行されなくなり、レプリケーションのパフォーマンスが向上します。

ローカルの出力レプリケーションは、以下のソフトウェア設定およびハードウェアでサポートされます。

- IPv4 出力レプリケーション モード
- デュアル ファブリック接続 DFC 搭載モジュール
- ポート チャネルの一部ではないレイヤ 3 ルーテッド インターフェイスおよびサブインターフェイス

ローカル出力レプリケーション機能は、以下の内部 VLAN ではサポートされません。

- 出力内部 VLAN
- 部分的なショートカット内部 VLAN
- マルチキャスト VPN Multicast Distribution Tree（MDT; マルチキャスト分散ツリー）トンネルの内部 VLAN
- ポイントツーポイント トンネル内部 VLAN
- QoS（サービス品質）内部 VLAN

（注） ローカル出力レプリケーション機能は、IPv6 マルチキャストト、および IPv4 と IPv6 混合マルチキャストがイネーブルであるシステムではサポートされません。

ローカル出力レプリケーションをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls ip multicast egress local`	ローカル出力レプリケーションをイネーブルにします。 **（注）** このコマンドで設定を有効にするには、システムをリセットする必要があります。
ステップ 2	`Router # reload`	システムをリロードします。
ステップ 3	`Router# show mls ip multicast capability` `Router# show mls cef ip multicast detail`	設定されているレプリケーション モードを表示します。

次に、ローカル出力レプリケーションをイネーブルにする例を示します。

```
Router (config)# mls ip multicast egress local
Router (config)# exit
Router # reload
Router # show mls ip multicast capability
Current mode of replication is Ingress
Configured replication mode is Egress
Egress Local is Enabled
Slot Multicast replication capability Egress Local
2 Egress No
3 Egress Yes
4 Ingress No
5 Egress No
6 Egress No
```

レイヤ 3 スイッチングのグローバル スレッシュホールドの設定

スレッシュホールドに満たないマルチキャスト トラフィックは、すべて MSFC によってルーティングされるように、グローバルなマルチキャスト レート スレッシュホールド（パケット/秒で指定）を設定できます。この設定により、低速のレイヤ 3 フローに対応するスイッチング キャッシュ エントリの作成を防止できます。

（注） このコマンドは、すでにルーティングされているフローには影響しません。既存のルートにスレッシュホールドを適用するには、ルートをいったん消去して、再び確立させます。

レイヤ 3 スイッチング スレッシュホールドを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls ip multicast threshold` *ppsec*	IP MMLS スレッシュホールドを設定します。
`Router(config)# no mls ip multicast threshold`	デフォルトの IP MMLS スレッシュホールドに戻します。

次に、レイヤ 3 スイッチング スレッシュホールドを 10 パケット/秒に設定する例を示します。

```
Router(config)# mls ip multicast threshold 10
Router(config)#
```

直接接続されたサブネットのインストールのイネーブル化

PIM sparse（疎）モードでは、インターフェイスの指定ルータであるファースト ホップ ルータが、送信元トラフィックを PIM 登録メッセージにカプセル化し、それを RP にユニキャストしなければならない場合があります。グループの新しい送信元がルーティング テーブルで学習されないようにするには、(*,G）フローを完全なハードウェア スイッチド フローのままにする必要があります。ハードウェアに（subnet/mask, 224/4）エントリをインストールすると、FIB によって（*,G）フローが完全なハードウェア スイッチド フローのままになり、新たに直接接続された送信元が正常に学習されます。直接接続されたサブネットのインストールは、デフォルトでグローバルにイネーブル化されます。PIM 対応のインターフェイスごとに（subnet/mask, 224/4）が 1 つインストールされます。

FIB エントリを表示するには、**show mls ip multicast connected** コマンドを入力します。

直接接続されたサブネットのインストールをイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mls ip multicast connected`	直接接続されたサブネットのインストールをイネーブルにします。
`Router(config)# no mls ip multicast connected`	直接接続されたサブネットのインストールをディセーブルにします。

次に、直接接続されたサブネットのインストールをイネーブルにする例を示します。

```
Router(config)# mls ip multicast connected
Router(config)#
```

フロー統計情報メッセージ インターバルの指定

デフォルトでは、スーパーバイザ エンジンはフロー統計情報メッセージを 25 秒ごとに MSFC へ転送します。メッセージはバッチ単位で転送され、各メッセージ バッチにはフロー全体の 25% の統計情報が含まれます。デフォルトの 25 秒にインターバルが設定されたままの場合、すべてのフローの統計情報を MSFC へ転送するには 100 秒かかります。

スーパーバイザ エンジンからフロー 統計情報メッセージを MSFC へ転送する頻度を指定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls ip multicast flow-stat-timer` *num*	スーパーバイザ エンジンがフロー 統計情報メッセージを MSFC へ転送する頻度を指定します。
`Router(config)# no mls ip multicast flow-stat-timer` *num*	デフォルトに戻します。

次に、10 秒ごとにフロー統計情報メッセージを MSFC へ転送するようにスーパーバイザ エンジンを設定する例を示します。

```
Router(config)# mls ip multicast flow-stat-timer 10
Router(config)#
```

ショートカット整合性検査のイネーブル化

ショートカット整合性検査機能をイネーブルにすると、マルチキャスト ルート テーブルおよびマルチキャスト ハードウェア エントリの整合性を検査し、矛盾を修正します。**show mls ip multicast consistency-check** コマンドを入力して、矛盾を表示できます。

整合性検査がイネーブルの場合、マルチキャスト ルート テーブルは 2 分ごとにスキャンされ、全体スキャンは 4 分以内に完了します。

ショートカットの整合性検査をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mls ip multicast consistency-check`	ショートカットの整合性検査をイネーブルにします。
`Router(config)# no mls ip multicast consistency-check` *num*	デフォルトに戻します。

次に、ハードウェア ショートカットの整合性検査をイネーブルにする例を示します。

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

RPF 障害に対する ACL ベースのフィルタリングの設定

RPF 障害に対する ACL ベースのフィルタリングを設定すると、ハードウェアで RPF 障害をフィルタリングするための ACL がハードウェア ベースの ACL エンジンにダウンロードされ、指定するインターフェイスに適用されます。

RPF 障害に対する ACL ベースのフィルタリングをインターフェイス上でイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan` *vlan_ID*`} | {`*type*[1] *slot/port*`} | {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 2	`Router(config-if)# mls ip multicast stub`	RPF 障害に対する ACL ベースのフィルタリングを、インターフェイス上でイネーブルにします。
	`Router(config-if)# no mls ip multicast stub`	RPF 障害に対する ACL ベースのフィルタリングを、インターフェイス上でディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

RPF 障害のレート制限情報の表示

RPF 障害のレート制限情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show mls ip multicast summary**	RPF 障害のレート制限情報を表示します。

次に、RPF 障害のレート制限情報を表示する例を示します。

```
Router# show mls ip multicast summary
10004 MMLS entries using 1280464 bytes of memory
Number of partial hardware-switched flows:4
Number of complete hardware-switched flows:10000
Router#
```

マルチキャスト境界の設定

マルチキャスト境界を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**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 2	Router(config-if)# **ip multicast boundary** *access_list* [**filter-autorp**]	インターフェイス上で管理上スコープ設定された境界をイネーブルにします。 • *access_list* には、この境界でのトラフィックをフィルタリングするように設定されたアクセスリストを指定します。 • （任意）この境界で自動 RP メッセージをフィルタリングするように **filter-autorp** を指定します。
	Router(config-if)# **no ip multicast boundary**	このインターフェイスのマルチキャスト境界をディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

（注） **filter-autorp** キーワードを設定すると、管理境界で自動 RP 検出メッセージと通知メッセージが調べられ、境界 ACL によって拒否される自動 RP パケットの自動 RP グループ範囲の通知はすべて削除されます。自動 RP グループ範囲通知は、自動 RP グループ範囲内のすべてのアドレスが境界 ACL によって許可されている場合にだけ許可され、境界で渡されます。許可されていないアドレスが 1 つでもあると、その自動 RP メッセージが転送される前に、そのグループ範囲全体がフィルタリングされ、自動 RP メッセージから削除されます。

次に、管理上スコープ設定されたすべてのアドレスのマルチキャスト境界をセットアップする例を示します。

```
Router (config)# access-list 1 deny 239.0.0.0 0.255.255.255
Router (config)# access-list 1 permit 224.0.0.0 15.255.255.255
Router (config)# interface gigabitethernet 5/2
Router (config-if)# ip multicast boundary 1
```

IPv4 マルチキャスト レイヤ 3 ハードウェア スイッチング要約情報の表示

（注）　**show interface statistics** コマンドでは、ハードウェア スイッチングされたパケットについては表示されず、ソフトウェア スイッチングされたパケットに関する情報だけが表示されます。

show ip pim interface count コマンドを実行すると、IP PIM インターフェイス上の IP マルチキャスト レイヤ 3 スイッチングのイネーブル ステート、およびそのインターフェイス上で送受信されたパケット数が表示されます。

IP PIM レイヤ 3 インターフェイスに関する IP マルチキャスト レイヤ 3 スイッチング情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Router# **show ip pim interface** [{{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}] **count**	すべての MSFC IP PIM レイヤ 3 インターフェイスに関する、IP マルチキャスト レイヤ 3 スイッチングのイネーブル ステート情報を表示します。
Router# **show ip interface**	レイヤ 3 インターフェイス上の IP マルチキャスト レイヤ 3 スイッチングのイネーブル ステートを表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイスの IP PIM 設定を表示する例を示します。

```
Router# show ip pim interface count

State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface          FS  Mpackets In/Out
10.15.1.20       GigabitEthernet4/8 * H 952/4237130770
10.20.1.7        GigabitEthernet4/9 * H 1385673757/34
10.25.1.7        GigabitEthernet4/10* H 0/34
10.11.1.30       FastEthernet6/26   * H 0/0
10.37.1.1        FastEthernet6/37   * H 0/0
1.22.33.44       FastEthernet6/47   * H 514/68
```

[*] フラグはこのインターフェイスを高速スイッチングできることを示し、[H] フラグはこのインターフェイスをハードウェアでスイッチングすることを示します。[In] フラグは、インターフェイスで受信されたマルチキャスト パケット バイト数を示します。[Out] フラグは、インターフェイスから転送されたマルチキャスト パケット バイト数を示します。

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```

（注）　-tive カウンタは、対応するエントリの出力インターフェイス リストがヌルであることを意味し、このフローが引き続きアクティブであることを表します。

次に、インターフェイス VLAN 10 について、IP マルチキャスト レイヤ 3 スイッチングの設定を表示する例を示します。

```
Router# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.0.0.6/8
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.13 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
IP multicast multilayer switching is enabled
IP mls switching is enabled
Router#
```

次に、ギガビット イーサネット インターフェイス 1/2 について、IP マルチキャスト レイヤ 3 スイッチングの設定を表示する例を示します。

```
Router# show interfaces gigabitEthernet 1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 0001.c9db.2441 (bia 0001.c9db.2441)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
  Last clearing of "show interface" counters 00:05:13
  ….
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 10000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     284 packets input, 113104 bytes, 0 no buffer
     Received 284 broadcasts (284 multicast)
     0 runts, 41 giants, 0 throttles
     41 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     198 packets output, 14732 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

IPv4 マルチキャスト ルーティング テーブルの表示

show ip mroute コマンドを実行すると、IP マルチキャスト ルーティング テーブルが表示されます。

IP マルチキャスト ルーティング テーブルを表示するには、次の作業を行います。

コマンド	目的
Router# **show ip mroute partical-sc** [*hostname* | *group_number*]	IP マルチキャスト ルーティング テーブルおよびハードウェア スイッチド インターフェイスを表示します。

次に、IP マルチキャスト ルーティング テーブルを表示する例を示します。

```
Router# show ip mroute 230.13.13.1
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
           Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:
 GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H
```

```
(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H
(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
 Outgoing interface list:Null
Router#
```

（注）　RPF-MFD フラグは、フローが完全にハードウェアでスイッチングされていることを表します。H フラグは、フローが出力インターフェイス上でハードウェアによってスイッチングされていることを示します。

IPv4 マルチキャスト レイヤ 3 スイッチング統計情報の表示

show mls ip multicast コマンドを実行すると、IP マルチキャスト レイヤ 3 スイッチングに関する詳細情報が表示されます。

IP マルチキャスト レイヤ 3 スイッチングに関する詳細情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Router# **show mls ip multicast group** *ip_address* [**interface** *type slot/port* | **statistics**]	IP マルチキャスト レイヤ 3 スイッチング グループの情報を表示します。
Router# **show mls ip multicast interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}} [**statistics** | **summary**]	すべてのインターフェイスについて、IP マルチキャスト レイヤ 3 スイッチングの詳細情報を表示します。
Router# **show mls ip multicast source** *ip_address* [**interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}} | **statistics**]	IP マルチキャスト レイヤ 3 スイッチングの送信元の情報を表示します。
Router# **show mls ip multicast summary**	IP マルチキャスト レイヤ 3 スイッチングの要約情報を表示します。
Router# **show mls ip multicast statistics**	IP マルチキャスト レイヤ 3 スイッチングの統計情報を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、特定の IP マルチキャスト レイヤ 3 スイッチング エントリに関する情報を表示する例を示します。

```
Router# show mls ip multicast group 10.1.0.11
Multicast hardware switched flows:
Total shortcut installed: 0
```

次に、IP マルチキャスト グループの情報を表示する例を示します。

```
Router# show mls ip multicast group 230.13.13.1 source 10.20.1.15
Multicast hardware switched flows:
(10.20.1.15, 230.13.13.1) Incoming interface:Gi4/8, Packets switched:0
Hardware switched outgoing interfaces:Gi4/9
RPF-MFD installed

Total hardware switched flows :1
Router#
```

次に、VLAN 10 について、IP マルチキャスト レイヤ 3 スイッチング情報を表示する例を示します。

```
Router# show mls ip multicast interface vlan 10
Multicast hardware switched flows:
(10.1.0.15, 224.2.2.15) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.19, 224.2.2.19) Incoming interface: Vlan10, Packets switched: 1970
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.11, 224.2.2.11) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.10, 224.2.2.10) Incoming interface: Vlan10, Packets switched: 2744
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.17, 224.2.2.17) Incoming interface: Vlan10, Packets switched: 3340
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.13, 224.2.2.13) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
```

次に、IP マルチキャスト レイヤ 3 スイッチングの統計情報を表示する例を示します。

```
Router# show mls ip multicast statistics
MLS Multicast Operation Status:
MLS Multicast configuration and state:
    Router Mac: 00e0.b0ff.7b00, Router IP: 33.0.33.24
    MLS multicast operating  state: ACTIVE
    Shortcut Request Queue size 4
    Maximum number of allowed outstanding messages: 1
    Maximum size reached from feQ: 3096
    Feature Notification sent: 1
    Feature Notification Ack received: 1
    Unsolicited Feature Notification received: 0
    MSM sent: 205170
    MSM ACK received: 205170
    Delete notifications received: 0
    Flow Statistics messages received: 35211
MLS Multicast statistics:
    Flow install Ack: 996508
    Flow install Nack: 1
    Flow update Ack: 1415959
    Flow update Nack: 0
    Flow delete Ack: 774953
    Complete flow install Ack: 958469
Router#
```

IPv4 双方向 PIM の設定

このセクションでは、IPv4 双方向 PIM を設定する手順について説明します。

IPv4 双方向 PIM のグローバルなイネーブル化

IPv4 双方向 PIM をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip pim bidir-enable`	スイッチ上で IPv4 双方向 PIM をグローバルにイネーブルにします。
`Router(config)# no ip pim bidir-enable`	スイッチ上で IPv4 双方向 PIM をグローバルにディセーブルにします。

次に、スイッチで IPv4 双方向 PIM をイネーブルにする例を示します。

```
Router(config)# ip pim bidir-enable
Router(config)#
```

IPv4 双方向 PIM グループの RP の設定

IPv4 双方向 PIM グループの RP をスタティックに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip pim rp-adress ip_address access_list [override]`	グループの RP の IP アドレスをスタティックに設定します。**override** オプションを指定する場合、スタティック RP が使用されます。
ステップ 2	`Router(config)# access-list access-list permit | deny ip_address`	アクセス リストを設定します。
ステップ 3	`Router(config)# ip pim send-rp-announce type number scope ttl_value [group-list access-list] [interval seconds] [bidir]`	Auto-RP を使用してルータが RP として動作するグループを設定するように、システムを設定します。
ステップ 4	`Router(config)# ip access-list standard access-list-name permit | deny ip_address`	標準 IP アクセス リストを設定します。
ステップ 5	`Router(config)# mls ip multicast`	MLS IP マルチキャストをイネーブルにします。

次に、IPv4 双方向 PIM グループのスタティック RP を設定する例を示します。

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255
```

IPv4 双方向 PIM スキャン インターバルの設定

IPv4 双方向 PIM RP RPF スキャンの間のインターバルを指定できます。

IPv4 双方向 PIM RP RPF スキャン インターバルを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls ip multicast bidir gm-scan-interval** *interval*	IPv4 双方向 PIM RP RPF スキャン インターバルを指定します。有効な範囲は、1 ～ 1000 秒です。デフォルト値は 10 秒です。
Router(config)# **no mls ip multicast bidir gm-scan-interval**	デフォルトに戻します。

次に、IPv4 双方向 PIM RP RPF スキャン インターバルを設定する例を示します。

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

IPv4 双方向 PIM 情報の表示

IPv4 双方向 PIM 情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
Router# **show ip pim rp mapping** [**in-use**]	PIM グループと RP の間のマッピング、および使用中の学習した RP を表示します。
Router# **show mls ip multicast rp-mapping** [*rp_address*]	アクティブな RP マッピングに対する PIM グループを表示します。
Router# **show mls ip multicast rp-mapping gm-cache**	RP マッピング キャッシュのグループ/マスク範囲に基づいた情報を表示します。
Router# **show mls ip multicast rp-mapping df-cache**	RP マッピング キャッシュの DF リストに基づいた情報を表示します。
Router# **show mls ip multicast bidir**	IPv4 双方向 PIM 情報を表示します。
Router# **show ip mroute**	マルチキャスト ルーティング テーブルの情報を表示します。

次に、PIM グループおよび RP マッピングの情報を表示する例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
  RP 60.0.0.60 (?), v2v1, bidir
    Info source:60.0.0.60 (?), elected via Auto-RP
         Uptime:00:03:47, expires:00:02:11
  RP 50.0.0.50 (?), v2v1, bidir
    Info source:50.0.0.50 (?), via Auto-RP
         Uptime:00:03:04, expires:00:02:55
  RP 40.0.0.40 (?), v2v1, bidir
    Info source:40.0.0.40 (?), via Auto-RP
         Uptime:00:04:19, expires:00:02:38
```

次に、IPv4 双方向 PIM に関連した IP マルチキャスト ルーティング テーブルの情報を表示する例を示します。

```
Router# show ip mroute bidirectional
    (*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H

    (*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H

    (*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
```

次に、特定のマルチキャスト ルートに関連した情報を表示する例を示します。次の出力では、余白の矢印は部分的なショートカット情報を示しています。

```
Router# show ip mroute 239.1.1.2 4.4.4.4
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
 Timers:Uptime/Expires
 Interface state:Interface, Next-Hop or VCD, State/Mode

(4.4.4.4, 239.1.1.2), 1d02h/00:03:20, flags:FTZ
 Incoming interface:Loopback0, RPF nbr 0.0.0.0, Partial-SC
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 1d02h/00:02:39 (ttl-threshold 5)
```

次に、特定のマルチキャスト グループ アドレスのエントリを表示する例を示します。

```
Router# show mls ip multicast group 230.31.31.1
Multicast hardware switched flows:
(*, 230.31.31.1) Incoming interface:Vlan611, Packets switched:1778
Hardware switched outgoing interfaces:Vlan131 Vlan151 Vlan415 Gi4/16 Vlan611
RPF-MFD installed
```

次に、アクティブな RP マッピングに対する PIM グループを表示する例を示します。

```
Router# show mls ip multicast rp-mapping
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State       RPF            DF-count    GM-count
60.0.0.60       H           Vl611                 4           1
```

次に、RP マッピング キャッシュのグループ/マスク範囲に基づいた情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping gm-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending,
       Z - Zombie

RP Address      State       Group           Mask            State         Packet/Byte-count
60.0.0.60       H           230.31.0.0      255.255.0.0     H             100/6400
```

次に、特定の MLS IP マルチキャスト グループの情報を表示する例を示します。

```
Router# show mls ip multicast rp-mapping df-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State        DF             State
60.0.0.60       H           Vl131           H
60.0.0.60       H           Vl151           H
60.0.0.60       H           Vl415           H
60.0.0.60       H           Gi4/16          H
```

IPv4 デバッグ コマンドの使用

表 28-2 に、IPv4 マルチキャスト レイヤ 3 スイッチングの デバッグ コマンドを示します。これらのコマンドを使用して、IP マルチキャスト レイヤ 3 スイッチングの問題をトラブルシューティングできます。

表 28-2　IP マルチキャスト レイヤ 3 スイッチングの デバッグ コマンド

コマンド	説明
[no] **debug mls ip multicast events**	IP マルチキャスト レイヤ 3 スイッチング イベントを表示します。
[no] **debug mls ip multicast errors**	マルチキャスト MLS 関連のエラーに関するデバッグ メッセージをオンにします。
[no] **debug mls ip multicast group** *group_id group_mask*	フローのサブセットに対してデバッグをオンにします。
[no] **debug mls ip multicast messages**	ハードウェア スイッチング エンジンとの間で送受信される IP マルチキャスト レイヤ 3 スイッチング メッセージを表示します。
[no] **debug mls ip multicast all**	すべての IP マルチキャスト レイヤ 3 スイッチング メッセージをオンにします。
[no] **debug mdss errors**	MDSS[1] エラー メッセージをオンにします。
[no] **debug mdss events**	デバッグ用の MDSS 関連イベントを表示します。
[no] **debug mdss events mroute-bidir**	デバッグ用の IPv4 双方向 PIM MDSS イベントを表示します。
[no] **debug mdss all**	すべての MDSS メッセージを表示します。
[no] **debug ip pim df** *ip_address*	デバッグするために、特定の RP の DF 選定を表示します。

1. MDSS = Multicast Distributed Switching Services

IPv4 マルチキャスト レイヤ 3 スイッチング統計情報の消去

IP マルチキャスト レイヤ 3 スイッチング統計情報を消去するには、次の作業を行います。

コマンド	目的
`Router# clear mls ip multicast statistics`	IP マルチキャスト レイヤ 3 スイッチング統計情報を消去します。

次に、IP マルチキャスト レイヤ 3 スイッチング統計情報を消去する例を示します。

```
Router# clear mls ip multicast statistics
```

show mls multicast statistics コマンドを実行すると、PFC が処理しているマルチキャスト フローに関する各種の情報が表示されます。関連する MSFC、VLAN、マルチキャスト グループ アドレス、またはマルチキャスト トラフィック送信元を任意に組み合わせて、エントリを表示できます。**show mls ip multicast statistics** コマンドの例は、「IPv4 マルチキャスト レイヤ 3 スイッチング統計情報の表示」（P.28-24）を参照してください。

マルチキャスト トラフィックの冗長性

マルチキャスト トラフィックに冗長性を持たせるには、以下の条件が必要です。

- OSPF、EIGRP などのユニキャスト ルーティング プロトコル

  PIM は、ユニキャスト ルーティング テーブルに対して RPF チェックを使用して、マルチキャスト データが経由する正しいパスを決定します。ユニキャスト ルーティング テーブルが変わると、PIM は、PIM に使用される RPF チェックが動作し続け、マルチキャスト ストリームの送信元サーバのソース IP アドレスとの間の有効なユニキャスト パスを示すことができるように、正しく収束させるために、ユニキャスト ルーティング プロトコル（OSPF）に頼ります。

- 関連するすべてのレイヤ 3 インターフェイスで設定された PIM

  PIM のパス選択を行うために、ユニキャスト ルーティング テーブルが使用されます。PIM は、クライアント（受信側 VLAN）とソース（マルチキャスト側 VLAN）の間の最も短いパス ツリー（SPT）を最終決定するために、RPF チェックを使用します。したがって、PIM の目標は、受信側サブネットとソース サブネットの間の最も短いユニキャスト パスを見つけることです。ユニキャスト ルーティング プロトコルが期待どおりに動作しており、ユニキャスト ルーティング プロトコルに関連付けられているすべてのレイヤ 3 リンク上で PIM が設定されている場合は、マルチキャストのためにその他のものは一切設定する必要がありません。

CHAPTER 29

IPv6 マルチキャスト トラフィック用の Multcast Listener Discovery version 2（MLDv2）スヌーピングの設定

この章では、Catalyst 6500 シリーズ スイッチの IPv6 マルチキャスト トラフィックに Multcast Listener Discovery version 2（MLDv2）スヌーピングを設定する手順について説明します。Release 12.2(18)SXE 以降のリリースでは、全バージョンの PFC3 で MLDv2 がサポートされます。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- IPv4 マルチキャスト トラフィックを抑制するには、第 30 章「IPv4 マルチキャスト トラフィック用インターネット グループ管理プロトコル（IGMP）スヌーピングの設定」を参照してください。
- MLD バージョン 1 はサポートされていません。

この章で説明する内容は、次のとおりです。

MLDv2 スヌーピングの機能概要

ここでは、MLDv2 スヌーピングについて説明します。

MLDv2 スヌーピングの概要

MLDv2 スヌーピングにより、Catalyst 6500 シリーズ スイッチで MLDv2 パケットを調べ、パケットの内容に基づいて転送先を決定できます。

MLDv2 または MLDv2 スヌーピング クエリアからの MLDv2 クエリーを受信するサブネットで、MLDv2 スヌーピングを使用するように、スイッチを設定できます。MLDv2 スヌーピングは、IPv6 マルチキャスト トラフィックが受信対象のポートだけに転送されるようにレイヤ 2 LAN ポートをダイナミックに設定し、それによって、レイヤ 2 で IPv6 マルチキャスト トラフィックを抑制します。

MLDv2 は、マルチキャスト ルータのレイヤ 3 で稼動し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 MLDv2 クエリーを生成します。MLDv2 の詳細については、次のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mcast.htm

MLDv2 スヌーピング クエリアをスイッチに設定して、マルチキャスト ルータ インターフェイスがないサブネットにおいて MLDv2 スヌーピングをサポートできます。MLDv2 スヌーピング クエリアの詳細については、「MLDv2 スヌーピング クエリアのイネーブル化」（P.29-10）を参照してください。

MLDv2（マルチキャスト ルータ上）または MLDv2 スヌーピング クエリア（スーパーバイザ エンジン上）は、スイッチが Virtual LAN（VLAN; 仮想 LAN）のすべてのポートを通じて転送する、一般的な MLDv2 クエリーを定期的に送信し、ホストがそれに応答します。MLDv2 スヌーピングは、レイヤ 3 MLDv2 トラフィックをモニタします。

（注）　PFC/DFC 3B/3BXL は送信元のみの Layer 2 エントリをサポートしていないため、送信元のみのネットワークでは IPv6 マルチキャスト フラッディングを防止できません。

（注）　マルチキャスト グループで、VLAN 中に送信元のみがありレシーバーがない場合は、MLDv2 スヌーピングはマルチキャスト トラフィックをマルチキャスト ルータ ポート宛てのみに抑制します。

MLDv2 メッセージ

MLDv2 で使用されるメッセージは以下のとおりです。

- マルチキャスト リスナー クエリー
  - 一般クエリー：どのマルチキャスト アドレスにリスナーがいるかを学習するためにマルチキャスト ルータから送信されます。
  - マルチキャスト アドレス固有クエリー：特定のマルチキャスト アドレスにリスナーがいるかどうかを学習するためにマルチキャスト ルータから送信されます。
  - マルチキャスト アドレスおよび送信元固有クエリー：特定のマルチキャスト アドレス用指定リストの送信元に、リスナーがいるかどうかを学習するために、マルチキャスト ルータから送信されます。
- マルチキャスト リスナー レポート
  - 現在のステート レコード（送信請求）：ホストが関係するすべてのマルチキャスト グループの INCLUDE または EXCLUDE モードを指定するために、クエリーに対する応答でホストから送信されます。
  - フィルタ モード変更レコード（非送信請求）：1 つまたは複数のマルチキャスト グループの INCLUDE または EXCLUDE モードを変更するためにホストから送信されます。
  - 送信元リスト変更レコード（非送信請求）：マルチキャスト送信元に関する情報を変更するためにホストから送信されます。

送信元ベースのフィルタリング

MLDv2 は送信元ベースのフィルタリングを使用します。これによりホストおよびルータは、特定のマルチキャスト グループで許可またはブロックされる送信元アドレスを特定できます。送信元ベースのフィルタリングでは、MLDv2 メッセージ内にある以下の情報に基づいてトラフィックの許可またはブロックを行います。

- 送信元リスト
- INCLUDE または EXCLUDE モード

レイヤ 2 テーブルが（Media Access Control（MAC; メディア アクセス制御）グループ、VLAN）ベースのため、MLDv2 のホストを使用する場合、マルチキャストの送信元は、各 MAC グループごとに 1 つだけ設定することを推奨します。

（注）　送信元ベースのフィルタリングは、ハードウェアではサポートされません。このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。

明示的なホスト トラッキング

MLDv2 では、ポート上のメンバシップ情報の明示的なホスト トラッキングをサポートします。明示的なトラッキング データベースは、高速脱退処理、プロキシ レポート機能、統計情報収集に使用されます。VLAN で 明示的なトラッキングがイネーブルの場合、MLDv2 スヌーピング ソフトウェアはホストから受信する MLDv2 通知を処理し、次の情報を含む明示的なトラッキング データベースを作成します。

- ホストに接続されたポート
- ホストによって通知されたチャネル
- ホストによって通知された各グループのフィルタ モード
- ホストによって通知された各グループの送信元リスト
- 各グループのルータ フィルタ モード
- 送信元を要求するグループごとのホスト リスト

（注）
- 明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。
- 明示的なホスト トラッキングがイネーブルでスイッチが report-suppression モードで動作している場合、マルチキャスト ルータは VLAN インターフェイスを介してアクセスされるホストをすべてトラッキングできない場合があります。

MLDv2 スヌーピング プロキシ レポート機能

MLDv2 にはレポート抑制がないので、すべてのホストがクエリーに応じて詳細なマルチキャスト メンバシップ情報をマルチキャスト ルータに送信します。スイッチは応答をスヌーピングし、データベースを更新し、レポートをマルチキャスト ルータに転送します。マルチキャスト ルータがレポートで過負荷になるのを防止するために、MLDv2 スヌーピングはプロキシ レポート機能を実行します。

プロキシ レポート機能は、マルチキャスト グループの最初のレポートのみをルータに転送し、同じマルチキャスト グループの他のレポートをすべて抑制します。

プロキシ レポート機能は、送信請求レポートと非送信請求レポートの両方を処理します。プロキシ レポート機能はイネーブルで、ディセーブルにすることはできません。

（注）　明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。

IPv6 マルチキャストグループへの加入

ホストは、IPv6 マルチキャスト ルータからの一般的なクエリーに応じて、非送信請求 MLDv2 レポートを送信するか、または MLDv2 レポートを送信して、IPv6 マルチキャスト グループに参加します（スイッチは、一般的なクエリーを、IPv6 マルチキャスト ルータから VLAN 中のすべてのポートに転送します）。スイッチは、これらのレポートをスヌーピングします。

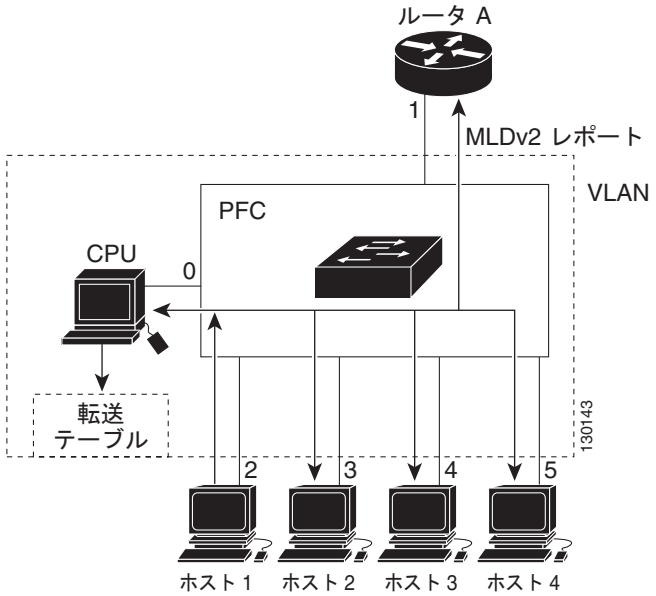
スヌーピングされた MLDv2 レポートに応じて、スイッチは、レポートを受信した VLAN のレイヤ 2 転送テーブルにエントリを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが MLDv2 レポートを送る場合、スイッチは、レポートをスヌーピングして既存のレイヤ 2 転送テーブル エントリにそれを追加します。スイッチは、MLDv2 レポートをスヌーピングする各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリのみを生成します。

MLDv2 スヌーピングは、マルチキャスト グループごとに 1 つを除いたすべてのホスト レポートを抑制し、その 1 つのレポートを IPv6 マルチキャスト ルータに転送します。

スイッチは、レポートで指定されたマルチキャスト グループ用のマルチキャスト トラフィックを、レポートを受信したインターフェイスに転送します（図 29-1 を参照）。

MLDv2 スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、**mac-address-table static** コマンドを使用して、レイヤ 2 マルチキャスト グループ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 アドレスのグループ メンバシップをスタティックに指定した場合、そのスタティックな設定は、MLDv2 スヌーピングの学習よりも優先されます。マルチキャスト グループ メンバシップのリストは、スタティックな設定値と、MLDv2 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。

図 29-1　　最初の MLDv2 リスナー レポート



マルチキャスト ルータ A が MLDv2 一般クエリーをスイッチに送信し、スイッチがそのクエリーを、同じ VLAN の全メンバのポート 2 ～ 5 に転送します。ホスト 1 は、IPv6 マルチキャスト グループに加入する意思があり、MLDv2 レポートを 0x0100.5E01.0203 と同じ MAC 宛先アドレスを持つグループにマルチキャストします。スイッチは、ホスト 1 による MLDv2 レポート マルチキャストをスヌーピングすると、スイッチは MLDv2 レポート内の情報を利用して、表 29-1 に示すように転送テーブル エントリを作成します。これには、ホスト 1 のポート番号、マルチキャスト ルータ、スイッチが含まれます。

表 29-1　MLDv2 スヌーピング転送テーブル

宛先 MAC アドレス	パケットのタイプ	ポート
0100.5exx.xxxx	MLDv2	0
0100.5e01.0203	!MLDv2	1, 2

スイッチ ハードウェアは、MLDv2 情報パケットを、マルチキャスト グループ用の他のパケットと区別できます。テーブル中の最初のエントリは、スイッチに対して、MLDv2 パケットのみを CPU に送信するように指示します。これによって、スイッチがマルチキャスト フレームで過負荷になるのを防止できます。2 番目のエントリは、スイッチに、0x0100.5E01.0203 マルチキャスト MAC アドレス宛てのフレームを送信するように指示します。このフレームは、マルチキャスト ルータ宛て、およびグループに参加しているホスト宛ての MLDv2 パケットではありません（!MLDv2）。

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 MLDv2 レポートを送る場合（図 29-2 を参照）、スイッチがそのメッセージをスヌーピングし、ホスト 4 のポート番号を転送テーブルに追加します（表 29-2 を参照）。転送テーブルはスイッチ宛てにのみ MLDv2 メッセージを送るので、メッセージは他のポートへフラッディングされません。認識されているマルチキャスト トラフィックは、スイッチ宛てではなくグループ宛てに転送されます。

図 29-2　2 番目のホストのマルチキャスト グループへの加入

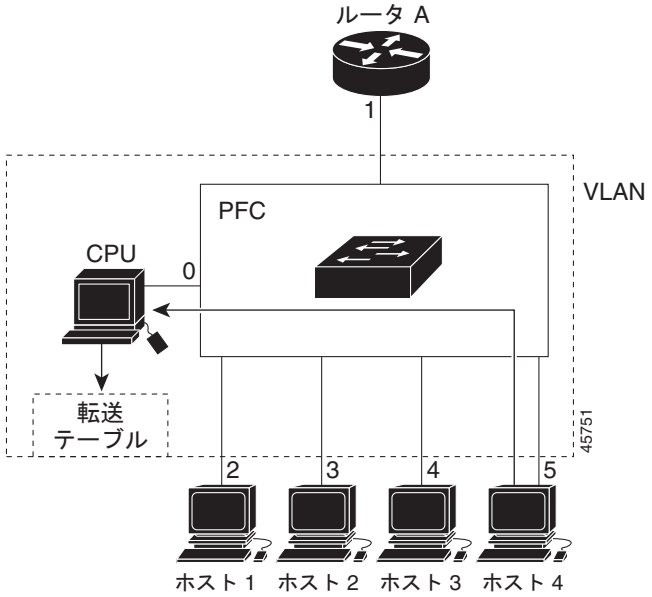


表 29-2　更新された MLDv2 スヌーピング転送テーブル

宛先 MAC アドレス	パケットのタイプ	ポート
0100.5exx.xxxx	MLDv2	0
0100.5e01.0203	!MLDv2	1, 2, 5

マルチキャスト グループからの脱退

ここでは、マルチキャスト グループからの脱退について説明します。

通常の脱退処理

関係するホストは、一般的 MLDv2 クエリーに定期的に応答を続ける必要があります。VLAN 中の少なくとも 1 つのホストが一般的 MLDv2 クエリーに定期的に応答している限り、マルチキャスト ルータは引き続きマルチキャスト トラフィックを VLAN に転送します。ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な一般的 MLDv2 クエリーを無視するか（「暗黙的脱退」といいます）、または MLDv2 フィルタ モード変更レコードを送信します。

MLDv2 スヌーピングが、グループの EXCLUDE モードを設定するホストからフィルタ モード変更レコードを受信すると、MAC アドレスの一般的なクエリーを送信して、そのインターフェイスに接続されている他のホストがその特定のマルチキャスト グループに対するトラフィックに関係があるかどうかを判断します。

MLDv2 スヌーピングが、この一般的クエリーに対して MLDv2 レポートを受信しなかった場合、インターフェイスに接続されている他のホストの中に、このマルチキャスト グループのトラフィックの受信に関与しているホストはないと見なし、指定されたマルチキャスト グループに対応するレイヤ 2 転送テーブル エントリからそのインターフェイスを削除します。

残りのインターフェイスのうち、グループに関係するホストが接続されたインターフェイスからのみフィルタ モード変更レコードが送信され、一般的なクエリーに応答する MLDv2 レポートを MLDv2 スヌーピングが受信しない場合、MLDv2 スヌーピングはグループ エントリを削除して、MLDv2 フィルタ モード変更レコードをマルチキャスト ルータにリレーします。マルチキャスト ルータが VLAN からレポートを受信しない場合、マルチキャスト ルータは MLDv2 キャッシュからその VLAN 用のグループを削除します。

テーブル エントリを更新するまでスイッチが待機する時間を、「最終メンバ クエリー時間」と呼びます。この時間を設定するには、**ipv6 mld snooping last-member-query-interval** *interval* コマンドを入力します。

高速脱退処理

高速脱退処理は、デフォルトでイネーブルに設定されています。高速脱退処理をディセーブルにするには、明示的なホスト トラッキングをオフにします。

高速脱退処理は、送信元グループ ベースのメンバシップ情報をソフトウェアに維持し、LTL インデックスを MAC GDA 単位で割り当てることによって実装されます。

高速脱退処理をイネーブルにすると、ホストは送信元からこれ以上トラフィックを受信しない場合に特定のグループに対し BLOCK_OLD_SOURCES{src-list} メッセージを送信します。スイッチがホストからこのメッセージを受信すると、スイッチは特定グループのホストの送信元リストを解析します。この送信元リストが Leave メッセージで受信されたリストとまったく同じである場合、スイッチは LTL インデックスからホストを削除し、このマルチキャスト グループ トラフィックをホストへ転送するのを停止します。

送信元リストが一致しない場合、ホストがいずれの送信元からのトラフィック受信にも関与しなくなるまで、スイッチはホストを LTL インデックスから削除しません。

（注）　明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。

MLDv2 スヌーピング クエリアの概要

マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLDv2 を設定していない VLAN 内で MLDv2 スヌーピングをサポートするには、MLDv2 スヌーピング クエリアを使用します。

IP マルチキャスト ルーティングが設定されたネットワークでは、IP マルチキャスト ルータが MLDv2 クエリアとして機能します。VLAN の IP マルチキャスト トラフィックに、レイヤ 2 スイッチングのみを行う必要がある場合、IP マルチキャスト ルータは必要ではありません。ただし、VLAN 上に IP マルチキャスト ルータがない場合には、クエリーを送信できるよう他のスイッチを MLDv2 クエリアとして設定する必要があります。

MLDv2 スヌーピング クエリアがイネーブルの場合、MLDv2 スヌーピング クエリアは、IP マルチキャスト トラフィックの受信を希望するスイッチから、MLDv2 レポート メッセージを開始する MLDv2 クエリーを定期的に送信します。MLDv2 スヌーピングはこれらの MLDv2 レポートを待ち受けて、適切な転送を確立します。

MLDv2 スヌーピング クエリアは、VLAN 内のすべての Catalyst 6500 シリーズ スイッチでイネーブルにできます。ただし VLAN が、MLDv2 を使用して IP マルチキャスト トラフィックの情報をレポートするスイッチに接続されている場合は、VLAN ごとに 1 つ以上のスイッチを MLDv2 スヌーピング クエリアとして設定する必要があります。

IP マルチキャスト ルーティングがイネーブルであるかどうかにかかわらず、VLAN 上で MLDv2 クエリーを生成するようにスイッチを設定できます。

MLDv2 スヌーピングのデフォルト設定

表 29-3 に、MLDv2 スヌーピングのデフォルト設定を示します。

表 29-3　MLDv2 スヌーピングのデフォルト設定

機能	デフォルト値
MLDv2 スヌーピング クエリア	ディセーブル
MLDv2 スヌーピング	イネーブル
マルチキャスト ルータ	設定なし
MLDv2 レポート抑制	イネーブル
MLDv2 スヌーピング ルータ学習方式	PIM または MLDv2 パケットによって自動的に学習
高速脱退処理	イネーブル
MLDv2 の明示的なホスト トラッキング	イネーブル

MLDv2 スヌーピング設定時の注意事項および制約事項

MLDv2 スヌーピングを設定する際に、以下の注意事項と制約事項に従ってください。

- MLDv2 は、Internet Group Management Protocol version 3（IGMPv3）から派生したものです。MLDv2 プロトコル動作とステート移行、ホストとルータの動作、クエリーとレポート メッセージの処理、メッセージ転送ルール、タイマー動作は、IGMPv3 とまったく同じです。MLDv2 プロトコルの詳細については、draft-vida-mld-v2.02.txt を参照してください。
- MLDv2 プロトコル メッセージは、Internet Control Message Protocol version 6（ICMPv6）メッセージです。
- MLDv2 メッセージ形式は、IGMPv3 メッセージとほぼ同一です。
- Cisco IOS ソフトウェアの IPv6 マルチキャストは、MLD バージョン 2 を使用します。この MLD バージョンは、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 のみをサポートするホストは、MLD バージョン 2 を実行しているルータと相互運用します。MLD バージョン 1 と MLD バージョン 2 ホストの両方が混在する LAN はサポートされます。
- MLDv2 スヌーピングはプライベート VLAN をサポートします。プライベート VLAN は、MLDv2 スヌーピングに制約を課しません。
- MLDv2 スヌーピングは MAC マルチキャスト グループ 0100.5e00.0001 ～ 0100.5eff.ffff のトラフィックを抑制します。
- MLDv2 スヌーピングは、ルーティング プロトコルによって生成されたレイヤ 2 マルチキャストは抑制しません。

MLDv2 スヌーピング クエリア設定時の注意事項および制約事項

MLDv2 スヌーピング クエリアを設定する際に、以下の注意事項と制約事項に従ってください。

- グローバル コンフィギュレーション モードで VLAN を設定します（第 14 章「仮想 LAN（VLAN）の設定」を参照）。
- VLAN インターフェイスの IPv6 アドレスを設定します（第 22 章「レイヤ 3 インターフェイスの設定」を参照）。MLDv2 スヌーピング クエリアがイネーブルの場合、IPv6 アドレスをクエリー送信元アドレスとして使用します。
- VLAN インターフェイスに IPv6 アドレスが設定されていないと、MLDv2 スヌーピング クエリアは起動しません。MLDv2 スヌーピング クエリアは、IPv6 アドレスが消去されるとディセーブルになります。MLDv2 スヌーピング クエリアは、イネーブルの場合、IPv6 アドレスを設定すると再起動します。
- MLDv2 スヌーピング クエリアをイネーブルにすると、IPv6 マルチキャスト ルータからの MLDv2 トラフィックを検出しても起動しません。
- MLDv2 スヌーピング クエリアをイネーブルにすると、IPv6 マルチキャスト ルータから MLDv2 トラフィックが検出されない場合、60 秒後に起動します。
- MLDv2 スヌーピング クエリアをイネーブルにしても、IPv6 マルチキャスト ルータからの MLDv2 トラフィックを検出するとディセーブルになります。
- MLDv2 スヌーピングをイネーブルにすると、QoS は MLDv2 パケットをサポートしません。
- VLAN 内の Catalyst 6500 シリーズ スイッチは、MLDv2 スヌーピング クエリアをサポートする場合はすべてで、MLDv2 スヌーピング クエリアをイネーブルにできます。1 つのスイッチをクエリアとして選択します。

MLDv2 スヌーピング クエリアのイネーブル化

マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLDv2 を設定していない VLAN 内で MLDv2 スヌーピングをサポートするには、MLDv2 スヌーピング クエリアを使用します。

VLAN で MLDv2 スヌーピング クエリアをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 address prefix/prefix_length`	IPv6 アドレスおよび IPv6 サブネットを設定します。
ステップ 3	`Router(config-if)# ipv6 mld snooping querier` `Router(config-if)# no ipv6 mld snooping querier`	MLDv2 スヌーピング クエリアをイネーブルにします。 MLDv2 スヌーピング クエリアをディセーブルにします。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show ipv6 mld interface vlan vlan_ID | include querier`	設定を確認します。

次に、VLAN 200 で MLDv2 スヌーピング クエリアをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 200
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
Router(config-if)# ipv6 mld snooping querier
Router(config-if)# end
Router# show ipv6 mld interface vlan 200 | include querier
  MLD snooping fast-leave is enabled and querier is enabled
Router#
```

MLDv2 スヌーピングの設定

（注）　MLDv2 スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用にサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアをイネーブルにします（「MLDv2 スヌーピング クエリアのイネーブル化」（P.29-10）を参照）。

ここでは、MLDv2 スヌーピングを設定する手順について説明します。

- 「MLDv2 スヌーピングのイネーブル化」（P.29-11）
- 「マルチキャスト レシーバーへのスタティックな接続の設定」（P.29-12）
- 「高速脱退処理のイネーブル化」（P.29-13）
- 「明示的なホスト トラッキングの設定」（P.29-14）
- 「レポート抑制の設定」（P.29-15）
- 「MLDv2 スヌーピング情報の表示」（P.29-15）

（注）　グローバルにイネーブルにするコマンドを除き、すべての MLDv2 スヌーピング コマンドは VLAN インターフェイス上でのみサポートされます。

MLDv2 スヌーピングのイネーブル化

グローバルに MLDv2 スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ipv6 mld snooping`	MLDv2 スヌーピングをイネーブルにします。
	`Router(config)# no ipv6 mld snooping`	MLDv2 スヌーピングをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show ipv6 mld interface vlan vlan_ID | include globally`	設定を確認します。

次に、MLDv2 スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router(config)# ipv6 mld snooping
Router(config)# end
Router# show ipv6 mld interface vlan 200 | include globally
  MLD snooping is globally enabled
Router#
```

特定の VLAN で MLDv2 スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping`	MLDv2 スヌーピングをイネーブルにします。
	`Router(config-if)# no ipv6 mld snooping`	MLDv2 スヌーピングをディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show ipv6 mld interface vlan vlan_ID | include snooping`	設定を確認します。

次に、VLAN 25 で MLDv2 スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 25
Router(config-if)# ipv6 mld snooping
Router(config-if)# end
Router# show ipv6 mld interface vlan 25 | include snooping
  MLD snooping is globally enabled
  MLD snooping is enabled on this interface
  MLD snooping fast-leave is enabled and querier is enabled
  MLD snooping explicit-tracking is enabled
  MLD snooping last member query response interval is 1000 ms
  MLD snooping report-suppression is disabled
Router#
```

マルチキャスト レシーバーへのスタティックな接続の設定

マルチキャスト レシーバーへのスタティックな接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mac-address-table static** *mac_addr* **vlan** *vlan_id* **interface** *type*[1] *slot/port* [**disable-snooping**]	マルチキャスト レシーバーへのスタティックな接続を設定します。
	Router(config)# **no mac-address-table static** *mac_addr* **vlan** *vlan_id*	マルチキャスト レシーバーへのスタティックな接続を消去します。
ステップ 2	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mac-address-table address** *mac_addr*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

スタティックな接続を設定する場合、**disable-snooping** キーワードを入力することで、スタティックに設定されたマルチキャスト MAC アドレスにアドレス指定されたマルチキャスト トラフィックが、同じ VLAN 内の別のポートに送信されるのも防止できます。

次に、マルチキャスト レシーバーへのスタティックな接続を設定する例を示します。

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 interface fastethernet 5/7
```

マルチキャスト ルータ ポートのスタティックな設定

マルチキャスト ルータへのスタティックな接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface vlan** *vlan_ID*	VLAN インターフェイスを選択します。
ステップ 2	Router(config-if)# **ipv6 mld snooping mrouter interface** *type*[1] *slot/port*	マルチキャスト ルータへのスタティックな接続を設定します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show ipv6 mld snooping mrouter**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ルータへのインターフェイスは、コマンドを入力する VLAN に存在する必要があります。インターフェイスは管理上アップ状態で、回線プロトコルはアップ状態である必要があります。

次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

MLD スヌーピング クエリー時間の設定

特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリーを送信したあとで、スイッチが待機する時間を設定できます。

（注）　MLD スヌーピング高速脱退処理と MLD スヌーピング クエリー時間の両方を設定した場合は、高速脱退処理が優先されます。

スイッチによって送信される MLD スヌーピング クエリーの待機時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping last-member-query-interval interval`	スイッチによって送信される IGMP クエリーの待機時間を設定します。デフォルトは 1 秒です。有効な範囲は 1000 ～ 9990 ミリ秒です。
	`Router(config-if)# no ipv6 mld snooping last-member-query-interval`	デフォルト値に戻します。
ステップ 3	`Router# show ipv6 mld interface vlan vlan_ID | include last`	設定を確認します。

次に、MLD スヌーピング クエリー時間を設定する例を示します。

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 1000
Router(config-if)# exit
Router# show ipv6 mld interface vlan 200 | include last
  MLD snooping last member query response interval is 1000 ms
```

高速脱退処理のイネーブル化

VLAN 上で高速脱退処理をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping fast-leave`	VLAN 上で高速脱退処理をイネーブルにします。
	`Router(config-if)# no ipv6 mld snooping fast-leave`	VLAN 上で高速脱退処理をディセーブルにします。
ステップ 3	`Router# show ipv6 mld interface vlan vlan_ID | include fast-leave`	設定を確認します。

次に、VLAN 200 インターフェイスで高速脱退処理をイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 200
Router(config-if)# ipv6 mld snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ipv6 mld interface vlan 200 | include fast-leave
  MLD snooping fast-leave is enabled and querier is enabled
Router#
```

送信元固有マルチキャスト（SSM）セーフ レポート機能のイネーブル化

Source-Specific Multicast（SSM; 送信元固有マルチキャスト）セーフ レポート機能をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping ssm-safe-reporting`	SSM セーフ レポート機能をイネーブルにします。
	`Router(config-if)# no ipv6 mld snooping ssm-safe-reporting`	設定を消去します。

次に、SSM セーフ レポート機能を設定する例を示します。

```
Router(config)# interface vlan 10
Router(config-if)# ipv6 mld snooping ssm-safe-reporting
```

明示的なホスト トラッキングの設定

（注）　明示的なホスト トラッキングをディセーブルにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。

VLAN で明示的なホスト トラッキングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping explicit-tracking`	明示的なホスト トラッキングをイネーブルにします。
	`Router(config-if)# no ipv6 mld snooping explicit-tracking`	明示的なホスト トラッキング設定を消去します。
ステップ 3	`Router# show ipv6 mld snooping explicit-tracking vlan vlan_ID`	明示的なホスト トラッキングのステータスを表示します。

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config)# interface vlan 25
Router(config-if)# ipv6 mld snooping explicit-tracking
Router(config-if)# end
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
-------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

レポート抑制の設定

VLAN 上でレポート抑制をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ipv6 mld snooping report-suppression`	レポート抑制をイネーブルにします。
	`Router(config-if)# no ipv6 mld snooping report-suppression`	レポート抑制設定を消去します。
ステップ 3	`Router# show ipv6 mld interface vlan_ID | include report-suppression`	レポート抑制のステータスを表示します。

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config)# interface vlan 25
Router(config-if)# ipv6 mld snooping report-suppression
Router(config-if)# end
Router# Router# show ipv6 mld interface vlan 25 | include report-suppression
  MLD snooping report-suppression is enabled
```

MLDv2 スヌーピング情報の表示

ここでは、MLDv2 スヌーピング情報の表示について説明します。

- 「マルチキャスト ルータ インターフェイスの表示」（P.29-15）
- 「MAC アドレス マルチキャスト エントリの表示」（P.29-16）
- 「VLAN インターフェイス用の MLDv2 スヌーピング情報の表示」（P.29-16）

マルチキャスト ルータ インターフェイスの表示

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。

マルチキャスト ルータ インターフェイスを表示するには、次の作業を行います。

コマンド	目的
`Router# show ipv6 mld snooping mrouter vlan_ID`	マルチキャスト ルータ インターフェイスを表示します。

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

MAC アドレス マルチキャスト エントリの表示

VLAN の MAC アドレス マルチキャスト エントリを表示するには、次の作業を行います。

コマンド	目的
Router# **show mac-address-table multicast** *vlan_ID* [**count**]	VLAN の MAC アドレス マルチキャスト エントリを表示します。

次に、VLAN 1 の MAC アドレス マルチキャスト エントリを表示する例を示します。

```
Router# show mac-address-table multicast vlan 1
vlan   mac address     type    qos             ports
-----+---------------+--------+---+--------------------------------
  1   0100.5e02.0203  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0127  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0128  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0001  static   --  Gi1/1,Gi2/1,Fa3/48,Router,Switch
Router#
```

次に、ある VLAN について MAC アドレス エントリの総数を表示する例を示します。

```
Router# show mac-address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

VLAN インターフェイス用の MLDv2 スヌーピング情報の表示

VLAN インターフェイスの MLDv2 スヌーピング情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ipv6 mld snooping** {{**explicit-tracking** *vlan_ID*}| {**mrouter** [**vlan** *vlan_ID*]} | {**report-suppression vlan** *vlan_ID*} | {**statistics vlan** *vlan_ID*}	VLAN インターフェイスの MLDv2 スヌーピング情報を表示します。

次に、VLAN 25 の明示的なトラッキング情報を表示する例を示します。

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
--------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

次に、VLAN 25 の IGMP スヌーピング統計情報の例を示します。

```
Router# show ipv6 mld snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
```

CHAPTER 30

IPv4 マルチキャスト トラフィック用インターネット グループ管理プロトコル（IGMP）スヌーピングの設定

この章では、Catalyst 6500 シリーズ スイッチに IPv4 マルチキャスト トラフィック用 Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングを設定する手順について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- IPv6 マルチキャスト トラフィックを抑制するには、第 29 章「IPv6 マルチキャスト トラフィック用の Multcast Listener Discovery version 2（MLDv2）スヌーピングの設定」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。

IGMP スヌーピングの機能概要

ここでは、IGMP スヌーピングについて説明します。

IGMP スヌーピングの概要

IGMP または IGMP スヌーピング クエリアからの IGMP クエリーを受信するサブネットで、IGMP スヌーピングを使用するように、スイッチを設定できます。IGMP スヌーピングは、IPv4 マルチキャスト トラフィックを受信するポートだけにそのトラフィックを転送するように、レイヤ 2 LAN ポートをダイナミックに設定することにより、レイヤ 2 で IPv4 マルチキャスト トラフィックを抑制します。

IGMP は、マルチキャスト ルータのレイヤ 3 で稼動し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 IGMP クエリーを生成します。IGMP の詳細については、第 28 章「IPv4 マルチキャスト レイヤ 3 スイッチングの設定」を参照してください。

IGMP スヌーピング クエリアをスイッチに設定して、マルチキャスト ルータ インターフェイスがないサブネットにおいて IGMP スヌーピングをサポートできます。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアのイネーブル化」（P.30-10）を参照してください。

IGMP（マルチキャスト ルータ上）または IGMP スヌーピング クエリア（スーパーバイザ エンジン上）は、スイッチが Virtual LAN（VLAN; 仮想 LAN）のすべてのポートを通じて、ホストの応答先となる、一般的な IGMP クエリーを定期的に送信します。IGMP スヌーピングはレイヤ 3 IGMP トラフィックをモニタします。

（注）　マルチキャスト グループで、VLAN 中に送信元のみがありレシーバーがない場合は、IGMP スヌーピングはマルチキャスト トラフィックをマルチキャスト ルータ ポート宛てのみに抑制します。

マルチキャスト グループへの加入

ホストは、マルチキャスト ルータからの一般的なクエリーに応じて、非送信請求 IGMP Join メッセージを送信するか、または IGMP Join メッセージを送信して、マルチキャスト グループに参加します（スイッチは、一般的なクエリーを、マルチキャスト ルータから VLAN 中のすべてのポートに転送します）。

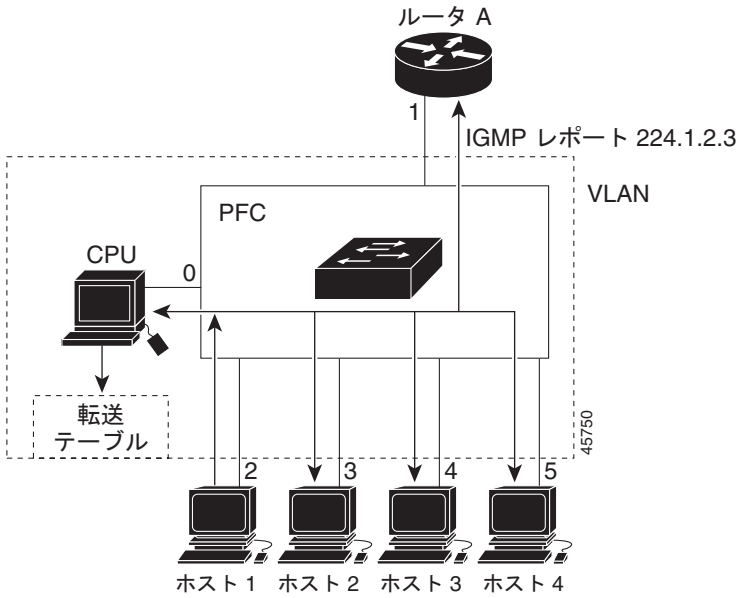
IGMP Join 要求に応じて、スイッチは、Join 要求を受信した VLAN のレイヤ 2 転送テーブルにエントリを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが IGMP Join 要求を送る場合、スイッチは、既存のレイヤ 2 転送テーブル エントリにそれを追加します。スイッチは、IGMP Join 要求を受信する各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリのみを生成します。

IGMP スヌーピングは、マルチキャスト グループごとに 1 つを残して他のすべてのホスト Join メッセージを抑制し、この 1 つの Join メッセージだけをマルチキャスト ルータに転送します。

スイッチは、Join メッセージで指定されたマルチキャスト グループ用のマルチキャスト トラフィックを、Join メッセージを受信したインターフェイスに転送します（図 30-1 を参照）。

IGMP スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、**mac-address-table static** コマンドを使用して、レイヤ 2 マルチキャスト グループ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 アドレスのグループ メンバシップをスタティックに指定した場合、そのスタティックな設定は、IGMP スヌーピングの学習よりも優先されます。マルチキャスト グループ メンバシップのリストは、スタティックな設定値と、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。

図 30-1　最初の IGMP Join メッセージ



マルチキャスト ルータ A が一般的なクエリーをスイッチに送信し、スイッチがそのクエリーを、同じ VLAN の全メンバのポート 2 ～ 5 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 に加入する意思があり、IGMP メンバシップ レポート（IGMP Join メッセージ）を 0x0100.5E01.0203 と同じ Media Access Control（MAC; メディア アクセス制御）宛先アドレスを持つグループにマルチキャストします。CPU が、ホスト 1 による IGMP レポート マルチキャストを受信すると、CPU は IGMP レポート内の情報を利用して、表 30-1 に示すように転送テーブル エントリを設定します。これには、ホスト 1 のポート番号、マルチキャスト ルータ、スイッチの内部 CPU が含まれます。

表 30-1　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
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2

スイッチ ハードウェアは、IGMP 情報パケットを、マルチキャスト グループ用の他のパケットと区別できます。テーブル中の最初のエントリは、スイッチング エンジンに対して、IGMP パケットのみを CPU に送信するように指示します。これによって、CPU がマルチキャスト フレームで過負荷になるのを防止できます。2 番目のエントリは、スイッチング エンジンに、0x0100.5E01.0203 マルチキャスト MAC アドレス宛てのフレームを送信するように指示します。このフレームは、マルチキャスト ルータ宛て、およびグループに参加しているホスト宛ての IGPM パケットではありません（!IGMP）。

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送る場合（図 30-2 を参照）、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します（表 30-2 を参照）。転送テーブルは CPU 宛てにのみ IGMP メッセージを送るので、メッセージは他のポートへフラッディングされません。認識されているマルチキャスト トラフィックは、CPU 宛てではなくグループ宛てに転送されます。

図 30-2　　2 番目のホストのマルチキャスト グループへの加入

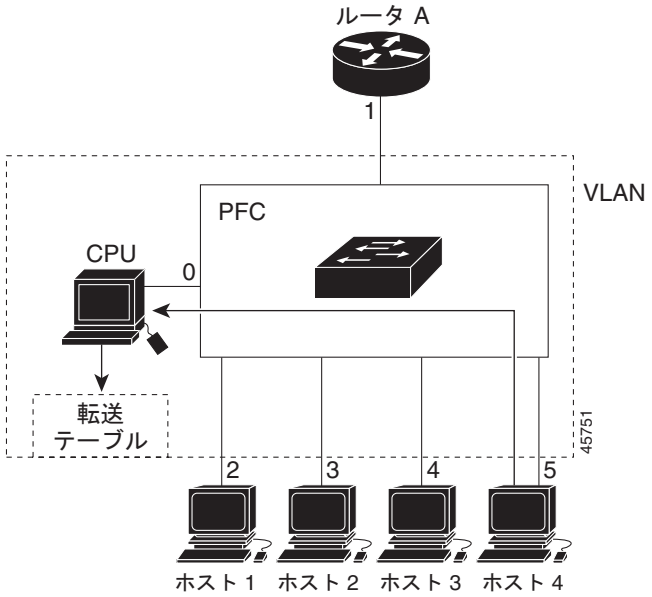


表 30-2　　更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2, 5

マルチキャスト グループからの脱退

ここでは、マルチキャスト グループからの脱退について説明します。

通常の脱退処理

関係するホストは、一般的 IGMP クエリーに定期的に応答を続ける必要があります。VLAN 中の少なくとも 1 つのホストが一般的 IGMP クエリーに定期的に応答している限り、マルチキャスト ルータは引き続きマルチキャスト トラフィックを VLAN に転送します。ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な一般的 IGMP クエリーを無視するか（「暗黙的脱退」といいます）、またはグループ固有の IGMPv2 Leave メッセージを送信します。

IGMP スヌーピングがグループ固有の IGMPv2 Leave メッセージをホストから受信すると、MAC ベースの一般的なクエリーを送信して、そのインターフェイスに接続されている他の装置がその特定のマルチキャスト グループに対するトラフィックに関係があるかどうかを判断します。IGMP スヌーピングが、この一般的クエリーに対して IGMP Join メッセージを受信しなかった場合、インターフェイスに接続されている他の装置の中に、このマルチキャスト グループのトラフィックの受信に関与している装置はないと見なし、マルチキャスト グループに対応するレイヤ 2 転送テーブル エントリからそのインターフェイスを削除します。残りのインターフェイスのうち、グループに関係するホストのインターフェイスからのみ Leave メッセージが送信され、一般的なクエリーに応答する IGMP Join メッセージを IGMP スヌーピングが受信しない場合、IGMP スヌーピングはグループ エントリを削除して、IGMP 脱退をマルチキャスト ルータにリレーします。マルチキャスト ルータが VLAN からレポートを受信しない場合、マルチキャスト ルータは IGMP キャッシュからその VLAN 用のグループを削除します。

テーブル エントリを更新するまでスイッチが待機する時間を、「最終メンバ クエリー時間」と呼びます。この時間を設定するには、**ip igmp snooping last-member-query-interval** *interval* コマンドを入力します。

高速脱退処理

IGMP スヌーピングの高速脱退処理を使用すると、IGMP スヌーピングは、レイヤ 2 LAN インターフェイスに IGMP グループ固有のクエリーを送信せずに、転送テーブル エントリからそのインターフェイスを削除します。グループ固有の IGMPv2 Leave メッセージを受信すると、IGMP スヌーピングはすぐに、そのマルチキャスト グループ用のレイヤ 2 転送テーブル エントリからインターフェイスを削除します（ポート上でマルチキャスト ルータが学習された場合は除きます）。高速脱退処理により、スイッチド ネットワーク上のすべてのホストの帯域幅管理が強化されます。

（注）　高速脱退処理は、各レイヤ 2 LAN ポートに 1 つのホストしか接続されていない VLAN に限って使用してください。レイヤ 2 LAN ポートに複数のホストが接続されている VLAN 上で高速脱退をイネーブルにすると、一部のホストが偶発的に廃棄される可能性があります。高速脱退処理は、IGMP バージョン 2 のホストについてのみサポートされます。

IGMP スヌーピング クエリアの概要

マルチキャスト トラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。

IP マルチキャスト ルーティングが設定されたネットワークでは、IP マルチキャスト ルータが IGMP クエリアとして機能します。VLAN 内のみの IP マルチキャスト トラフィックに、レイヤ 2 スイッチングを行う必要がある場合、IP マルチキャスト ルータは必要ではありません。ただし、VLAN 上に IP マルチキャスト ルータがない場合には、クエリーを送信できるよう他のスイッチを IGMP クエリアとして設定する必要があります。

IGMP スヌーピング クエリアがイネーブルの場合、IGMP スヌーピング クエリアは、IP マルチキャスト トラフィックを受信したいスイッチから IGMP レポート メッセージを開始する IGMP クエリーを定期的に送信します。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP を使用して IP マルチキャスト トラフィックの情報をレポートするスイッチ上でサポートされる各 VLAN の IGMP スヌーピング クエリアとして、スイッチを 1 つ設定します。

（注）　VLAN 内の 1 つのスイッチでのみ IGMP スヌーピング クエリアをイネーブルにします。

IP マルチキャスト ルーティングがイネーブルであるかどうかにかかわらず、VLAN 上で IGMP クエリーを生成するようにスイッチを設定できます。

IGMP バージョン 3 サポートの概要

ここでは、IGMP バージョン 3 のサポートについて説明します。

IGMP バージョン 3 サポートの概要

IGMP スヌーピングは、IGMP バージョン 3 をサポートします。IGMP バージョン 3 は送信元ベースのフィルタリングを使用します。これによりホストおよびルータは、特定のマルチキャスト グループで許可またはブロックされる送信元アドレスを特定できます。Catalyst 6500 シリーズ スイッチで IGMP バージョン 3 スヌーピングをイネーブルにした場合、システムは特定の VLAN の特定のグループ用に受信したメッセージに基づいて IGMP バージョン 3 ステートを維持し、このメッセージの次の情報に基づいてトラフィックを許可またはブロックします。

- 送信元リスト
- 許可（include）またはブロック（exclude）フィルタリング オプション

レイヤ 2 テーブルが（MAC グループ、VLAN）ベースのため、IGMPv3 のホストを使用する場合、マルチキャストの送信元は、各 MAC グループごとに 1 つだけ設定することを推奨します。

（注）　IGMP バージョン 3 レポート用の送信元ベースのフィルタリングは、ハードウェアではサポートされません。このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。送信元のみのエントリは、常に有効な状態に保つために、5 分ごとに削除されて再学習されます。

IGMPv3 高速脱退処理

IGMP バージョン 3 高速脱退処理は、デフォルトでイネーブルに設定されています。IGMP バージョン 3 高速脱退処理をディセーブルにするには、明示的なホスト トラッキングをオフにします。

IGMPv3 での高速脱退処理は、ソフトウェアの送信元グループ ベースのメンバシップ情報を維持し、LTL インデックスを MAC GDA 単位で割り当てることによって実装されます。

高速脱退処理をイネーブルにすると、ホストは送信元からこれ以上トラフィックを受信しない場合に特定のグループに対し BLOCK_OLD_SOURCES{src-list} メッセージを送信します。スイッチがホストからこのメッセージを受信すると、スイッチは特定グループのホストの送信元リストを解析します。この送信元リストが Leave メッセージで受信されたリストとまったく同じである場合、スイッチは LTL インデックスからホストを削除し、このマルチキャスト グループ トラフィックをホストへ転送するのを停止します。

送信元リストが一致しない場合、ホストがいずれの送信元からのトラフィック受信にも関与しなくなるまで、スイッチはホストを LTL インデックスから削除しません。

プロキシ レポート機能

IGMP では、IGMPv1 および IGMPv2 メッセージのプロキシ レポートをサポートして、グループ固有のクエリーを処理します。これらのクエリーはダウンストリームには送信されませんが、スイッチは直接クエリーに応答します。スイッチは、受信したグループ固有のクエリーを終了させ、グループにレシーバーがある場合は、IGMP プロキシ レポートを送信します。IGMPv3 メッセージにはプロキシ レポートがありません。IGMPv3 の場合、グループ固有のクエリーまたはグループの送信元固有のクエリーは、すべての VLAN メンバ ポートでフラッディングします。IGMPv3 メンバシップ レポートのデータベースは、受信されるレポートに基づいて構築されます。

特定のクエリーに応答するホスト レポートは、レポート抑制機能により抑制できます。レポート抑制は、IGMPv1、IGMPv2、IGMPv3 メッセージに関してサポートされています。レポート抑制がイネーブルである場合（デフォルト）、スイッチは一般的なクエリーを受信すると、すべてのホストから各グループまたはチャネル（S,G）へとレポートの抑制サイクルを開始します。検出されたマルチキャスト ルータへの最初のレポートのみが転送されます。これ以外のレポートは、抑制されます。IGMPv1 および IGMPv2 の場合、抑制時間は一般的なクエリー メッセージで示されるレポート応答時間です。IGMPv3 の場合は、一般的なクエリー時間全体で抑制が行われます。

（注）
- IGMP バージョン 3 レポート用の送信元ベースのフィルタリングは、ハードウェアではサポートされません。このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。送信元のみのエントリは、常に有効な状態に保つために、5 分ごとに削除されて再学習されます。
- 明示的なホスト トラッキングをオフにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。

明示的なホスト トラッキング

IGMPv3 では、ポート上のメンバシップ情報の明示的なホスト トラッキングをサポートします。明示的なトラッキング データベースは、IGMPv3 ホストの高速脱退処理、プロキシ レポート機能、統計情報収集に使用されます。VLAN で明示的なトラッキングがイネーブルの場合、IGMP スヌーピング ソフトウェアはホストから受信する IGMPv3 通知を処理し、次の情報を含む明示的なトラッキング データベースを作成します。

- ホストに接続されたポート
- ホストによって通知されたチャネル
- ホストによって通知された各グループのフィルタ モード
- ホストによって通知された各グループの送信元リスト
- 各グループのルータ フィルタ モード
- 送信元を要求するグループごとのホスト リスト

（注）

- 明示的なホスト トラッキングをオフにすると、高速脱退処理およびプロキシ レポート機能がディセーブルになります。
- 明示的なホスト トラッキングがイネーブルでスイッチが proxy-reporting モードで動作している場合、ルータは VLAN インターフェイスの下位にあるホストのすべてをトラッキングできない場合があります。

IGMP スヌーピングのデフォルト設定

表 30-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 30-3　IGMP スヌーピングのデフォルト設定

機能	デフォルト値
IGMP スヌーピング クエリア	ディセーブル
IGMP スヌーピング	イネーブル
マルチキャスト ルータ	設定なし
IGMPv3 プロキシ レポート機能	イネーブル
IGMP スヌーピング ルータの学習方式	PIM または IGMP パケットによって自動的に学習
高速脱退処理	ディセーブル
IGMPv3 明示的ホスト トラッキング	イネーブル
IGMPv3 Source-Specific Multicast（SSM; 送信元固有マルチキャスト）セーフ レポート機能	ディセーブル。Release 12.2(18)SXE 以降のリリースでは推奨しません。

IGMP スヌーピング設定時の注意事項および制約事項

IGMP スヌーピングを設定する際に、以下の注意事項と制約事項に従ってください。

- Cisco Group Management Protocol（CGMP）クライアント装置をサポートするには、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を CGMP サーバとして設定します。次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』Release 12.2 の「IP Multicast」、「Configuring IP Multicast Routing」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfmulti.htm

- 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。
- IGMP スヌーピングは、プライベート VLAN をサポートします。プライベート VLAN は、IGMP スヌーピングに制約を課しません。
- IGMP スヌーピングは MAC マルチキャスト グループ 0100.5e00.0001 ～ 0100.5eff.ffff のトラフィックを抑制します。
- IGMP スヌーピングは、ルーティング プロトコルによって生成されたレイヤ 2 マルチキャストは抑制しません。

IGMP スヌーピング クエリア設定時の注意事項および制約事項

IGMP スヌーピング クエリアを設定する際に、以下の注意事項と制約事項に従ってください。

- IGMP スヌーピング クエリアはクエリア選択をサポートしません。VLAN 内の 1 つのスイッチでのみ IGMP スヌーピング クエリアをイネーブルにします （CSCsk48795）。
- グローバル コンフィギュレーション モードで VLAN を設定します（第 14 章「仮想 LAN（VLAN）の設定」を参照）。
- VLAN インターフェイスの IP アドレスを設定してください（第 22 章「レイヤ 3 インターフェイスの設定」を参照）。IGMP クエリアをイネーブルにすると、IGMP スヌーピング クエリアはこの IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイスに IP アドレスが設定されていないと、IGMP スヌーピング クエリアは起動しません。IP アドレスが消去されると、IGMP スヌーピング クエリアは自身をディセーブルにします。IGMP スヌーピング クエリアをイネーブルにした場合、IP アドレスが設定されていれば、IGMP スヌーピング クエリアが再起動します。
- IGMP スヌーピング クエリアは、IGMP バージョン 2 をサポートします。
- IGMP スヌーピング クエリアをイネーブルにしても、IGMP スヌーピング クエリアがマルチキャスト ルータからの IGMP トラフィックを検出すると、IGMP スヌーピング クエリアは起動しません。
- IGMP スヌーピング クエリアをイネーブルにすると、マルチキャスト ルータから IGMP トラフィックが検出されなければ、IGMP スヌーピング クエリアは 60 秒後に起動します。
- IGMP スヌーピング クエリアをイネーブルにしても、マルチキャスト ルータからの IGMP トラフィックが検出されると、IGMP スヌーピング クエリアは自らをディセーブルにします。
- IGMP スヌーピングがイネーブルの場合、Quality of Service（QoS; サービス品質）は IGMP パケットをサポートしません。

（注）　コンフィギュレーション モードで EXEC モード レベルのコマンドを入力するには、コマンドの前に **do** キーワードを入力します。

IGMP スヌーピング クエリアのイネーブル化

マルチキャスト トラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。

VLAN で IGMP スヌーピング クエリアをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip address ip_address subnet_mask`	IP アドレスおよび IP サブネットを設定します。
ステップ 3	`Router(config-if)# ip igmp snooping querier` `Router(config-if)# no ip igmp snooping querier`	IGMP スヌーピング クエリアをイネーブルにします。 IGMP スヌーピング クエリアをディセーブルにします。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show ip igmp interface vlan vlan_ID | include querier`	設定を確認します。

次に、VLAN 200 で IGMP スヌーピング クエリアをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 200
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include querier
IGMP snooping fast-leave (for v2) is disabled and querier is enabled
Router#
```

IGMP スヌーピングの設定

（注）　IGMP スヌーピングを使用するには、マルチキャスト ルーティングできるようにサブネットでレイヤ 3 インターフェイスを設定するか（第 28 章「IPv4 マルチキャスト レイヤ 3 スイッチングの設定」を参照）、またはサブネットで IGMP スヌーピング クエリアをイネーブルにします（「IGMP スヌーピング クエリアのイネーブル化」（P.30-10）を参照）。

IGMP スヌーピングにより、Catalyst 6500 シリーズ スイッチで IGMP パケットを調べ、パケットの内容に基づいて転送先を決定できます。

ここでは、IGMP スヌーピングを設定する手順について説明します。

- 「IGMP スヌーピングのイネーブル化」（P.30-11）
- 「マルチキャスト レシーバーへのスタティックな接続の設定」（P.30-12）
- 「マルチキャスト ルータ ポートのスタティックな設定」（P.30-13）
- 「IGMP スヌーピング クエリー時間の設定」（P.30-13）
- 「IGMP 高速脱退処理のイネーブル化」（P.30-14）
- 「送信元固有マルチキャスト（SSM）マッピングの設定」（P.30-14）
- 「SSM セーフ レポート機能のイネーブル化」（P.30-15）
- 「IGMPv3 明示的なホスト トラッキングの設定」（P.30-15）
- 「IGMP スヌーピング情報の表示」（P.30-16）

（注）　グローバルにイネーブルにするコマンドを除き、すべての IGMP スヌーピング コマンドは VLAN インターフェイス上でのみサポートされます。

IGMP スヌーピングのイネーブル化

IGMP スヌーピングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip igmp snooping`	IGMP スヌーピングをイネーブルにします。
	`Router(config)# no ip igmp snooping`	IGMP スヌーピングをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show ip igmp interface vlan vlan_ID | include globally`	設定を確認します。

次に、IGMP スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
  IGMP snooping is globally enabled
Router#
```

特定の VLAN で IGMP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip igmp snooping`	IGMP スヌーピングをイネーブルにします。
	`Router(config-if)# no ip igmp snooping`	IGMP スヌーピングをディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show ip igmp interface vlan vlan_ID | include snooping`	設定を確認します。

次に、VLAN 25 で IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 25
Router(config-if)# ip igmp snooping
Router(config-if)# end
Router# show ip igmp interface vl25 | include snooping
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

マルチキャスト レシーバーへのスタティックな接続の設定

マルチキャスト レシーバーへのスタティックな接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mac-address-table static mac_addr vlan vlan_id interface type[1] slot/port [disable-snooping]`	マルチキャスト レシーバーへのスタティックな接続を設定します。
	`Router(config)# no mac-address-table static mac_addr vlan vlan_id`	マルチキャスト レシーバーへのスタティックな接続を消去します。
ステップ 2	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mac-address-table address mac_addr`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

スタティックな接続を設定する場合、**disable-snooping** キーワードを入力することで、スタティックに設定されたマルチキャスト MAC アドレスにアドレス指定されたマルチキャスト トラフィックが、同じ VLAN 内の別のポートに送信されるのも防止できます。

次に、マルチキャスト レシーバーへのスタティックな接続を設定する例を示します。

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 interface fastethernet 5/7
```

マルチキャスト ルータ ポートのスタティックな設定

マルチキャスト ルータへのスタティックな接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# ip igmp snooping mrouter interface` *type*[1] *slot/port*	マルチキャスト ルータへのスタティックな接続を設定します。
ステップ 2	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show ip igmp snooping mrouter`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ルータへのインターフェイスは、コマンドを入力する VLAN に存在する必要があります。インターフェイスは管理上アップ状態で、回線プロトコルはアップ状態である必要があります。

次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

IGMP スヌーピング クエリー時間の設定

特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリーを送信したあとで、スイッチが待機する時間を設定できます。

（注） IGMP 高速脱退処理と IGMP クエリー時間の両方を設定した場合は、高速脱退処理が優先されます。

スイッチによって送信される IGMP スヌーピング クエリー時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan` *vlan_ID*	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip igmp snooping last-member-query-interval` *interval*	スイッチによって送信される IGMP スヌーピング クエリー時間を設定します。デフォルトは 1 秒です。有効な範囲は 100 ～ 999 ミリ秒です。
	`Router(config-if)# no ip igmp snooping last`	デフォルト値に戻します。

次に、IGMP スヌーピング クエリー時間を設定する例を示します。

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include last
  IGMP snooping last member query interval on this interface is 200 ms
```

IGMP 高速脱退処理のイネーブル化

特定の VLAN 上で IGMP 高速脱退処理をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip igmp snooping fast-leave`	VLAN 上で IGMP 高速脱退処理をイネーブルにします。
	`Router(config-if)# no ip igmp snooping fast-leave`	VLAN 上で IGMP 高速脱退処理をディセーブルにします。

次に、VLAN 200 インターフェイスで IGMP 高速脱退処理をイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 200
Router(config-if)# ip igmp snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include fast-leave
IGMP snooping fast-leave is enabled on this interface
Router(config-if)#
```

送信元固有マルチキャスト（SSM）マッピングの設定

（注）
- Release 12.2(18)SXD3 以降のリリースで、SSM マッピングがサポートされます。
- IGMPv3 マルチキャスト レシーバーをサポートする VLAN では、SSM マッピングを設定しないでください。

SSM マッピングを設定するには、次のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm

SSM セーフ レポート機能のイネーブル化

（注）　送信元固有マルチキャスト（SSM）セーフ レポート機能は、Release 12.2(18)SXE 以降のリリースでは推奨しません。

SSM セーフ レポート機能を設定すると、IGMPv1 および IGMPv2 ホストが存在する場合でも、グループ モードは IGMPv3 です。

スイッチが同じ VLAN の IGMPv1、IGMPv2、IGMPv3 ホストを確実にサポートできるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip igmp snooping ssm-safe-reporting`	IGMPv2 および IGMPv3 ホスト両方のサポートをイネーブルにします。
	`Router(config-if)# no ip igmp snooping ssm-safe-reporting`	設定を消去します。

次に、IGMPv2 および IGMPv3 ホスト両方をサポートするように、スイッチを設定する例を示します。

```
Router(config)# interface vlan 10
Router(config-if)# ip igmp snooping ssm-safe-reporting
```

IGMPv3 明示的なホスト トラッキングの設定

VLAN で明示的なホスト トラッキングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan vlan_ID`	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip igmp snooping explicit-tracking`	明示的なホスト トラッキングをイネーブルにします。
	`Router(config-if)# no ip igmp snooping explicit-tracking`	明示的なホスト トラッキング設定を消去します。
ステップ 3	`Router# show ip igmp snooping explicit-tracking {vlan vlan-id}`	IGMPv3 ホストの明示的なホスト トラッキング ステータスに関する情報を表示します。

次に、明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config)# interface vlan 25
Router(config-if)# ip igmp snooping explicit-tracking
Router(config-if)# end
Router# show ip igmp snooping explicit-tracking vlan 25

Source/Group                    Interface    Reporter        Filter_mode
--------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     16.27.2.3       INCLUDE
```

IGMP スヌーピング情報の表示

ここでは、IGMP スヌーピング情報の表示方法について説明します。

マルチキャスト ルータ インターフェイスの表示

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。

マルチキャスト ルータ インターフェイスを表示するには、次の作業を行います。

コマンド	目的
Router# **show ip igmp snooping mrouter** *vlan_ID*	マルチキャスト ルータ インターフェイスを表示します。

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show ip igmp snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

MAC アドレス マルチキャスト エントリの表示

VLAN の MAC アドレス マルチキャスト エントリを表示するには、次の作業を行います。

コマンド	目的
Router# **show mac-address-table multicast** *vlan_ID* [**count**]	VLAN の MAC アドレス マルチキャスト エントリを表示します。

次に、VLAN 1 の MAC アドレス マルチキャスト エントリを表示する例を示します。

```
Router# show mac-address-table multicast vlan 1
vlan   mac address     type    qos             ports
-----+---------------+--------+---+--------------------------------
  1   0100.5e02.0203  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0127  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0128  static   --  Gi1/1,Gi2/1,Fa3/48,Router
  1   0100.5e00.0001  static   --  Gi1/1,Gi2/1,Fa3/48,Router,Switch
Router#
```

次に、ある VLAN について MAC アドレス エントリの総数を表示する例を示します。

```
Router# show mac-address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#
```

VLAN インターフェイスの IGMP スヌーピング情報の表示

特定の VLAN インターフェイスについて IGMP スヌーピング情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ip igmp interface** *vlan_ID*	特定の VLAN インターフェイス上の IGMP スヌーピング情報を表示します。

次に、VLAN 200 インターフェイスの IGMP スヌーピング情報を表示する例を示します。

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
  Internet address is 43.0.0.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 43.0.0.1 (this system)
  IGMP querying router is 43.0.0.1 (this system)
  Multicast groups joined by this system (number of users):
      224.0.1.40(1)
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

IGMP スヌーピング統計情報の表示

show ip igmp snooping statistics interface *vlan_ID* コマンドを入力すると、次の情報が表示されます。

- グループのメンバであるポート リスト
- フィルタ モード
- ポートの下位のレポータのアドレス
- **clear ip igmp snooping statistics** コマンドの前回入力後に収集された最終加入および最終脱退情報

IGMP スヌーピング統計情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ip igmp snooping statistics interface** *vlan_ID*	特定の VLAN インターフェイス上の IGMP スヌーピング情報を表示します。

次に、インターフェイス VLAN 25 の IGMP スヌーピング統計情報の例を示します。

```
Router# show ip igmp snooping statistics interface vlan 25

Snooping statistics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      16.27.2.3     00:01:47      00:00:50      -
Router#
```

CHAPTER 31

Protocol Independent Multicast（PIM）スヌーピングの設定

この章では、Catalyst 6500 シリーズ スイッチに Protocol Independent Multicast（PIM）スヌーピングを設定する手順について説明します。Release 12.2(17a)SX 以降のリリースで、PIM スヌーピングがサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

PIM スヌーピングの機能概要

レイヤ 2 スイッチが複数のルータと相互接続しているネットワーク（Internet Exchange Point（IXP）など）では、マルチキャスト レシーバー ダウンストリームがない場合でもデフォルトでは、スイッチはすべてのマルチキャスト ルータ ポート上で IP マルチキャスト パケットをフラッディングします。PIM スヌーピングがイネーブルの場合、スイッチは各 IP マルチキャスト グループのマルチキャスト パケットを、グループに加入しているダウンストリーム レシーバーがあるマルチキャスト ルータ ポートのみに制限します。PIM スヌーピングがイネーブルの場合、スイッチは PIM Hello メッセージ、PIM Join およびプルーニング メッセージ、双方向 PIM designated forwarder-election メッセージを待ち受けることにより、特定の Virtual LAN（VLAN; 仮想 LAN）内のマルチキャスト トラフィックを受信する必要があるマルチキャスト ルータ ポートを学習します。

（注）　PIM スヌーピングを使用するには、Catalyst 6500 シリーズ スイッチ上で Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングをイネーブルにする必要があります。IGMP スヌーピングは、ホストが接続されている LAN ポートからのマルチキャスト トラフィックの送信を制限します。IGMP スヌーピングは、1 つまたは複数のマルチキャスト ルータが接続されている LAN ポートからのトラフィックは制限しません。

次の図では、PIM スヌーピングがイネーブルでないネットワークによるトラフィックおよびフラッディング フローと、PIM スヌーピングがイネーブルのときのトラフィック フローおよびトラフィック制限を示します。

図 31-1 では、PIM スヌーピングがイネーブルでない場合の PIM Join メッセージのフローを示します。この図では、スイッチはルータ B を対象とした PIM Join メッセージを、接続されたすべてのルータにフラッディングします。

図 31-1　PIM スヌーピングがない場合の PIM Join メッセージ フロー

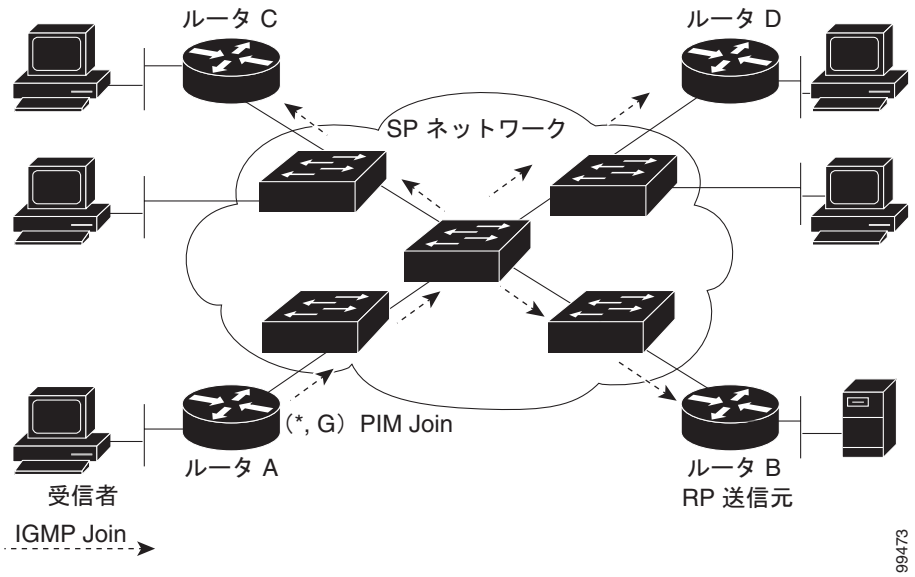


図 31-2 では、PIM スヌーピングがイネーブルの場合の PIM Join メッセージ フローを示します。この図では、スイッチは PIM Join メッセージを制限し、このメッセージを受信する必要があるルータ（ルータ B）にのみ転送します。

図 31-2　PIM スヌーピングがある場合の PIM Join メッセージ フロー

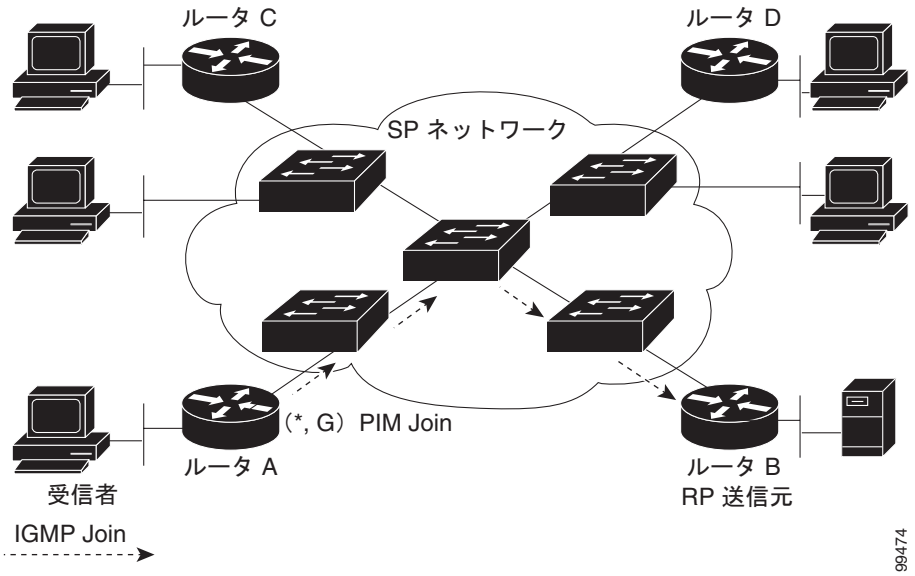


図 31-3 では、PIM スヌーピングがイネーブルでない場合のデータ トラフィック フローを示します。この図では、スイッチはルータ A を対象としたデータ トラフィックを接続されたすべてのルータにフラッディングします。

図 31-3　PIM スヌーピングがない場合のデータ トラフィック フロー

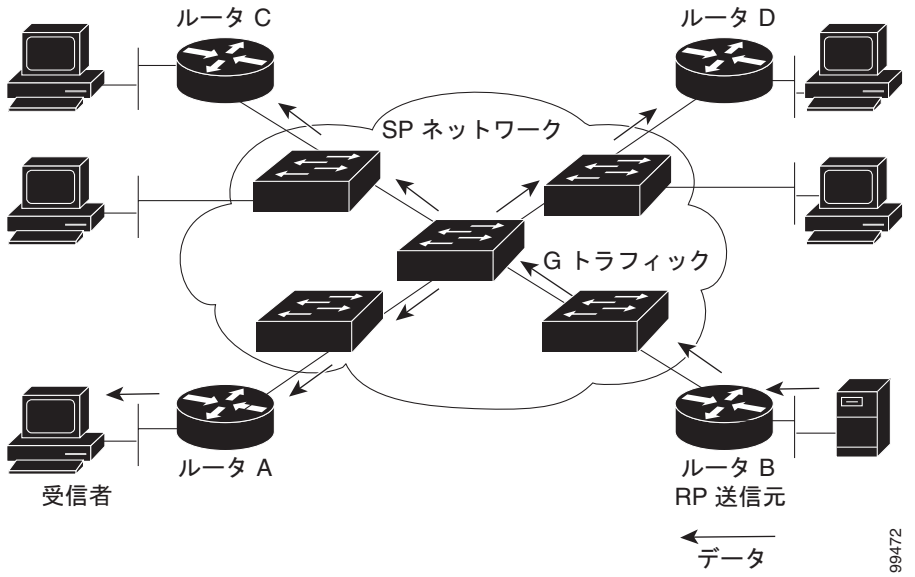
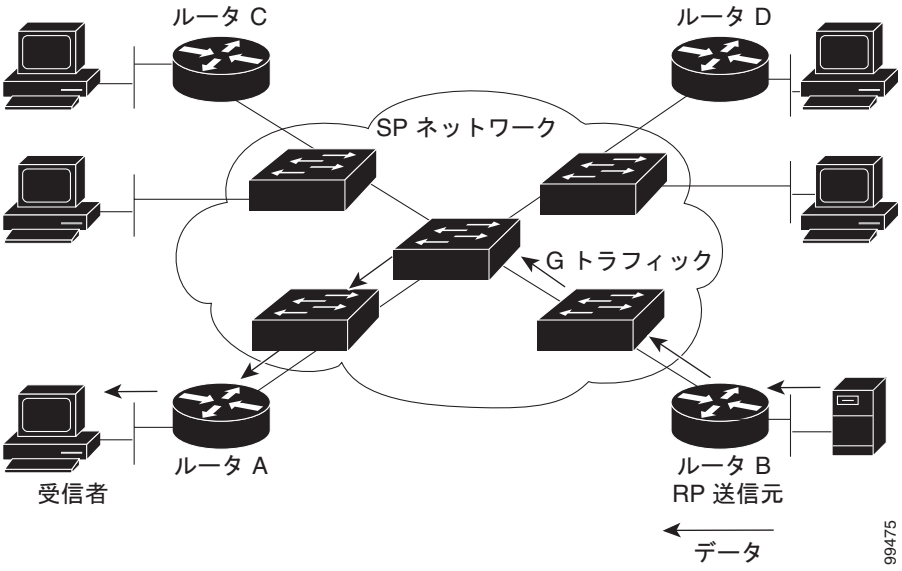


図 31-4 では、PIM スヌーピングがイネーブルの場合のデータ トラフィック フローを示します。この図では、スイッチはデータ トラフィックを 受信する必要があるルータ（ルータ A）にのみ転送します。

図 31-4　PIM スヌーピングがある場合のデータ トラフィック フロー



PIM スヌーピングのデフォルト設定

PIM スヌーピングは、デフォルトではディセーブルに設定されています。

PIM スヌーピング設定時の注意事項および制約事項

PIM スヌーピングを設定する際に、以下の注意事項と制約事項に従ってください。

- PIM Sparse（疎）モード（PIM-SM）機能を使用すると、ダウンストリーム ルータは、PIM Join またはプルーニング メッセージを通じて事前に関与を示す場合、トラフィックのみを監視します。アップストリーム ルータは、PIM Join またはプルーニング プロセス中にアップストリーム ルータとして使用された場合、トラフィックのみを監視します。
- Join またはプルーニング メッセージは、ルータ ポートすべてにフラッディングされるわけではありませんが、Join またはプルーニング メッセージのペイロードに指定されたアップストリーム ルータに対応するポートにのみ、送信されます。
- 直接接続された送信元は、双方向 PIM グループでサポートされます。直接接続された送信元からのトラフィックは、VLAN の Designated Router（DR; 指定ルータ）および指定フォワーダに転送されます。Nondesignated Router（NDR）がダウンストリーム（S, G）Join を受信できる場合があります。送信元のみのネットワークでは、初回の不明なトラフィックは指定ルータおよび指定フォワーダにのみ転送されます。
- dense（密）グループ モード トラフィックは、不明なトラフィックとして見なされ廃棄されます。
- AUTO-RP グループ（224.0.1.39 および 224.0.1.40）は常にフラッディングされます。
- スイッチは指定フォワーダ選定でスヌーピングを実行し、VLAN のさまざまな RP 用に指定フォワーダ ルータすべてのリストを維持します。すべてのトラフィックは 指定フォワーダすべてに送信されます。これにより双方向機能が正しく動作します。
- PIM スヌーピングおよび IGMP スヌーピングを、VLAN で同時にイネーブルできます。Router-Port Group Management Protocol（RGMP）または PIM スヌーピングいずれかを VLAN でイネーブルにできますが、両方同時にはイネーブルにできません。
- 非 PIMv2 マルチキャスト ルータは、すべてのトラフィックを受信します。
- PIM スヌーピングは、VLAN 単位でイネーブルおよびディセーブルにできます。
- PIM Hello および Join/プルーニング制御パケットに示されたホールドタイムに基づき、mroute およびルータ情報はすべて時間切れとなります。mroute ステートおよびネイバ情報はすべて VLAN 単位で維持されます。

PIM スヌーピングの設定

ここでは、PIM スヌーピングを設定する手順について説明します。

- 「PIM スヌーピングのグローバルなイネーブル化」（P.31-6）
- 「VLAN での PIM スヌーピングのイネーブル化」（P.31-6）
- 「PIM スヌーピングの DR フラッディングのディセーブル化」（P.31-7）

PIM スヌーピングのグローバルなイネーブル化

PIM スヌーピングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip pim snooping`	PIM スヌーピングをイネーブルにします。
	`Router(config)# no ip pim snooping`	PIM スヌーピングをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show ip pim snooping`	設定を確認します。

次に、PIM スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router(config)# ip pim snooping
Router(config)# end
Router# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
Router#
```

（注）　PIM スヌーピングを実行するには、IP アドレスまたは IP PIM を設定する必要はありません。

VLAN での PIM スヌーピングのイネーブル化

特定の VLAN で PIM スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface vlan` *vlan_ID*	VLAN インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip pim snooping`	PIM スヌーピングをイネーブルにします。
	`Router(config-if)# no ip pim snooping`	PIM スヌーピングをディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show ip pim snooping`	設定を確認します。

次に、VLAN 10 で PIM スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 10
Router(config-if)# ip pim snooping
Router(config-if)# end
Router# show ip pim snooping vlan 10
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
Router#
```

PIM スヌーピングの DR フラッディングのディセーブル化

（注）
- PIM スヌーピングの DR フラッディングの拡張機能は、以下のリリースでサポートされます。
  - Supervisor Engine 720 の Release 12.2(18)SXF 以降のリリース
  - Supervisor Engine 32 および Supervisor Engine 2 の Release 12.2(18)SXF2 以降のリリース
- マルチキャスト送信元をサポートするレイヤ 2 ブロードキャスト ドメイン上のスイッチで、DR フラッディングをディセーブルにしないでください。

デフォルトで、PIM スヌーピングがイネーブルのスイッチは、マルチキャスト トラフィックを DR にフラッディングします。この動作方法では、不要なマルチキャスト パケットが DR に送信される可能性があります。ネットワークは不要なトラフィックを伝送しなければならず、DR は不要なトラフィックを処理するか廃棄しなければなりません。

ネットワークから DR に送信されるトラフィックを削減するには、DR フラッディングをディセーブルにします。DR フラッディングをディセーブルにすると、PIM スヌーピングはマルチキャスト グループにある DR トラフィックへと移動し、DR へ向かうリンクの明示的な Join の受信のみを行います。

PIM スヌーピング DR フラッディングをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# no ip pim snooping dr-flood`	PIM スヌーピングの DR フラッディングをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show running-config | include dr-flood`	設定を確認します。

次に、PIM スヌーピングの DR フラッディングをディセーブルにする例を示します。

```
Router(config)# no ip pim snooping dr-flood
Router(config)# end
```

CHAPTER 32

Router-Port Group Management Protocol（RGMP）の設定

この章では、次の URL にある Release 12.2 のマニュアルに記載されている Router-Port Group Management Protocol（RGMP）に関する情報および手順を補足します。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/1cfrgmp.htm

この章で説明する内容は、次のとおりです。

RGMP の機能概要

RGMP は、無関係なマルチキャスト ルータにしか接続されていない Catalyst 6500 シリーズ スイッチ ポートからの、マルチキャスト トラフィックの送信を抑制します。RGMP はマルチキャスト トラフィックを受信するように設定されたルータにだけマルチキャスト トラフィックを転送して、ネットワークの輻輳を抑えます。

（注）　RGMP を使用するには、Catalyst 6500 シリーズ スイッチ上で IGMP スヌーピングをイネーブルにする必要があります。IGMP スヌーピングは、ホストが接続されている LAN ポートからのマルチキャスト トラフィックの送信を抑制します。IGMP スヌーピングは、1 つまたは複数のマルチキャスト ルータが接続されている LAN ポートからのトラフィックは抑制しません。

（注）　RGMP を動作させるには、すべてのルータおよびスイッチ上で、Protocol Independent Multicast（PIM）をイネーブルにする必要があります。現在サポートされているのは、PIM sparse（疎）モードだけです。

ネットワーク上のすべてのルータが RGMP 対応でなければなりません。RGMP 対応ルータは、RGMP Hello メッセージを定期的に送信します。RGMP Hello メッセージは Catalyst 6500 シリーズ スイッチに対して、ルータから Catalyst 6500 シリーズ スイッチに RGMP Join メッセージも送信された場合に限り、そのルータにマルチキャスト データを送信するように指示します。RGMP Join メッセージが送信されると、ルータはマルチキャスト データを受信できるようになります。

マルチキャスト データの受信を中止する場合、ルータから Catalyst 6500 シリーズ スイッチへ、RGMP Leave メッセージを送信する必要があります。ルータ上で RGMP をディセーブルにするには、ルータから Catalyst 6500 シリーズ スイッチへ、RGMP Bye メッセージを送信しなければなりません。

表 32-1 に、RGMP パケット タイプの要約を示します。

表 32-1　RGMP パケット タイプ

説明	アクション
Hello	ルータ上で RGMP がイネーブルになっている場合、Catalyst 6500 シリーズ スイッチがルータにマルチキャスト データ トラフィックを送信するのは、グループに対して RGMP Join が送信された場合に限られます。
Bye	ルータ上で RGMP がディセーブルになっている場合、Catalyst 6500 シリーズ スイッチはすべてのマルチキャスト データ トラフィックをルータへ送信します。
Join	マルチキャスト MAC（メディア アクセス制御）アドレスに対応するマルチキャスト データ トラフィックが、レイヤ 3 グループ アドレス G からルータへ送信されます。これらのパケットは、RGMP パケットの [Group Address] フィールドにグループ G が指定されています。
Leave	グループ G のマルチキャスト データ トラフィックは、ルータに送信されません。これらのパケットは、RGMP パケットの [Group Address] フィールドにグループ G が指定されています。

RGMP のデフォルト設定

レイヤ 2 LAN ポート上では、RGMP が永続的にイネーブルになっています。レイヤ 3 インターフェイス上では、RGMP はデフォルトでディセーブルに設定されています。

RGMP 設定時の注意事項および制約事項

RGMP を設定する際に、以下の注意事項と制約事項に従ってください。

- RGMP または PIM スヌーピングいずれかを VLAN でイネーブルにできますが、両方同時にはイネーブルにできません。
- RGMP は、PIM sparse（疎）モードをサポートしています。RGMP は、PIM dense（密）モードをサポートしていません。ただし、RGMP では、2 つの AutoRP グループが dense（密）モードでサポートされます。これらのグループへのトラフィックは抑制されず、すべてのルータ ポートにフラッディングされます。そのため、PIM sparse-dense モードを設定する必要があります。AutoRP グループ以外のグループを dense（密）モードに設定すると、これらのトラフィックは、RGMP 対応ルータ ポートからは正しく転送されません。
- RGMP を使用してマルチキャスト トラフィックを効率的に抑制するには、RGMP 対応ルータを、RGMP 対応 Catalyst 6500 シリーズ スイッチ上の個別のポートに接続してください （VLAN インターフェイスは、この条件を満たします）。
- RGMP は、RGMP 対応ルータを検出した LAN ポートからのトラフィック送信を抑制するだけです。LAN ポート上で RGMP 非対応ルータが検出されると、その LAN ポートはすべてのマルチキャスト トラフィックを受信します。
- RGMP は、ネットワーク上の直接接続されたマルチキャスト送信元をサポートしていません。直接接続されたマルチキャスト送信元は、RGMP または PIM を介してシグナリングせずにネットワーク上にマルチキャスト トラフィックを送信します。RGMP 対応ルータは、RGMP を介したそのマルチキャスト グループからの受信をあらかじめ要求している場合以外、このマルチキャスト トラフィックを受信しません。この制約は、ホストおよびルータのマルチキャスト トラフィック送信機能（**ping** コマンドおよび **mtrace** コマンド、および UDPTN などのマルチキャスト トラフィックを送信するマルチキャスト アプリケーションなど）に適用されます。
- RGMP は、ネットワーク上の直接接続されたレシーバーをサポートしています。これらのレシーバーへのトラフィックは、IGMP スヌーピングによって抑制されるか、レシーバーがルータの場合には PIM および RGMP によって抑制されます。
- ルータ上で RGMP がイネーブルになっている場合、ネットワーク上の Cisco Group Management Protocol（CGMP）はサポートされません。レイヤ 3 インターフェイス上で RGMP および CGMP を両方ともイネーブルにすることはできません。レイヤ 3 インターフェイス上で RGMP をイネーブルにすると、CGMP は自動的にディセーブルになります。逆の場合も同様です。
- 次の RGMP の特性は、IGMP スヌーピングと同様です。
  - RGMP は、送信元の IP アドレスではなく、マルチキャスト グループに基づいてトラフィックを抑制します。
  - ネットワーク上でスパニング ツリー トポロジが変化した場合、Cisco Group Management Protocol（CGMP）のように、そのステートが消去されることはありません。
  - RGMP は、RGMP 制御ネットワークで PIMv2 Bootstrap Router（BSR; ブートストラップ ルータ）を使用できるマルチキャスト グループ 224.0.0.x（x は 0 ～ 255）のトラフィックは抑制しません。
  - シスコ製ネットワーク装置の RGMP は、IP マルチキャスト アドレス上ではなく、MAC アドレス上で適用されます。1 つの MAC アドレスに複数の IP マルチキャスト アドレスをマッピングできますが（RFC1112 を参照）、RGMP は 1 つの MAC アドレスにマッピングされた複数の IP マルチキャスト グループを識別しません。
  - Catalyst 6500 シリーズ スイッチがトラフィックを抑制する性能は、スイッチの CAM（連想メモリ）テーブルの容量によって制限されます。

レイヤ 3 インターフェイス上での RGMP のイネーブル化

レイヤ 3 インターフェイス上で RGMP をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**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 2	Router(config-if)# **ip rgmp**	レイヤ 3 インターフェイス上で RGMP をイネーブルにします。
	Router(config-if)# **no ip rgmp**	レイヤ 3 インターフェイス上で RGMP をディセーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **debug ip rgmp** [*name_or_group_address*]	（任意）RGMP をモニタします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、または **ge-wan**

次に、ファスト イーサネット ポート 3/3 に RGMP を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/3
Router(config-if)# ip rgmp
Router(config-if)# end
Router#
```

CHAPTER 33

ネットワーク セキュリティの設定

この章では、Catalyst 6500 シリーズ スイッチ固有のネットワーク セキュリティ機能について説明します。これは、次のマニュアルに記載されているネットワーク セキュリティに関する情報および手順を補足するためのものです。

- 次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
- 次の URL にある『*Cisco IOS Security Command Reference*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

MAC アドレスベースのトラフィック ブロッキングの設定

特定の VLAN 内の MAC（メディア アクセス制御）アドレスを経由するすべてのトラフィックをブロックするには、次の作業を行います。

コマンド	目的
`Router(config)# mac-address-table static mac_address vlan vlan_ID drop`	特定の VLAN 内で設定されている MAC アドレスを経由するすべてのトラフィックをブロックします。
`Router(config)# no mac-address-table static mac_address vlan vlan_ID`	MAC アドレスベースのブロッキングを消去します。

次に、VLAN 12 内で MAC アドレス 0050.3e8d.6400 を経由するすべてのトラフィックをブロックする例を示します。

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

TCP インターセプトの設定

TCP インターセプト フローはハードウェアで処理されます。

設定手順については、下記の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」、「Configuring TCP Intercept（Preventing Denial-of-Service Attacks）」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfdenl.htm

ユニキャスト RPF チェックの設定

ここでは、Cisco IOS ユニキャスト Reverse Path Forwarding（RPF）チェック（ユニキャスト RPF チェック）について説明します。

ポリシー フィーチャ カード 3（PFC3）ユニキャスト RPF チェックのサポートの概要

ユニキャスト RPF チェック機能概要の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Other Security Features」、「Configuring Unicast Reverse Path Forwarding」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）は、複数のインターフェイスからのトラフィックの RPF チェックをハードウェアでサポートします。

strict 方式 ユニキャスト RPF チェックの場合、PFC3 はルーティング テーブルのプレフィクスすべてに対し 2 つのパラレル パスと、4 つのユーザ設定変更可能な RPF インターフェイス グループ（各インターフェイス グループには 4 つのインターフェイスが含まれます）のいずれかを通じて到達したプレフィクスに対し最大 4 つのパラレル パスをサポートします。

loose 方式ユニキャスト RPF チェック（別名 exist-only 方式）の場合、PFC3 は最大 8 つのリバース パス インターフェイスをサポートします（Cisco IOS ソフトウェアはルーティング テーブルでは 8 つのリバース パスに制限されます）。

Cisco IOS でユニキャスト RPF チェックを実行する方式は、次の 4 つです。

- strict ユニキャスト RPF チェック
- allow-default を使用した strict ユニキャスト RPF チェック
- loose ユニキャスト RPF チェック
- allow-default を使用した loose ユニキャスト RPF チェック

ユニキャスト RPF チェックをインターフェイス単位で設定できますが、ユニキャスト RPF チェックがイネーブルであるインターフェイスすべてに対して PFC3 がサポートするのは、ユニキャスト RPF 方式だけです。現在設定されている方式とは異なるユニキャスト RPF 方式を使用するようにインターフェイスを設定する場合、ユニキャスト RPF チェックがイネーブルになっているシステムのインターフェイスすべてが、新しい方式を使用します。

PFC2 ユニキャスト RPF チェックのサポートの概要

PFC2 は、1 つのリターン パスを持つパケットをハードウェアで処理することによってユニキャスト RPF チェックをサポートしています。Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）2 は、複数のリターン パスを持つトラフィックをソフトウェアで処理します（負荷分散など）。

ユニキャスト RPF チェックの注意事項および制約事項

ユニキャスト RPF チェック を設定する際に、以下の注意事項と制約事項に従ってください。

- ユニキャスト RPF チェックを設定し、Access Control List（ACL; アクセス制御リスト）でフィルタをかける場合、PFC はトラフィックが ACL と一致するかどうかを判断します。PFC は、RPF ACL に拒否されたトラフィックを MSFC へ送信してユニキャスト RPF チェックを行います。ACL によって許可されたパケットは、ユニキャスト RPF チェックを受けずにハードウェアで転送されます（CSCdz35099）。
- 通常、Denial of Service（DoS; サービス拒絶）攻撃のパケットは拒否 Access Control Entry（ACE; アクセス制御エントリ）と一致し、ユニキャスト RPF チェックを受けるため MSFC に送信されます。そのため、送信されたパケットで MSFC は過負荷状態になる可能性があります。
- PFC は、ユニキャスト RPF チェックの ACL とは一致しなくても、入力セキュリティ ACL と一致するトラフィックをハードウェアでサポートします。
- PFC では、Policy-Based Routing（PBR; ポリシーベース ルーティング）トラフィックの ユニキャスト RPF チェックをハードウェアでサポートしません （CSCea53554）。

ユニキャスト RPF チェックの設定

ここでは、ユニキャスト RPF チェックの設定手順について説明します。

- 「ユニキャスト RPF チェック モードの設定」（P.33-4）
- 「PFC3 での複数パスのユニキャスト RPF チェック モードの設定」（P.33-6）
- 「self-ping のイネーブル化」（P.33-7）

ユニキャスト RPF チェック モードの設定

ユニキャスト RPF には、次に示す 2 つのチェック モードがあります。

- strict チェック モード - 送信元 IP アドレスが Forwarding Information Base（FIB; 転送情報ベース）テーブルにあること、および入力ポートから到達可能な範囲内にあることを確認します。
- exist-only チェック モード - 送信元 IP アドレスが FIB テーブルにあるかどうかだけを確認します。

（注）　ユニキャスト RPF チェック用に設定されたすべてのポートには、その時点で設定されているモードが自動的に適用されます。

ユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID}	{type[1] slot/port}	{port-channel number}}`	設定するインターフェイスを選択します。 （注）　ユニキャスト RPF チェックは次の宛先にパケットを転送する前に、入力ポートに基づいて、最適なリターン パスを確認します。
ステップ 2	`Router(config-if)# ip verify unicast source reachable-via {rx	any} [allow-default] [list]` `Router(config-if)# no ip verify unicast`	ユニキャスト RPF チェック モードを設定します。 デフォルトのユニキャスト RPF チェック モードに戻します。
ステップ 3	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls cef ip rpf`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ユニキャスト RPF チェック モードを設定する場合、次の情報に注意してください。

- strict チェック モードをイネーブルにするには、**rx** キーワードを使用します。
- exist-only チェック モードをイネーブルにするには、**any** キーワードを使用します。
- RPF の確認にデフォルト ルートを使用できるようにするには、**allow-default** キーワードを使用します。
- アクセス リストを識別するには、*list* オプションを使用します。
  - アクセス リストによってネットワークへのアクセスが拒否された場合は、スプーフィングされたパケットがポートで廃棄されます。
  - アクセス リストによってネットワークへのアクセスが許可された場合は、スプーフィングされたパケットが宛先アドレスに転送されます。転送されたパケットは、インターフェイスの統計情報にカウントされます。
  - アクセス リストにログ アクションが含まれている場合、スプーフィングされたパケットに関する情報がログ サーバに送信されます。

（注）　**ip verify unicast source reachable-via** コマンドを入力すると、ユニキャスト RPF チェック モードがスイッチのすべてのポートで変更されます。

次に、ギガビット イーサネット ポート 4/1 でユニキャスト RPF の exist-only チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 4/2 でユニキャスト RPF の strict チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 4/2
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/2
ip address 42.0.0.1 255.0.0.0
ip verify unicast reverse-path
no cdp enable
end
Router# show running-config interface gigabitethernet 4/1
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/1
ip address 41.0.0.1 255.0.0.0
➔ ip verify unicast reverse-path (RPF mode on g4/1 also changed to strict-check RPF mode)
no cdp enable
end
Router#
```

PFC3 での複数パスのユニキャスト RPF チェック モードの設定

PFC3 で複数パスのユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls ip cef rpf multipath** {**punt** | **pass** | **interface-group**}	PFC3 で複数のパス RPF チェック モードを設定します。
	Router(config)# **no mls ip cef rpf multipath** {**punt** | **interface-group**}	デフォルト値に戻します（**mls ip cef rpf multipath punt**）。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls cef ip rpf**	設定を確認します。

複数のパス RPF チェックを設定する場合、次の情報に注意してください。

- **punt**（デフォルト）– PFC3 は、プレフィクス単位で最大 2 つのインターフェイスに対し、ハードウェアのユニキャスト RPF チェックを実行します。追加のインターフェイスに着信するパケットは MSFC3 にリダイレクト（パント）されて、ソフトウェアでユニキャスト RPF チェックが実行されます。
- **pass** – PFC3 は、single-path および two-path プレフィクスに対し、ハードウェアでユニキャスト RPF チェックを実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある multipath プレフィクスから着信するパケットに対し、ディセーブルです（このパケットは常にユニキャスト RPF チェックに合格します）。
- **interface-group** – PFC3 は、single-path および two-path プレフィクスに対し、ハードウェアでユニキャスト RPF チェックを実行します。PFC3 はプレフィクス単位で最大 4 つの追加インターフェイスに対し、ユーザ設定変更可能なマルチパス ユーザ RPF チェック インターフェイス グループを介して、ユニキャスト RPF チェックを実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある他の multipath プレフィクスから着信するパケットに対し、ディセーブルです（このパケットは常にユニキャスト RPF チェックが行われます）。

次に、複数パスの RPF チェックを設定する例を示します。

```
Router(config)# mls ip cef rpf multipath punt
```

PFC3 での複数パスのインターフェイス グループの設定

複数パスのユニキャスト RPF インターフェイス グループを PFC3 に設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls ip cef rpf interface-group** [**0** | **1** | **2** | **3**] *interface1* [*interface2* [*interface3* [*interface4*]]]	複数パスの RPF インターフェイス グループを PFC3 に設定します。
ステップ 2	Router(config)# **mls ip cef rpf interface-group** *group_number*	インターフェイス グループを削除します。
ステップ 3	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show mls cef ip rpf**	設定を確認します。

次に、インターフェイス グループ 2 を設定する例を示します。

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

self-ping のイネーブル化

ユニキャスト RPF チェックがイネーブルの場合、スイッチはデフォルトで self-ping を実行できません。

self-ping をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**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 2	Router(config-if)# **ip verify unicast source reachable-via any allow-self-ping**	self-ping またはセカンダリ アドレスへの ping を実行できるように、スイッチをイネーブルにします。
	Router(config-if)# **no ip verify unicast source reachable-via any allow-self-ping**	self-ping をディセーブルにします。
ステップ 3	Router(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、self-ping をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```

CHAPTER 34

Cisco IOS ACL サポートの概要

この章では、Catalyst 6500 シリーズ スイッチの Cisco IOS Access Control List（ACL; アクセス制御リスト）サポートについて説明します。

Cisco IOS ACL 設定の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm

Cisco IOS ACL 設定時の注意事項および制約事項

Cisco IOS ACL 設定には、次の注意事項および制約事項が適用されます。

- Cisco IOS ACL をレイヤ 3 ポートおよび Virtual LAN（VLAN; 仮想 LAN）インターフェイスに直接、適用できます。
- VLAN ACL（VACL）を VLAN に適用できます（第 35 章「VLAN アクセス制御リスト（VACL）の設定」を参照）。
- 各タイプの ACL（IP、Internetwork Packet Exchange（IPX）、および Media Access Control（MAC; メディア アクセス制御））は対応するトラフィック タイプだけをフィルタリングします。Cisco IOS MAC ACL が IP または IPX トラフィックと一致することはありません。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、MSFC のソフトウェアでサポートされます。
- パケットがアクセス グループによって拒否された場合、デフォルトで MSFC が Internet Control Message Protocol（ICMP）到達不能メッセージを送信します。

  ip unreachables コマンドがイネーブルの場合（デフォルト）、スーパーバイザ エンジンは拒否されたパケットの大部分をハードウェアで廃棄し、一部のパケット（最大で 10 パケット/秒）だけが MSFC に送信されて廃棄されます（これにより ICMP 到達不能メッセージが生成されます）。

  拒否されたパケットを廃棄し、ICMP 到達不能メッセージを生成することによって MSFC の CPU にかかる負荷を軽減するには、**no ip unreachables** 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、ICMP 到達不能メッセージをディセーブルにします。これにより、アクセス グループによって拒否されたすべてのパケットがハードウェアで廃棄されます。

- パケットが VACL によって拒否された場合、ICMP 到達不能メッセージは送信されません。
- 名前付き ACL（番号付けされた ACL ではなく）を使用することを強くお勧めします。名前付き ACL を使用すると、ACL 設定を作成または編集したとき、およびシステムの再起動時の CPU 利用を節約できます。ACL エントリを作成すると（または既存 ACL エントリを編集すると）、ACL 設定を PFC ハードウェアにロードするために ACL 結合と呼ばれる CPU 負荷の高い処理が発生します。ACL 結合は、システムの再起動中にスタートアップ コンフィギュレーションが適用されるときにも発生します。

  名前付き ACL では、ACL 結合が開始されるのはユーザが **named-acl** 設定モードを終了したときだけです。一方、番号付けされた ACL では、ACE 定義ごとに ACL 結合が開始され、ACL の設定中に大量の中間結合が発生します。

ハードウェアおよびソフトウェア ACL のサポート

ACL は、ハードウェアの場合には PFC、Distributed Forwarding Card（DFC）で、ソフトウェアの場合には MSFC で処理できます。次の動作における、ACL のソフトウェアとハードウェア処理を説明します。

- 標準 ACL および拡張 ACL（入力および出力）の [deny] ステートメントに一致する ACL フローは、[ipunreachables] がディセーブルに設定されている場合、ハードウェアによって廃棄されます。
- 標準 ACL および拡張 ACL（入力および出力）の [permit] ステートメントに一致する ACL フローは、ハードウェアで処理されます。
- VACL フローはハードウェアで処理されます。VACL match コマンド文で指定されたフィールドがハードウェア処理でサポートされていない場合、そのフィールドは無視されるか（たとえば、**log** キーワードが入っていて、ACL が match コマンド文に使用された）、または設定全体が破棄されます（たとえば、IPX ACL パラメータを含む VACL）。VACL ログ機能は、action コマンドを使用して、ソフトウェアで処理されます。
- VACL ログ機能はソフトウェアで処理されます。
- ダイナミック ACL フローはハードウェアで処理されます。
- アイドル タイムアウトはソフトウェアで処理されます。

（注） アイドル タイムアウトは、設定できません。Catalyst 6500 シリーズ スイッチでは、**access-enable host timeout** コマンドはサポートされていません。

- MPLS インターフェイスを除き、セッション内の最初のパケットが RP 上のソフトウェアで処理されたあと、再帰 ACL フローがハードウェアで処理されます。
- 特定のポート上の ACL アクセス違反の IP アカウントは、そのポート上で拒否された全パケットを MSFC に転送し、ソフトウェアで処理させることによってサポートされます。この動作は他のフローには影響しません。
- PFC では、ハードウェアで Cisco IOS IPX ACL をサポートしません。Cisco IOS IPX ACL は、MSFC のソフトウェアでサポートされます。
- 名前ベースの拡張 MAC アドレス ACL は、ハードウェアでサポートされています。

- 次の ACL タイプは、ソフトウェアによって処理されます。
  - Internetwork Packet Exchange（IPX）アクセス リスト
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - 拡張 MAC アドレス アクセス リスト
  - プロトコル タイプコード アクセス リスト

（注）　ヘッダー長が 5 バイト未満の IP パケットは、アクセス制御されません。

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）を設定しない場合、ロギングを必要とするフローはソフトウェアで処理され、ハードウェアでの非ロギング フローの処理には影響しません（「PFC3 での OAL」（P.34-5）を参照）。
- ソフトウェアで処理されるフローの転送レートは、ハードウェアで処理されるフローに比べると、大幅に小さくなります。
- **show ip access-list** コマンドの出力に表示されるマッチ カウントには、ハードウェアで処理されたパケットは含まれません。

IPv6 アドレス圧縮の設定

アクセス制御リスト（ACL）は、ハードウェアの Policy Feature Card（PFC; ポリシー フィーチャ カード）内に実装されます。PFC では、ACL テーブルをインデックス化するために、パケット内の送信元または宛先の IP アドレスとポート番号が使用されます。インデックスでのアドレスの長さは、最大 128 ビットです。

IPv6 パケット内の IP アドレス フィールドは 128 ビットで、ポート フィールドは 16 ビットです。ACL ハードウェアで完全な IPv6 アドレスを使用するには、**mls ipv6 acl compress address unicast** コマンドを使用して、IPv6 アドレスの圧縮を有効にする必要があります。この機能は、未使用の 16 ビットを IPv6 アドレスから削除することによって、IPv6 アドレス（ポートも含む）を 128 ビットに圧縮します。圧縮可能なアドレス タイプは、情報を一切失うことなく圧縮できます。圧縮方法の詳細については、表 34-1 を参照してください。

リリース 12.2(17a)SX 以降では、Supervisor Engine 720 での IPv6 圧縮コマンドがサポートされています。このコマンドは、Supervisor Engine 2 ではサポートされていません。

デフォルトでは、このコマンドは圧縮なしに設定されています。

注意　ネットワーク上に圧縮不可能なアドレス タイプがある場合は、圧縮モードをイネーブルにしないでください。圧縮可能なアドレス タイプとアドレス圧縮方法の一覧を表 34-1 に示します。

表 34-1　圧縮可能なアドレス タイプと圧縮方法

アドレス タイプ	圧縮方法
MAC アドレスに基づいた EUI-64	このアドレスは、ビット位置 [39:24] からの 16 ビットを削除することにより圧縮されます。これらのアドレスをハードウェア圧縮した場合、情報は一切失われません。
埋め込み IPv4 アドレス	このアドレスは、上位 16 ビットを削除することにより圧縮されます。これらのアドレスをハードウェア圧縮した場合、情報は一切失われません。
リンク ローカル	このアドレスは、ビット [95:80] 内の 0 を削除することにより圧縮され、埋め込み IPv4 アドレスと同じパケット タイプを使用して識別されます。これらのアドレスをハードウェア圧縮した場合、情報は一切失われません。
その他	上記のどの分類にも入らない IPv6 アドレスは、その他に分類されます。IPv6 アドレスがその他に分類される場合は、次のようになります。 • 圧縮モードがオンになっている場合は、IPv6 アドレスは、EUI-64 圧縮法と同じように圧縮され（ビット [39:24] が削除されます）。レイヤ 4 のポート情報は QoS TCAM の検索に使用されるキーの一部として使用できますが、レイヤ 3 情報は失われます。 • グローバル圧縮モードがオフになっている場合は、IPv6 アドレスの 128 ビット全体が使用されます。IPv6 検索キーのサイズの制約が原因で、QoS TCAM を検索するためにレイヤ 4のポート情報をキーに含めることはできません。

IPv6 アドレスの圧縮をオンにするには、**mls ipv6 acl compress address unicast** コマンドを入力します。IPv6 アドレスの圧縮をオフにするには、このコマンドを **no** の形式で入力します。

次に、IPv6 アドレスのアドレス圧縮をオンにする例を示します。

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

次に、IPv6 アドレスのアドレス圧縮をオフにする例を示します。

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

PFC3 での OAL

（注）　Supervisor Engine 2 は、OAL をサポートしていません。

Release 12.2(17d)SXB 以降のリリースでは、PFC3 での OAL をサポートしています。ここでは OAL について説明します。

OAL の概要

OAL は、ACL ロギングをハードウェアでサポートしています。OAL を設定しない限り、ロギングを必要とするパケットは、MSFC のソフトウェアで完全に処理されます。OAL では、PFC3 のハードウェアでパケットの許可または廃棄を行い、最適化ルーチンを使用して情報を MSFC3 に送信し、ロギング メッセージを生成します。

OAL に関する注意事項および制約事項

OAL には、次の注意事項および制約事項が適用されます。

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）キャプチャと VACL キャプチャには互換性がありません。スイッチに両方の機能を混在させないでください。OAL が設定された状態で、SPAN を使用してトラフィックをキャプチャします。
- OAL は、PFC3 のみでサポートされます。
- OAL は IPv4 ユニキャスト パケットのみをサポートしています。
- OAL は、許可された入力トラフィックの VACL ロギングをサポートしています。
- OAL は、ポート ACL（PACL）はサポートしていません。
- OAL は、次のものに対してはハードウェアでのサポートをしていません。
  - 再帰 ACL
  - 他の機能（QoS など）のトラフィックのフィルタ処理に使用される ACL
  - ユニキャスト Reverse Path Forwarding（uRPF）チェック例外の ACL
  - 例外パケット（TTL 障害や MTU 障害など）
  - IP オプションが指定されたパケット
  - レイヤ 3 でルータへのアドレスが指定されたパケット
  - ICMP 到達不能メッセージを生成するために MSFC3 へ送信されるパケット
  - ハードウェアでは加速されず、機能によって処理されるパケット
- 拒否されたパケットに OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL の設定

ここでは、OAL の設定手順について説明します。

（注）
- この項で使用してい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 Master Command List*, Release 12.2SX』を参照してください。
- 拒否されたパケットに OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL グローバル パラメータの設定

OAL グローバル パラメータを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# logging ip access-list cache {{entries` *number_of_entries*`} | {interval` *seconds*`} | {rate-limit` *number_of_packets*`} | {threshold` *number_of_packets*`}}`	OAL グローバル パラメータを設定します。
`Router(config)# no logging ip access-list cache {entries | interval | rate-limit | threshold}`	OAL グローバル パラメータをデフォルトに戻します。

OAL グローバル パラメータを設定する場合、次の情報に注意してください。

- **entries** *number_of_entries*:
  - キャッシュされるエントリの最大数を設定します。
  - 範囲：0 ～ 1,048,576（カンマを付けずに入力）
  - デフォルト：8192
- **interval** *seconds*:
  - ログのためにエントリが送信されるまでの最大時間を設定します。この時間中エントリが非アクティブの場合、キャッシュから削除されます。
  - 範囲：5 ～ 86,400（1440 分つまり 24 時間、カンマを付けずに入力）
  - デフォルト：300 秒（5 分）
- **rate-limit** *number_of_packets*:
  - ソフトウェアで 1 秒間にログに記録されるパケット数を設定します。
  - 範囲：10 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト：0（レート制限がオフになり、すべてのパケットがログに記録されます）

- **threshold** *number_of_packets*:
  - エントリがログに記録されるまでに一致するパケット数を設定します。
  - 範囲：1 ～ 1,000,000（カンマを付けずに入力）
  - デフォルト：0（一致パケット数に達してもログの記録は開始されません）

インターフェイスでの OAL の設定

インターフェイスで OAL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# logging ip access-list cache in`	インターフェイスの入力トラフィックに対して OAL をイネーブルにします。
	`Router(config-if)# no logging ip access-list cache`	インターフェイスでの OAL をディセーブルにします。
ステップ 3	`Router(config-if)# logging ip access-list cache out`	インターフェイスの出力トラフィックに対して OAL をイネーブルにします。
	`Router(config-if)# no logging ip access-list cache`	インターフェイスでの OAL をディセーブルにします。

1. *type* = レイヤ 3 スイッチド トラフィックをサポートする任意のタイプ

OAL 情報の表示

OAL 情報を表示するには、次の作業を行います。

コマンド	目的
`Router # show logging ip access-list cache`	OAL 情報を表示します。

キャッシュされた OAL エントリのクリア

キャッシュされた OAL エントリをクリアするには、次の作業を行います。

コマンド	目的
`Router # clear logging ip access-list cache`	キャッシュされた OAL エントリをクリアします。

ACL におけるレイヤ 4 演算の使用上の注意事項および制約事項

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

レイヤ 4 演算の使用

次のタイプの演算子を指定できます。

- gt（greater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する*演算*は、*9* つまでにしてください。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

レイヤ 4 演算を使用するときは、次の 2 つの注意事項に従ってください。

- レイヤ 4 演算は、演算子またはオペランドが異なっていると、違う演算であると見なされます。たとえば、次の ACL には 3 つの異なるレイヤ 4 演算が定義されています（[gt 10] と [gt 11] は 2 つの異なるレイヤ 4 演算です）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

（注）　[eq] 演算子の使用に制限はありません。[eq] 演算子は Logical Operator Unit（LOU; 論理演算ユニット）またはレイヤ 4 演算ビットを使用しないためです。LOU については、「LOU の使用」（P.34-9）を参照してください。

- レイヤ 4 演算は、同じ演算子 / オペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。たとえば次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

LOU の使用

LOU は、演算子 / オペランドの組み合わせを保存するレジスタです。ACL はすべて、LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子 / オペランドの組み合わせが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

レイヤ 4 演算数と LOU 数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU 1 に、[gt 10] と [lt 9] が保存されます。
- LOU 2 に、[gt 11] と [neq 6] が保存されます。
- LOU 3 に、[gt 20] が保存されます（半分は空き）。
- LOU 4 に、[range 11 13] が保存されます（範囲に LOU 全体が必要）。

CHAPTER 35

VLAN アクセス制御リスト（VACL）の設定

この章では、Catalyst 6500 シリーズ スイッチで VLAN Access Control List（VACL; VLAN アクセス制御リスト）を設定する手順を説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

- Supervisor Engine 720 および Release 12.2(17d)SXB よりも前のリリースの場合、VACL キャプチャは、WS-SVC-IDSM2-K9 Intrusion Detection System Module 2（IDSM2; 侵入検知システム モジュール 2）および WS-SVC-NAM-2/WS-SVC-NAM-1 ネットワーク解析モジュールとともに使用する場合にだけサポートされます。この制限事項は、Release 12.2(17d)SXB 以降では解消されています。
- Optimized ACL Logging（OAL; 最適化された ACL ロギング）キャプチャと VACL キャプチャには互換性がありません。スイッチに両方の機能を混在させないでください。OAL が設定されている場合は（「PFC3 での OAL」（P.34-5）を参照）、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を使用してトラフィックをキャプチャします。

この章で説明する内容は、次のとおりです。

VACL の概要

ここでは VACL について説明します。

VACL の概要

VACL は、Virtual LAN（VLAN; 仮想 LAN）内でブリッジされるか、VLAN または VACL キャプチャの WAN インターフェイスとの間でルーティングされているすべてのパケットのアクセス制御を行います。ルータ インターフェイスでだけ設定され、ルーティング対象パケットにだけ適用される通常の Cisco IOS 標準または拡張 ACL と異なり、VACL はすべてのパケットに適用され、どの VLAN または WAN インターフェイスにも適用できます。VACL はハードウェアで処理されます。VACL は Cisco IOS ACL を使用します。VACL は、ハードウェアでサポートされていないすべての Cisco IOS ACL フィールドを無視します。

IP、Internetwork Packet Exchange（IPX）、および Media Access Control（MAC; メディア アクセス制御）レイヤ トラフィックの場合は、VACL を設定できます。WAN インターフェイスに適用される VACL は、VACL キャプチャの IP トラフィックだけをサポートします。

VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットが、この VACL と照合されます。VACL を VLAN に適用し、ACL を VLAN 内のルーティング対象インターフェイスに適用すると、VLAN に着信するパケットは最初に VACL と照合されます。そこで許可されると、次に入力 ACL と照合され、それからルーティング対象インターフェイスで処理されます。別の VLAN にルーティングされるパケットは、最初に、ルーティング対象インターフェイスに適用される出力 ACL と照合されます。そこで許可されると、宛先 VLAN 用に設定された VACL が適用されます。VACL が特定のパケット タイプ用に設定されていて、VACL と該当タイプのパケットとが一致しない場合、デフォルト動作では、パケットが拒否されます。

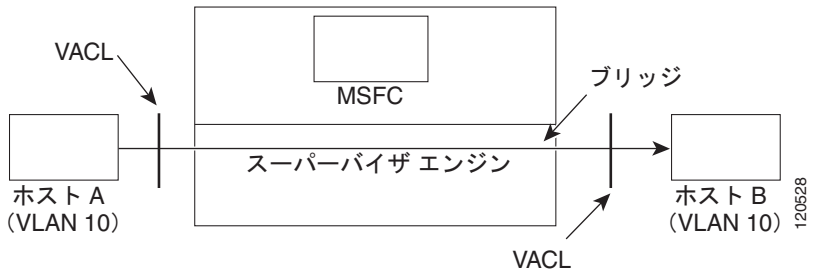
（注）

- Transmission Control Protocol（TCP）インターセプトおよび再帰 ACL は、VACL と同じインターフェイスに設定されている場合、VACL よりも優先されます。
- VACL および Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）は、同じインターフェイス上に設定できません。
- Internet Group Management Protocol（IGMP）パケットは VACL と照合されません。
- Policy Based Routing（PBR; ポリシー ベース ルーティング）によって、同じインターフェイス上に VACL キャプチャが設定されている場合、Binary Decision Diagram（BDD）を ACL 結合アルゴリズムとして選択しないでください。スーパーバイザ エンジン 720 のデフォルト ACL 結合アルゴリズム、Order Dependent Merge（ODM）の使用を推奨します。

ブリッジド パケット

図 35-1 に、ブリッジド パケットに適用される VACL を示します。

図 35-1　　ブリッジド パケットへの VACL の適用

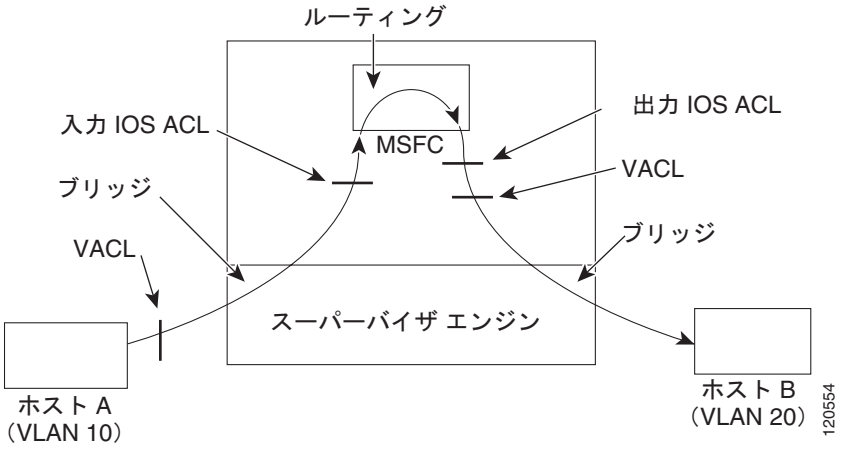


ルーティング対象パケット

図 35-2 に、ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに ACL を適用する方法を示します。ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに対して、ACL は次の順番で適用されます。

1. 入力 VLAN 用 VACL
2. 入力 Cisco IOS ACL
3. 出力 Cisco IOS ACL
4. 出力 VLAN 用 VACL

図 35-2　　ルーティング対象パケットへの VACL の適用

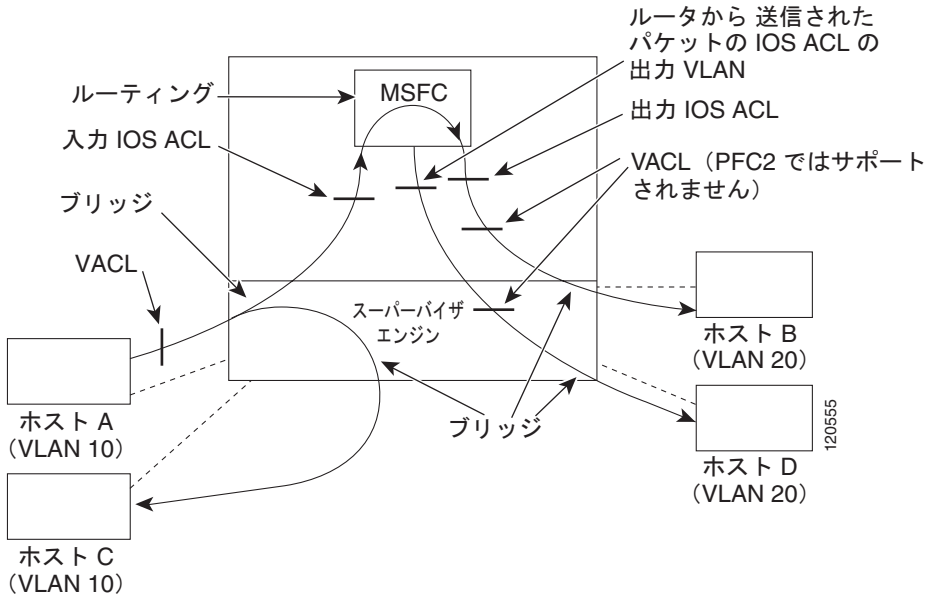


マルチキャスト パケット

図 35-3 に、マルチキャスト拡張が必要なパケットに ACL を適用する方法を示します。マルチキャスト拡張が必要なパケットに対して、ACL は次の順番で適用されます。

1. マルチキャスト拡張が必要なパケット：
   a. 入力 VLAN 用 VACL
   b. 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット：
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN 用 VACL
3. ルータから送信されるパケット - 出力 VLAN 用 VACL

図 35-3　マルチキャスト パケットへの VACL の適用



VACL の設定

ここでは、VACL の設定手順について説明します。

VACL の設定の概要

VACL は標準および拡張 Cisco IOS IP と IPX ACL、MAC レイヤ名前付き ACL（「MAC ACL の設定」（P.41-71）を参照）、および VLAN アクセス マップを使用します。

VLAN アクセス マップは、VLAN または VACL キャプチャの WAN インターフェイスに適用されます。WAN インターフェイスに付加された VACL は、標準または拡張 Cisco IOS IP ACL だけをサポートします。

各 VLAN アクセス マップは、1 つまたは複数のマップ シーケンスで構成できます。各シーケンスには match コマンドと action コマンドが含まれます。match コマンドはトラフィック フィルタリング用の IP、IPX、または MAC ACL を指定します。action コマンドは一致した場合に実行するアクションを指定します。フローが許可（permit）ACL エントリと一致した場合、関連付けられたアクションが実行され、それ以降の残りのシーケンスに対してフローはチェックされません。フローが拒否（deny）ACL エントリと一致した場合、同じシーケンス内の次の ACL、または次のシーケンスに対してフローがチェックされます。フローがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。

ブリッジド トラフィックおよびルーティング対象トラフィックの両方にアクセス制御を使用するには、VACL を単独で使用するか、または VACL と ACL を組み合わせて使用します。VLAN インターフェイス上で ACL を定義して、入力と出力のルーティング対象トラフィックに対してアクセスを制御できます。VACL を定義して、ブリッジド トラフィックに対してアクセス制御を使用します。

VACL とともに ACL を使用する場合は、次の点に注意してください。

- 発信 ACL での記録の必要があるパケットは、VACL で拒否された場合、記録されません。
- VACL は Network Address Translation（NAT; ネットワーク アドレス変換）変換前のパケットに適用されます。アクセス制御されなかった変換フローは、VACL 設定により、変換後にアクセス制御される場合があります。

VACL の action コマンドには、転送（forward）、廃棄（drop）、キャプチャ（capture）、またはリダイレクト（redirect）を指定できます。トラフィックをログに記録することもできます。WAN インターフェイスに適用された VACL は、リダイレクトまたはログ アクションをサポートしません。

（注）

- VACL のマップの最後には、暗黙的な拒否エントリがあります。パケットがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。
- 空または未定義の ACL が VACL 内で指定されている場合、すべてのパケットはこの ACL に一致し、関連付けられたアクションが実行されます。

VLAN アクセス マップの定義

VLAN アクセス マップを定義するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan access-map map_name [0-65535]`	VLAN アクセス マップを定義します。任意で、VLAN アクセス マップのシーケンス番号を指定できます。
`Router(config)# no vlan access-map map_name 0-65535`	VLAN アクセス マップからマップ シーケンスを削除します。
`Router(config)# no vlan access-map map_name`	VLAN アクセス マップを削除します。

VLAN アクセス マップを定義する場合、次の情報に注意してください。

- エントリを追加または変更する場合は、マップのシーケンス番号を指定します。
- マップのシーケンス番号を指定しないと、番号が自動的に割り当てられます。
- 各マップ シーケンスには、match コマンドおよび action コマンドをそれぞれ 1 つだけ指定できます。
- マップ シーケンスを削除する場合は、シーケンス番号を指定して **no** キーワードを使用します。
- マップを削除する場合は、シーケンス番号を指定しないで、**no** キーワードを使用します。

（「VLAN アクセス マップの設定および確認の例」（P.35-10）を参照）。

VLAN アクセス マップ シーケンスでの match コマンドの設定

VLAN アクセス マップ シーケンスに match コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップ シーケンスに match コマンドを設定します。
`Router(config-access-map)# no match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップ シーケンスから match コマンドを削除します。

VLAN アクセス マップ シーケンスに match コマンドを設定する場合、次の情報に注意してください。

- 1 つまたは複数の ACL を選択できます。
- WAN インターフェイスに付加された VACL は、標準または拡張 Cisco IOS IP ACL だけをサポートします。
- match コマンドを削除したり、match コマンド内の特定の ACL を削除したりする場合は、**no** キーワードを使用します。
- 名前付き MAC レイヤ ACL の詳細については、「MAC ACL の設定」（P.41-71）を参照してください。
- Cisco IOS ACL の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm

（「VLAN アクセス マップの設定および確認の例」（P.35-10）を参照）。

VLAN アクセス マップ シーケンスでの action コマンドの設定

VLAN アクセス マップ シーケンスに action コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# action {drop [log]} | {forward [capture]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスに action コマンドを設定します。
`Router(config-access-map)# no action {drop [log]} | {forward [capture]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスから action コマンドを削除します。

VLAN アクセス マップ シーケンスに action コマンドを設定する場合、次の情報に注意してください。

- パケットを廃棄、転送、転送してキャプチャ、またはリダイレクトするアクションを設定できます。
- WAN インターフェイスに適用される VACL は、転送してキャプチャするアクションだけをサポートします。WAN インターフェイスに適用された VACL は、廃棄、転送、またはリダイレクト アクションをサポートしません。
- 転送されたパケットも、設定済み Cisco IOS セキュリティ ACL による制約を受けます。
- **capture** アクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。**capture** アクションの詳細については、「キャプチャ ポートの設定」（P.35-11）を参照してください。
- WAN インターフェイスに適用された VACL は、**log** アクションをサポートしません。
- **log** アクションが指定されている場合、廃棄されたパケットがソフトウェアで記録されます。記録できるのは、廃棄された IP パケットだけです。
- **redirect** アクションを指定すると、物理インターフェイスまたは EtherChannel のいずれかのインターフェイスを 5 つまで指定できます。EtherChannel メンバまたは VLAN インターフェイスにパケットをリダイレクトするように指定することはできません。
- リダイレクト インターフェイスは、VACL アクセス マップが設定されている VLAN 内に存在する必要があります。
- Policy Feature Card（PFC; ポリシー フィーチャ カード）3 では、VACL が出力 SPAN 送信元ポートにトラフィックをリダイレクトした場合、SPAN は VACL リダイレクト トラフィックをコピーしません。
- PFC2 では、VACL が出力 SPAN 送信元ポートにトラフィックをリダイレクトした場合、SPAN は VACL リダイレクト トラフィックをコピーします。
- SPAN および Remote SPAN（RSPAN）宛先ポートは、VACL リダイレクト トラフィックを送信します。
- action コマンドを削除するか、または指定されたリダイレクト インターフェイスを削除する場合は、**no** キーワードを使用します。

（「VLAN アクセス マップの設定および確認の例」（P.35-10）を参照）。

VLAN アクセス マップの適用

VLAN アクセス マップを適用するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan filter map_name {vlan-list vlan_list | interface type[1] number[2] }`	指定した VLAN または WAN インターフェイスに VLAN アクセス マップを適用します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*。サブインターフェイスまたはチャネル グループ ディスクリプタを含むことができます。

VLAN アクセス マップを適用する場合、次の情報に注意してください。

- VLAN アクセス マップは、1 つまたは複数の VLAN または WAN インターフェイスに適用できます。
- *vlan_list* パラメータには単一の VLAN ID、カンマで区切った VLAN ID のリスト、または VLAN ID の範囲（*vlan_ID*-*vlan_ID*）を指定できます。
- VACL が適用された WAN インターフェイスを削除すると、インターフェイス上の VACL 設定も削除されます。
- 各 VLAN または WAN インターフェイスには、VLAN アクセス マップを 1 つだけ適用できます。
- VLAN に適用した VACL がアクティブになるのは、レイヤ 3 VLAN インターフェイスが設定されている VLAN に対してだけです。レイヤ 3 VLAN インターフェイスを持たない VLAN に VLAN アクセス マップを適用すると、VLAN アクセス マップをサポートするために、レイヤ 3 VLAN インターフェイスが、管理上のダウン状態で作成されます。
- VLAN に適用される VACL は、レイヤ 2 VLAN が存在しないか動作していない場合は非アクティブです。
- セカンダリ プライベート VLAN に VACL を適用することはできません。プライマリ プライベート VLAN に適用された VACL は、セカンダリ プライベート VLAN にも適用されます。
- VLAN または WAN インターフェイスから VLAN アクセス マップを消去する場合は、**no** キーワードを使用します。

（「VLAN アクセス マップの設定および確認の例」（P.35-10）を参照）。

VLAN アクセス マップの設定の確認

VLAN アクセス マップの設定を確認するには、次の作業を行います。

コマンド	目的
`Router# show vlan access-map [map_name]`	VLAN アクセス マップの内容を表示して、VLAN アクセス マップの設定を確認します。
`Router# show vlan filter [access-map map_name | vlan vlan_id | interface type[1] number[2] ]`	VACL と VLAN 間のマッピングの内容を表示して、VLAN アクセス マップの設定を確認します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*。サブインターフェイスまたはチャネル グループ ディスクリプタを含むことができます。

VLAN アクセス マップの設定および確認の例

net_10 および **any_host** という名前の IP ACL が、次のように定義されていると想定します。

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

次に、IP パケットを転送するよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送され、それ以外のすべての IP パケットはデフォルトの廃棄アクションによって廃棄されます。このマップは VLAN 12 ～ 16 に適用されます。

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

次に、IP パケットを廃棄および記録するよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは廃棄および記録され、それ以外のすべての IP パケットは転送されます。

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

次に、IP パケットを転送およびキャプチャするよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送およびキャプチャされ、それ以外のすべての IP パケットは廃棄されます。

```
Router(config)# vlan access-map mordred 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter mordred vlan-list 2, 4-6
```

キャプチャ ポートの設定

VACL フィルタリングされたトラフィックをキャプチャするよう設定されたポートを、「キャプチャ ポート」といいます。

（注）　キャプチャされたトラフィックに Institute of Electrical and Electronic Engineers（IEEE; 米国電気電子学会）802.1Q または Inter-Switch Link（ISL; スイッチ間リンク）タグを適用するには、キャプチャ ポートで無条件にトランクするように設定します（「ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-10）および「DTP を使用しないようにするためのレイヤ 2 トランクの設定」（P.10-11）を参照）。

キャプチャ ポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# switchport capture allowed vlan {add | all | except | remove} vlan_list`	（任意）宛先 VLAN 単位で、キャプチャされたトラフィックをフィルタリングします。デフォルトは、**all** です。
	`Router(config-if)# no switchport capture allowed vlan`	設定された宛先 VLAN リストを消去して、デフォルト値に戻します（**all**）。
ステップ 3	`Router(config-if)# switchport capture`	VACL フィルタリングされたトラフィックをキャプチャするよう、ポートを設定します。
	`Router(config-if)# no switchport capture`	インターフェイス上のキャプチャ機能をディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

キャプチャ ポートを設定する場合、次の情報に注意してください。

- 任意のポートをキャプチャ ポートとして設定できます。
- *vlan_list* パラメータには単一の VLAN ID、カンマで区切った VLAN ID のリスト、または VLAN ID の範囲（*vlan_ID-vlan_ID*）を指定できます。
- キャプチャされたトラフィックをカプセル化するには、**switchport trunk encapsulation** コマンドでキャプチャ ポートを設定してから（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.10-9）を参照）、**switchport capture** コマンドを入力します。
- キャプチャされたトラフィックをカプセル化しない場合は、**switchport mode access** コマンドでキャプチャ ポートを設定してから（「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」（P.10-16）を参照）、**switchport capture** コマンドを入力します。
- キャプチャ ポートは、出力トラフィックだけをサポートします。トラフィックは、キャプチャ ポートからスイッチに入ることができません。

次に、ファスト イーサネット インターフェイス 5/1 をキャプチャ ポートとして設定する例を示します。

```
Router(config)# interface gigabitEthernet 5/1
Router(config-if)# switchport capture
Router(config-if)# end
```

次に、VLAN アクセス マップの情報を表示する例を示します。

```
Router# show vlan access-map mordred
Vlan access-map "mordred"  10
        match: ip address net_10
        action: forward capture
Router#
```

次に、VACL と VLAN 間のマッピングを表示する例を示します。各 VACL マップでは、マップが設定されている VLAN、およびマップがアクティブである VLAN についての情報があります。VLAN 内にインターフェイスがない場合、VACL は、アクティブになりません。

```
Router# show vlan filter
VLAN Map mordred:
        Configured on VLANs:  2,4-6
            Active on VLANs:  2,4-6
Router#
```

VACL ログ機能の設定

VACL ログ機能が設定されているときに、次の状況で IP パケットが拒否されると、ログ メッセージが生成されます。

- 一致する最初のパケットを受信した場合
- 直前の 5 分間に、一致するパケットを受信した場合
- 5 分経過する前にスレッシュホールドに達している場合

ログ メッセージはフロー単位で生成されます。フローは、同じ IP アドレスおよびレイヤ 4（User Datagram Protocol（UDP）または TCP）ポート番号を持つパケットとして定義されます。ログ メッセージが生成されると、タイマーおよびパケット カウントがリセットされます。

VACL ログ機能には、次の制限事項が適用されます。

- リダイレクトされたパケットにはレート制限機能が適用されるので、VACL ログ カウンタが不正確になることがあります。
- 拒否された IP パケットだけが記録されます。

VACL ログ機能を設定するには、VLAN アクセス マップ サブモードの **action drop log** コマンド アクションを使用します（設定情報については、「VACL の設定」（P.35-5）を参照してください）。この作業をグローバル コンフィギュレーション モードで実行して、グローバル VACL ログ パラメータを指定します。

	コマンド	目的
ステップ 1	`Router(config)# vlan access-log maxflow` *max_number*	ログ テーブルのサイズを設定します。maxflow の値を 0 に設定すると、ログ テーブルの内容を削除できます。デフォルトは 500、有効範囲は 0 ～ 2048 です。ログ テーブルが満杯になると、新しいフローのパケットが記録されても、ソフトウェアによって廃棄されます。
ステップ 2	`Router(config)# vlan access-log ratelimit` *pps*	VACL ログ パケットの最大リダイレクト速度を設定します。デフォルトのパケット転送速度は 2000 パケット/秒、有効範囲は 0 ～ 5000 です。制限を超えたパケットは、ハードウェアによって廃棄されます。

	コマンド	目的
ステップ 3	`Router(config)# vlan access-log threshold pkt_count`	ログ スレッシュホールドを設定します。5 分経過する前にフローのスレッシュホールドに達すると、ログ メッセージが生成されます。デフォルトでは、スレッシュホールドは設定されていません。
ステップ 4	`Router(config)# exit`	VLAN アクセス マップ コンフィギュレーション モードを終了します。
ステップ 5	`Router# show vlan access-log config`	（任意）設定された VACL ログ プロパティを表示します。
ステップ 6	`Router# show vlan access-log flow protocol {{src_addr src_mask} | any | {host {hostname | host_ip}}} {{dst_addr dst_mask} | any | {host {hostname | host_ip}}} [vlan vlan_id]`	（任意）VACL ログ テーブルの内容を表示します。
ステップ 7	`Router# show vlan access-log statistics`	（任意）パケット数、メッセージ数などの統計情報を表示します。

次に、グローバル VACL ログ機能をハードウェア内で設定する例を示します。

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

CHAPTER 36

サービス拒絶（DoS）からの保護の設定

この章では、Catalyst 6500 シリーズ スイッチを Denial of Service（DoS; サービス拒絶）攻撃から保護する手順について説明します。この章で説明する内容は Catalyst 6500 シリーズ スイッチに固有のものであり、このマニュアルの「ネットワーク セキュリティの設定」の章で説明するネットワーク セキュリティ情報とその手順、および以下のマニュアルでのネットワーク セキュリティ情報とその手順を補完します。

- 次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
- 次の URL にある『*Cisco IOS Security Command Reference*』Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

この章で説明する内容は、次のとおりです。

DoS からの保護の機能概要

ここでは、DoS からの Catalyst 6500 シリーズ スイッチの保護の概要、およびいくつかの種類の DoS 攻撃シナリオについて説明します。

PFC2 での DoS からの保護

ここでは、Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）への DoS 攻撃に対して有効な対処方法についての情報を説明し、その設定例を示します。ここでは以下の保護手段について説明します。

セキュリティ ACL

Catalyst 6500 シリーズ スイッチでは、セキュリティ Access Control List（ACL; アクセス制御リスト）を使用することで、DoS パケットをハードウェア内で拒否できます。セキュリティ ACL は、ハードウェア内で TCAM によってトラフィックに適用されます。このトラフィックは、レイヤ 3 またはレイヤ 4 データを使用して簡単に識別されます。セキュリティ ACL は、DoS 攻撃を受ける前に予防措置として適用することも、攻撃が検出されたあとに適用することもできます。

次に、セキュリティ ACL を使用して DoS パケットを廃棄する例を示します。

```
Router# clear mls ip mod 9
Router# show mls ip mod 9
Displaying Netflow entries in module 9
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
192.168.0.0  192.168.1.0 0   :0      :0        0   : 0
1843         84778       2     02:30:17   L3 - Dynamic
192.168.1.0  192.168.0.0       0   :0      :0        0   : 0
➔ 2742416      126151136   2     02:30:17   L3 - Dynamic   <== Note: traffic flow identified
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no access-list 199
Router(config)# access-list 199 deny ip host 192.168.0.0 any
Router(config)# access-list 199 permit ip any any
Router(config)# interface g9/1
➔ Router(config-if)# ip access 199 in                  <======== Note: security ACL applied
Router(config-if)# end
Router#
1w6d: %SYS-5-CONFIG_I: Configured from console by console
Router# clear mls ip mod 9
```

```
Router# show mls ip mod 9
Displaying Netflow entries in module 9
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
192.168.0.0  192.168.1.0 0   :0      :0        0   : 0
1542         70932       2     02:31:56   L3 - Dynamic
192.168.1.0  192.168.0.0       0   :0      :0        0   : 0
0            0           2     02:31:56   L3 - Dynamic  <======== Note: hardware-forwarded
                                                        <======== Note: traffic stopped
Extended IP access list 199
    deny ip host 192.168.0.0 any (100 matches)
    permit ip any any
Router# show access-list 199
Extended IP access list 199
    deny ip host 192.168.0.0 any (103 matches
    permit ip any any
Router #
```

セキュリティ VACL

セキュリティ VACL は、レイヤ 2、レイヤ 3、およびレイヤ 4 情報に基づくセキュリティ強化ツールです。セキュリティ VACL によるパケット検索の結果は、許可（permit）、拒否（deny）、許可およびキャプチャ（permit and capture）、またはリダイレクト（redirect）のいずれかになります。セキュリティ VACL を特定の VLAN に関連付けると、トラフィックがこの VLAN に許可されるには、すべてのトラフィックにセキュリティ VACL による許可が必要になります。セキュリティ VACL はハードウェア内で適用されます。したがって、Catalyst 6500 シリーズ スイッチの VLAN にセキュリティ VACL を適用しても、パフォーマンス ペナルティは発生しません。

QoS ACL

QoS ACL を使用すると、セキュリティ ACL と異なり、フロー内のすべてのトラフィックへのアクセスを拒否することなく、トラフィック レートを制限できます。

次に、QoS ACL を使用して、スイッチに対する ping 攻撃を防止する例を示します。QoS ACL をすべてのインターフェイスに対して設定および適用することで、受信する ICMP パケットのレートを制限します。

```
Router# show ip ospf neighbors

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.122         1   FULL/BDR        00:00:30    6.6.6.122       Vlan46
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          11 00:06:07    4   200  0  6555
Router#                                                 <======== Note: ping attack starts
Router# show proc cpu | include CPU utilization
CPU utilization for five seconds: 99%/90%; one minute: 48%; five minutes: 25%
Router#
2w0d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from FULL to DOWN, Neighbor
Down: Dead timer expired
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-list 199 permit icmp any any echo
```

```
Router(config)# class-map match-any icmp
Router(config-cmap)# match access-group  199
Router(config-cmap)# exit
Router(config)# policy-map icmp
Router(config-pmap)# class icmp
Router(config-pmap-c)# police 96000 16000 16000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface range g4/1 - 9
Router(config-if-range)# service-policy input icmp          <======== Note: policy applied
Router(config-if-range)# end
2w0d: %SYS-5-CONFIG_I: Configured from console by console
2w0d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from LOADING to FULL, Loading
Done
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44        13 00:00:48    8     200  0  6565
Router#
```

FIB レート制限

（注）　PFC2 の CPU レート リミッタは、デフォルトでオフにされています。

Forwarding Information Base（FIB; 転送情報ベース）によるレート制限機能を使用すると、ソフトウェア処理の必要なすべてのパケットをレート制限できます。

次の例では、ローカルに接続したサブネット上の、存在しないホスト アドレス宛てのトラフィックを示します。通常は、Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に対して ARP 応答が返され、このトラフィックに対する FIB 隣接テーブルが実装されます。ただし、この宛先サブネットに対する FIB の隣接テーブルは、転送およびソフトウェア処理の必要なトラフィックを受信し続けます。このトラフィックにレート制限を適用することで、ソフトウェア処理のために転送されるトラフィック レートを、管理可能な量にまで制限できます。

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          11 00:00:26    8   200  0  6534
Router# show ip ospf neighbors

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.122         1   FULL/BDR        00:00:36    6.6.6.122       Vlan46
Router#                                                 <==================== Note: attack starts
Router# show arp | include 199.2.250.250
Internet  199.2.250.250           0   Incomplete      ARPA
Router#
1w6d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from FULL to DOWN, Neighbor Down: Dead
timer expired
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls rate-limit unicast cef receive 1000 <====== Note: traffic rate limited to 1000 pps
Router(config)# end
Router#
1w6d: %SYS-5-CONFIG_I: Configured from console by console
```

```
Router#
1w6d: %OSPF-5-ADJCHG: Process 100, Nbr 6.6.6.122 on Vlan46 from LOADING to FULL, Loading Done
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
0   4.4.4.122               Vl44          12 00:00:07   12   200  0  6536
Router#
```

トラフィック ストーム制御

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、ネットワーク設定の誤り、またはユーザによる DoS 攻撃の開始が原因となり、物理インターフェイス上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 ストームによって LAN ポートが中断されるのを防ぎます。トラフィック ストーム制御（トラフィック抑制とも呼ぶ）は、1 秒間のトラフィック ストーム制御インターバルにおいて受信するトラフィックのレベルをモニタします。このインターバルの間、設定済みのトラフィック ストーム制御レベルに対し、トラフィック レベルが比較されます。トラフィック ストーム制御レベルは、ポートの利用可能な帯域幅全体に対するパーセンテージです。各ポートには、すべてのタイプのトラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）用に使用されている単一のトラフィック ストーム制御レベルがあります。

トラフィック ストーム制御はインターフェイスに対して設定され、デフォルトではディセーブルにされています。次の設定例では、ファスト イーサネット インターフェイス 2/3 上で、レベル 20% のブロードキャスト アドレス ストーム制御をイネーブルにしています。1 秒間のトラフィック ストーム制御インターバルで、ブロードキャスト トラフィックが、設定されたレベルであるポートの有効帯域幅合計の 20% を超えると、このトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャスト トラフィックが廃棄されます。

```
Router(config-if)# storm-control broadcast level 20
```

Catalyst 6500 シリーズ スイッチは、すべての LAN ポートでブロードキャスト ストーム制御をサポートし、ギガビット イーサネット ポートではユニキャスト ストーム制御をサポートします。

2 つまたは 3 つの抑制モードを同時に設定する場合は、同じレベル設定が共有されます。ブロードキャスト抑制をイネーブルにした場合に、マルチキャスト抑制もイネーブルにし、そのスレッシュホールドを 70% に設定すると、ブロードキャスト抑制にもこの 70% の設定が適用されます。

トラフィック ストーム制御の設定の詳細については、第 39 章「トラフィック ストーム制御の設定」を参照してください。

ARP スロットリング

ARP スロットリングは、ハードウェア ベースの FIB および隣接エントリを自動的にインストールし、ARP 解決の実行時にパケットを廃棄するために使用します。これらのほとんどのパケットは廃棄されますが、このうち少数のパケットは Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）に送信されます（レート制限）。

uRPF チェック

unicast Reverse Path Forwarding（uRPF）チェックをイネーブルにすると、スプーフィングされた IP 送信元アドレスなど、確認可能な送信元 IP アドレスを持たないパケットが廃棄されます。送信元アドレスと、これが受信されたインターフェイスとが、スーパーバイザ エンジンの FIB テーブルと一致しているかどうかを確認するには、Cisco Express Forwarding（CEF）テーブルが使用されます。

インターフェイス上で uRPF チェックをイネーブルにすると（VLAN 単位）、受信パケットは逆引き参照によって CEF テーブルと比較されます。いずれかのリバース パス ルートから受信されたパケットは転送されます。受信パケットに対し、インターフェイス上にリバース パス ルートが 1 つも存在しない場合は、このパケットは uRPF チェックに失敗したことになります。このパケットは、uRPF チェックに失敗したトラフィックに ACL が適用されるかどうかに応じて廃棄または転送されます。CEF テーブルに ACL が指定されていない場合は、偽装パケットはただちに廃棄されます。

uRPF チェックの ACL は、uRPF チェックに失敗したパケットにのみ指定できます。この ACL は、パケットをただちに廃棄するか、または転送するかをチェックします。ACL による uRPF チェックは、ハードウェア内の PFC3 ではサポートされません。uRPF ACL で拒否されたパケットは、ハードウェア内で転送されます。許可されたパケットは CPU に送信されます。

PFC2 では、uRPF チェックはハードウェア内でサポートされますが、リターン パスは 1 つだけです。ただし、uRPF チェックに失敗し、適用された ACL によって転送されるすべてのパケットは、MSFC に送信およびレート制限され、ICMP 到達不能メッセージを生成します。これらの動作は、すべてソフトウェアによって制御されます。ハードウェアでの uRPF チェックは、最大 2 つのリターン パス（インターフェイス）を持つルートに対してサポートされ、インターフェイス グループが設定された場合は最大 6 つのリターン パス（2 つは FIB テーブルから、4 つはインターフェイス グループから）を持つルートに対してサポートされます。

TCP インターセプト

TCP インターセプトは、TCP トラフィックの受信者を、TCP SYN フラッディング DoS 攻撃から保護する機能です。通常の TCP 接続は、スリーウェイ ハンドシェイクによって開始されます。ホスト A はホスト B に、新たな TCP セッションの開始を要求する SYN 要求を送信します。ホスト B は SYN 要求の受信を伝える確認応答として、SYN ACK を送信します。さらに、ホスト B の SYN ACK に対してホスト A が ACK を返信し、セッションが開始されます。SYN フラッディング攻撃とは、ハッカーが到達不能なリターン アドレスによる接続要求でサーバを過負荷にすることによって発生します。この場合、スリーウェイ ハンドシェイクは決して完了することがなく、接続が確立されません。サーバ ホストが応答すべきセッション要求の量によっては、サーバ ホストの処理能力が限界を超えてしまい、この結果、正規のユーザが正規のサービス（Web サイト、E メール サーバなど）に接続できなくなる場合があります。

TCP インターセプトは、TCP 要求を代行受信および検証することで、SYN フラッディングを防止します。TCP インターセプトは以下のモードをサポートします。

- インターセプト モード - TCP インターセプト ソフトウェアは、拡張アクセス リストと一致するサーバ宛ての、クライアントからの TCP 同期（SYN）パケットを代行受信します。ソフトウェアは、宛先サーバに代わってクライアントと接続を確立します。これに成功すると、今度はクライアントに代わってサーバと接続を確立し、これらの 2 つの片側接続を透過的に接続します。到達不能ホストからの接続の試みが、サーバに到達することはありません。ソフトウェアは接続の間中、パケットの代行受信と転送を続行します。

  潜在的なハッカーから不正な要求があった場合は、ソフトウェアはハーフオープン状態の接続に対するアグレッシブ タイムアウト、および TCP 接続要求のスレッシュホールドを使用して宛先サーバを保護しつつ、有効な要求は引き続き許可します。TCP インターセプトを使用してネットワーク セキュリティ ポリシーを構築する場合は、すべての要求を代行受信するのか、あるいは特定ネットワークからの要求、または特定サーバ宛ての要求だけを代行受信するのかを選択できます。また、接続レートや、未完了接続に対するスレッシュホールドも設定できます。

- ウォッチ モード - ソフトウェアは、スイッチ経由で伝送される接続要求を受動的にモニタします。設定可能なインターバルにおいて接続が確立できなかった場合は、ソフトウェアが仲介し、要求された接続を中止します。

TCP インターセプトは、アクティブなインターセプト モードでも、パッシブなウォッチ モードでも使用できます。したがって、どちらのモードがネットワークに適するかを判断し、それに従ってネットワークを構成することが重要です。TCP インターセプトは、PFC2 および PFC3（全タイプ）においてハードウェア補助される機能です。アクティブ インターセプト モードで多数の送信元および宛先サーバを指定すると、CPU のオーバーランが生じる可能性があるので、クリティカルなサーバだけをアクティブ インターセプト モードで保護することを推奨します。

処理のデフォルト モードはインターセプト モードです。インターセプト モードでは、ソフトウェアは送られてくる個々の接続要求（SYN）をアクティブに代行受信し、サーバの代わりに SYN-ACK を返信してから、クライアントからの ACK を待機します。こうした前処理が完了すると、元の SYN がサーバに送信され、ソフトウェアはサーバとのスリーウェイ ハンドシェイクを行います。こうして 2 つの片側接続が、1 つに結合されます。

ウォッチ モードでは、接続要求はスイッチを通過してサーバに送信されますが、接続が確立するまで監視されます。30 秒間（この値は設定可能）のうちに接続が確立できない場合は、ソフトウェアはサーバにリセット命令を送り、サーバの状態を消去します。スイッチをウォッチ モードで設定すると、インターセプト モードほど CPU に負荷がかかりません。ウォッチ モードでは、CPU はチェックを行わず、2 つの片側接続を結合します。CPU は接続を受動的にモニタし、処理が実際に行われたあとで、失敗した接続に対処します。

TCP インターセプトはグローバルに設定します。これには、まず代行受信するトラフィックに対して拡張アクセス リストを作成してから、TCP インターセプト リストを作成します。代行受信するトラフィックのタイプは、以下のいずれかです。

- すべての要求
- 特定のネットワークから送信される要求のみ
- 特定のサーバ宛てに送信される要求のみ

次に、アクセス リストの送信元をすべて（any）と定義する例を示します。代行受信するパケットの送信元を正確に把握することは難しいため、ここでは送信元アドレスはフィルタリングしません。TCP SYN フラッド攻撃からの保護対象となる宛先サーバは指定します。アクセス リスト内のエントリと一致しないトラフィックは通過を許可され、それ以上のアクションは実行されません。

```
Router(config)# access-list 101 permit tcp any 10.1.1.1 0.0.0.255
Router(config)# ip tcp intercept list 101
```

表 36-1 は、TCP インターセプトの設定に使用するコマンドの一覧を示します。

表 36-1　TCP インターセプトの設定

コマンド	目的
Router(config)# **access-list** *access-list-number* {**deny** | **permit**} **tcp any** *destination destination-wildcard*	IP 拡張アクセス リストを定義します。
Router(config)# **ip tcp intercept list** *access-list-number*	TCP インターセプトをイネーブルにします。
Router(config)# **ip tcp intercept mode** {**intercept** | **watch**}	TCP インターセプト モードを設定します。
Router(config)# **ip tcp intercept drop-mode** {**oldest** | **random**}	廃棄モードを設定します。
Router(config)# **ip tcp intercept watch-timeout** *seconds*	接続確立状態に達するまでの許容時間を変更します。有効値の範囲は 1 ～ 2147483 秒です。

表 36-1　TCP インターセプトの設定 （続き）

コマンド	目的
Router(config)# **ip tcp intercept finrst-timeout** *seconds*	リセット要求（reset）または接続終了要求（FIN-exchange）を受信してから、接続を廃棄するまでの時間を変更します。有効値の範囲は 1 ～ 2147483 秒です。
Router(config)# **ip tcp intercept connection-timeout** *seconds*	何の動作も行われなくなったあと、ソフトウェアが接続を管理する時間を変更します。有効値の範囲は 1 ～ 2147483 秒です。
Router(config)# **ip tcp intercept max-incomplete low** *number*	ソフトウェアがアグレッシブ モードを終了する基準となる未完了接続数を定義します。有効値の範囲は 1 ～ 2147483647 秒です。
Router(config)# **ip tcp intercept max-incomplete high** *number*	ソフトウェアがアグレッシブ モードを開始するまでの、許容される未完了接続の最大数を定義します。有効値の範囲は 1 ～ 2147483647 秒です。
Router(config)# **ip tcp intercept one-minute low** *number*	ソフトウェアがアグレッシブ モードを終了する基準となる接続要求数を定義します。有効値の範囲は 1 ～ 2147483647 秒です。
Router(config)# **ip tcp intercept one-minute high** *number*	ソフトウェアがアグレッシブ モードを開始するまでの、最後の 1 分間のサンプリング期間中に受信する接続要求数を定義します。有効値の範囲は 1 ～ 2147483647 秒です。
Router# **show tcp intercept connections**	未完了接続と確立された接続を表示します。
Router# **show tcp intercept statistics**	TCP インターセプトの統計情報を表示します。

PFC2 のハードウェア ベース レート リミッタ

PFC2 では、ハードウェア ベースのレート リミッタを追加で使用できます。PFC2 は、新たなレート リミッタに対応する 4 つのレート リミッタ レジスタを備えています。これらはすべて、スイッチ上でグローバルに設定します。これらのレート リミッタ レジスタはレイヤ 3 転送エンジン（PFC）上にあり、使用可能なさまざまな設定済みレート リミッタと一致した各パケットに関する、レート制限情報の格納を行います。

4 つのレート リミッタ レジスタは、レイヤ 3 転送エンジン上のみに実装されているため、異なる複数のレート制限シナリオで、同一レジスタが強制的に共有される場合もあります。各レジスタは、先着順に割り当てられます。すべてのレジスタが使用されている場合、もう 1 つのレート リミッタを新たに設定する唯一の方法は、いずれか 1 つのレジスタを解放することです。

PFC2 で使用可能なハードウェア ベースのレート リミッタは、次のとおりです。

- 入力および出力 ACL ブリッジド パケット
- FIB 受信および FIB 収集
- VACL ログ
- レイヤ 3 機能

入出力 ACL ブリッジド パケット（ユニキャストのみ）

このレート リミッタは、入出力 ACL ブリッジの結果として MSFC に送信されたパケットをレート制限します。スイッチはこの機能を実現するため、TCAM ブリッジの結果を表す既存および新規の ACL TCAM エントリを、MSFC をポイントするレイヤ 3 リダイレクトの結果に変更します。TCAM エントリが、変更したレイヤ 3 リダイレクト レート制限の結果と一致するパケットは、ネットワーク管理者が CLI で設定した指示に従ってレート制限されます。入力値および出力値は、いずれも同一のレート リミッタ レジスタを共有するため、同じ値となります。ACL ブリッジの入出力レート制限をディセーブルにすると、レイヤ 3 リダイレクトによるレート制限の結果は、ブリッジの結果に変換されます。

入力または出力 ACL ブリッジド パケットのレート制限は、1 つのレート リミッタ レジスタを共有します。この機能をオンにすると、入力および出力 ACL にはいずれも、同じレート リミッタ値が使用されます。

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを 50000 pps（パケット/秒）に制限し、バースト値を 50 に制限します。

```
Router(config)# mls rate-limit unicast acl input 50000 50
```

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを、出力 ACL ブリッジの結果と同じレート（50000 pps、バースト値 50）に制限します。

```
Router(config)# mls rate-limit unicast acl output 50000 50
```

入力または出力のいずれかでレート リミッタの値が変更されると（両方がイネーブルになっている場合）、両方の値が新しい値に変更されます。次の例では、出力レートが 40000 pps に変更されます。

```
Router(config)# mls rate-limit unicast acl output 40000 50
```

show mls rate-limit コマンドを入力すると、ACL ブリッジド入力（ACL BRIDGED IN）および出力（ACL BRIDGED OUT）の値がどちらも 40000 pps に変わっていることを確認できます。

```
Router# sh mls rate-limit
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0% Time source is NTP,
10:32:15.584 PDT Fri Aug 5 2005

 Rate Limiter Type   Status       Packets/s
 -----------------   ----------   ---------
     ACL BRIDGE IN   Off                  -
    ACL BRIDGE OUT   Off                  -
   L3_SEC_FEATURES   Off                  -
          VACL LOG   Off                  -
       FIB RECEIVE   Off                  -
         FIB GLEAN   Off                  -
```

FIB（CEF）受信および FIB 収集（ユニキャストのみ）

FIB 受信レート リミッタの機能は、宛先アドレスとして MSFC IP を保持するすべてのパケットをレート制限することです。レート リミッタは、正しいフレーム（good frame）と不正なフレーム（bad frame）を区別しません。

（注） CoPP を使用する場合は、FIB 受信レート リミッタをイネーブルにしないでください。FIB 受信レート リミッタは、CoPP ポリシーを上書きします。

次の例では、トラフィックを 25000 pps、およびバースト値 60 にレート制限します。

```
Router(config)# mls rate-limit unicast cef receive 25000 60
```

FIB 収集レート リミッタは ARP トラフィックを制限しません。しかし、アドレス解決（ARP）を必要とし、MSFC に送信されるトラフィックをレート制限する機能を備えます。この状況は、ポートに送られたトラフィックに含まれるホスト アドレスが、MSFC にローカル接続されているサブネット上のアドレスであり、この宛先ホストに対する ARP エントリが存在しない場合に発生します。この場合、この宛先ホストの MAC アドレスに対しては、直接接続されているサブネットが不明であるため、このサブネット上のどのホストからも回答がありません。したがって、[glean] 隣接が該当し、トラフィックは MSFC に直接送られ、ここで ARP 解決が行われます。このレート リミッタは、このような ARP 要求によって CPU を過負荷にする攻撃の可能性を制限します。

次の例では、MSFC に送信されるトラフィックを 20000 pps、およびバースト値 60 に制限します。

```
Router(config)# mls rate-limit unicast cef glean 20000 60
```

VACL ログ（ユニキャストのみ）

VLAN-ACL ロギングの結果によって MSFC に送信されたパケットをレート制限すると、ロギング タスクによって CPU が過負荷になることを防止できます。VACL はハードウェア処理されますが、MSFC によるロギングが行われます。スイッチで VACL ロギングを設定しておくと、VACL で拒否された IP パケットに対するログ メッセージが生成されます。

次の例では、ロギング要求を 5000 pps（このレート リミッタの有効範囲は 10 ～ 5000 pps）に制限します。

```
Router(config)# mls rate-limit unicast acl vacl-log 5000
```

レイヤ 3 セキュリティ機能（ユニキャストのみ）

いくつかのセキュリティ機能では、パケットはまず MSFC に送信されてから処理されます。このようなセキュリティ機能では、MSFC に送信されるパケットの数をレート制限することで、過負荷の可能性を抑える必要があります。これは、認証プロキシ（auth-proxy）、IPSEC、検査などのセキュリティ機能です。

認証プロキシは、入力ユーザまたは出力ユーザ、またはその両方の認証に使用されます。通常これらのユーザはアクセス リストによってブロックされますが、認証プロキシを使用すると、ユーザはブラウザを開いてファイアウォールを通過し、IP アドレスに基づき Terminal Access Controller Access Control System Plus（TACACS+）または RADIUS サーバの認証を受けることができます。このサーバは追加のアクセス リスト エントリをスイッチに渡し、認証を受けたユーザの通過を許可します。これらの ACL はソフトウェア内で保存および処理されます。このため、認証プロキシを使用するユーザ数が多すぎると、MSFC が過負荷になるおそれがあります。このような場合にレート制限を行うと効果的です。

IPSec および検査も MSFC によって実行されるので、状況によってはレート制限が必要です。レイヤ 3 セキュリティ機能レート リミッタをイネーブルにすると、認証プロキシ、IPSec、および検証すべてが同時にイネーブルになります。

次の例では、セキュリティ機能を 100000 pps、およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit unicast ip features 100000 10
```

PFC3 での DoS からの保護

ここでは、Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）への DoS 攻撃に対して有効な対処方法についての情報を提供し、その設定例を示します。PFC3 は、次の方法を使用して、DoS 攻撃に対する多層防御を実現します。

- CPU レート リミッタ - トラフィックの種類を制御します。
- CoPP - コントロール プレーンのトラフィックをフィルタおよびレート制限します。CoPP の詳細については、「CoPP の機能概要」（P.36-30）を参照してください。

ここでは、PFC3 での DoS からの保護について説明します。

セキュリティ ACL および VACL

ネットワークが実際に DoS 攻撃を受けた場合は、ターゲットに到達する前に DoS パケットを廃棄するための有効な手段として、ACL を使用できます。セキュリティ ACL は、特定のホストから攻撃が検出されたときに使用します。次の例では、ホスト 10.1.1.10 と、このホストからのすべてのトラフィックを拒否します。

```
Router(config)# access-list 101 deny ip host 10.1.1.10 any
Router(config)# access-list 101 permit ip any any
```

また、セキュリティ ACL はアドレスのスプーフィングも防止します。たとえば、ネットワークの内側、およびインターネットをポイントするスイッチインターフェイスの内側に、A という送信元アドレスがあるとします。この場合は、スイッチのインターネット インターフェイスに、送信元 A（内部アドレス）からのすべてのアドレスを拒否する入力 ACL を適用します。これで、内部のこの送信元アドレスを偽装する攻撃を防止できます。このようなパケットがスイッチインターフェイスに到達すると、このパケットは ACL と一致するため、被害が発生する前に廃棄されます。

Catalyst 6500 シリーズ スイッチとともに Cisco Intrusion Detection Module（CIDM）を使用すると、検知エンジンが攻撃を検知した時点で、セキュリティ ACL をダイナミックにインストールできます。

VACL は、レイヤ 2、レイヤ 3、およびレイヤ 4 情報に基づくセキュリティ強化ツールです。VACL によるパケット検索の結果は、許可（permit）、拒否（deny）、許可およびキャプチャ（permit and capture）、またはリダイレクト（redirect）のいずれかになります。VACL を特定の VLAN に関連付けると、トラフィックがこの VLAN に許可されるには、すべてのトラフィックが VACL によって許可されなければならなくなります。VACL はハードウェア内で適用されます。したがって Catalyst 6500 シリーズ スイッチの VLAN に VACL を適用しても、パフォーマンス ペナルティは発生しません。

QoS レート制限

QoS ACL は、MSFC3 によって処理される、特定の種類のトラフィックの量を制限します。MSFC に対して DoS 攻撃が開始されると、QoS ACL は DoS トラフィックが MSFC データ パスに到達し、輻輳を防ぎます。PFC3 は QoS をハードウェア内で実行します。この仕組みは、DoS トラフィックを制限して（DoS トラフィックの検知後）、スイッチが MSFC に影響を与えることを防ぐ上で効果的です。

たとえば、ネットワークが ping-of-death や smurf 攻撃などを受けた場合、管理者はこの DoS 攻撃に対処するため ICMP トラフィックをレート制限する必要がありますが、同時に正規のトラフィックのプロセッサ処理、または MSFC やホストへの転送を許可する必要があります。このレート制限は、レート制限の必要な個々のフローに設定し、レート制限ポリシー アクションをインターフェイスに適用する必要があります。

次の例に示すアクセス リスト 101 は、すべての送信元からすべての宛先にトラフィックとして流れる ping（エコー）ICMP メッセージを許可および識別します。ポリシー マップ内では、ポリシー ルールによって指定の Committed Information Rate（CIR; 認定情報速度）およびバースト値（96000 bps、16000 bps）を定義し、シャーシを通過する ping（ICMP）トラフィックをレート制限します。このポリシー マップは、インターフェイスまたは VLAN に適用されます。ping トラフィックがポリシー マップの適用された VLAN またはインターフェイスで指定のレートを超えると、このトラフィックはマークダウン マップに従って廃棄されます（この例では、通常のバースト設定に対するマークダウン マップは掲載していません）。

```
Router(config)# access-list 101 permit icmp any any echo
Router(config)# class-map match-any icmp_class
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map icmp_policer
Router(config-pmap)# class icmp_class
Router(config-pmap-c)# police 96000 16000 conform-action transmit exceed-action
policed-dscp-transmit drop
```

```
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

uRPF チェック

unicast Reverse Path Forwarding（uRPF）チェックをイネーブルにすると、スプーフィングされた IP 送信元アドレスなど、確認可能な送信元 IP アドレスを持たないパケットが廃棄されます。送信元アドレスと、これが受信されたインターフェイスとが、スーパーバイザ エンジンの FIB テーブルと一致しているかどうかを確認するには、Cisco Express Forwarding（CEF）テーブルが使用されます。

インターフェイス上で uRPF チェックをイネーブルにすると（VLAN 単位）、受信パケットは逆引き参照によって CEF テーブルと比較されます。いずれかのリバース パス ルートから受信されたパケットは転送されます。受信パケットに対し、インターフェイス上にリバース パス ルートが 1 つも存在しない場合は、このパケットは uRPF チェックに失敗したことになります。このパケットは、uRPF チェックに失敗したトラフィックに ACL が適用されるかどうかに応じて廃棄または転送されます。CEF テーブルに ACL が指定されていない場合は、偽装パケットはただちに廃棄されます。

uRPF チェックの ACL は、uRPF チェックに失敗したパケットにのみ指定できます。この ACL は、パケットをただちに廃棄するか、または転送するかをチェックします。ACL による uRPF チェックは、ハードウェア内の PFC3 ではサポートされません。uRPF ACL で拒否されたパケットは、ハードウェア内で転送されます。許可されたパケットは CPU に送信されます。

PFC3 では、uRPF チェックはハードウェア内でサポートされます。PFC2 でもハードウェア内でサポートされますが、リターン パスは 1 つだけです。ただし、uRPF チェックに失敗し、適用された ACL によって転送されるすべてのパケットは、MSFC に送信およびレート制限され、ICMP 到達不能メッセージを生成します。これらの動作は、すべてソフトウェアによって制御されます。ハードウェアでの uRPF チェックは、最大 2 つのリターン パス（インターフェイス）を持つルートに対してサポートされ、インターフェイス グループが設定された場合は最大 6 つのリターン パス（2 つは FIB テーブルから、4 つはインターフェイス グループから）を持つルートに対してサポートされます。

トラフィック ストーム制御

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、ネットワーク設定の誤り、またはユーザによる DoS 攻撃の開始が原因となり、物理インターフェイス上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 ストームによって LAN ポートが中断されるのを防ぎます。トラフィック ストーム制御（トラフィック抑制とも呼ぶ）は、1 秒間のトラフィック ストーム制御インターバルにおいて受信するトラフィックのレベルをモニタします。このインターバルの間、設定済みのトラフィック ストーム制御レベルに対し、トラフィック レベルが比較されます。トラフィック ストーム制御レベルは、ポートの利用可能な帯域幅全体に対するパーセンテージです。各ポートには、すべてのタイプのトラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）用に使用されている単一のトラフィック ストーム制御レベルがあります。

トラフィック ストーム制御はインターフェイスに対して設定され、デフォルトではディセーブルにされています。次の設定例では、ファスト イーサネット インターフェイス 2/3 上で、レベル 20% のブロードキャスト アドレス ストーム制御をイネーブルにしています。1 秒間のトラフィック ストーム制御インターバルで、ブロードキャスト トラフィックが、設定されたレベルであるポートの有効帯域幅合計の 20% を超えると、このトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャスト トラフィックが廃棄されます。

```
Router(config-if)# storm-control broadcast level 20
```

Catalyst 6500 シリーズ スイッチは、すべての LAN ポートでブロードキャスト ストーム制御をサポートし、ギガビット イーサネット ポートではユニキャスト ストーム制御をサポートします。

2 つまたは 3 つの抑制モードを同時に設定する場合は、同じレベル設定が共有されます。ブロードキャスト抑制をイネーブルにした場合に、マルチキャスト抑制もイネーブルにし、そのスレッシュホールドを 70% に設定すると、ブロードキャスト抑制にもこの 70% の設定が適用されます。

SYN 攻撃を受けたネットワーク

SYN 攻撃を受けたネットワークは、簡単に見分けることができます。ターゲット ホストは極端に低速になるか、クラッシュするか、または処理が中断されます。ターゲット ホストから返されたトラフィックによって MSFC に問題が生じることもあります。これは、リターン トラフィックが、元のパケットからランダムに抽出された送信元アドレスに送信され、「本物」の IP トラフィックのローカル性が失われることで、ルート キャッシュまたは CEF テーブルでオーバーフローが生じる可能性があるためです。

ネットワークが SYN 攻撃を受けると、TCP インターセプト機能がアグレッシブな防御モードに変わります。スイッチ上でアグレッシブな動作が開始および終了するタイミングは、次の 2 つの要素によって決定されます。

- 未完了接続の合計数
- 最後の 1 分間のサンプリング期間における接続要求数

両方の要素には、最小値と最大値の両方を設定します。

未完了接続の数が 1,100 を超えると、または最後の 1 分間の接続数が 1,100 に達すると、新たな接続が確立されるたびに、最も古い部分接続（ランダム接続）が削除されるようになります。これはデフォルト値であり、変更できます。いずれかのスレッシュホールドが超過すると、サーバが攻撃を受けたと見なされ、TCP インターセプト機能はアグレッシブ モードに変わり、以下が行われます。

- 新たに接続が確立するたびに、最も古い部分接続（ランダムな部分接続）が削除されます。
- 最初の再送信タイムアウトが半減されて 0.5 秒となり、この結果、接続の確立を試みる合計時間も半減します。
- ウォッチ モードでは、ウォッチ タイムアウトも半減されます。

（注） 設定した最小値を両方のスレッシュホールドが下回ると、アグレッシブ モードは終了します（デフォルト値はいずれも 900）。TCP インターセプト設定の詳細については、表 36-1 を参照してください。

TCP フローは、PFC2 および PFC3（すべての PFC3 タイプ）においてハードウェア補助される機能です。

ARP ポリシング

悪意あるユーザが攻撃を仕掛ける際、ルーティング プロトコルや ARP パケットなどの制御パケットによって、MSFC CPU を過負荷にしようと試みる場合があります。このような特殊な制御パケットは、特定のルーティング プロトコルおよび ARP ポリシング機能によって、ハードウェアでレート制限することができます。これは、**mls qos protocol** コマンドによって設定します。RIP、BGP、LDP、OSPF、IS-IS、IGRP、EIGRP といったルーティング プロトコルがサポートされます。たとえば **mls qos protocol arp police 32000** というコマンドは、ARP パケットをハードウェア内で 32,000 bps にレート制限します。このポリシング機能は、ラインレート ARP 攻撃などの攻撃から MSFC CPU を効果的に保護しますが、スイッチへのルーティング プロトコルおよび ARP パケットのポリシングだけに留まらず、CoPP より低い粒度で機器を通過するトラフィックもポリシングします。

ポリシング メカニズムは、ポリシング回避メカニズムとルート設定を共有します。ポリシング回避メカニズムは、QoS ポリサーに到達したルーティング プロトコルおよび ARP パケットに対し、ネットワークの通過を許可します。このメカニズムを設定するには、**mls qos protocol** *protocol* **pass-through** コマンドを使用します。

次の例では、ARP ポリシングで使用可能なプロトコルを一覧表示する方法を示します。

```
Router(config)# mls qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp
```

次の例では、**mls qos protocol arp** コマンドで使用可能なキーワードを一覧表示する例を示します。

```
Router(config)# mls qos protocol arp ?
  pass-through  pass-through keyword
  police        police keyword
  precedence    change ip-precedence(used to map the dscp to cos value)
```

推奨されるレート リミッタ設定

レート リミッタは、次のように設定することを推奨します。

- DoS 攻撃で使用される可能性が最も高い種類のトラフィックに対し、レート リミッタをイネーブルにします。
- VACL ロギングを設定していない場合は、VACL ロギングにレート リミッタを使用しないでください。
- ハードウェア転送をサポートするプラットフォーム（Catalyst 6500 シリーズ スイッチなど）では、リダイレクトの必要性が少なくされているため、リダイレクトをディセーブルにします。
- ハードウェア転送をサポートするプラットフォーム（Catalyst 6500 シリーズ スイッチなど）では、到達不能メッセージの必要性が少なくされているため、到達不能レート リミッタをディセーブルにします。
- すべてのインターフェイスの MTU が同じである場合は、MTU レート リミッタをイネーブルにしないでください。
- レイヤ 2 Protocol Data Unit（PDU; プロトコル データ ユニット）レート リミッタを設定する場合は、次の点に注意してください。
  - 有効な PDU の予測値（可能な値）を計算し、この値を 2 倍または 3 倍にします。
  - PDU には、BPDU、DTP、VTP、PAgP、LACP、UDLD などが含まれます。
  - 各レート リミッタは、正しいフレーム（good frame）と不正なフレーム（bad frame）を区別しません。

PFC3 のハードウェア ベース レート リミッタ

PFC3 では、ハードウェア ベースのレート リミッタを追加で使用できます。PFC3 は、新たなレート リミッタに対応する 8 つのレート リミッタ レジスタを備えています。これらはすべて、スイッチ上でグローバルに設定します。これらのレート リミッタ レジスタはレイヤ 3 転送エンジン（PFC）上にあり、使用可能なさまざまな設定済みレート リミッタと一致した各パケットに関する、レート制限情報の格納を行います。

8 つのレート リミッタ レジスタは、PFC3 に実装されているため、異なる複数のレート制限シナリオで、同一レジスタが強制的に共有される場合もあります。各レジスタは、先着順に割り当てられます。すべてのレジスタが使用されている場合、もう 1 つのレート リミッタを新たに設定する唯一の方法は、いずれか 1 つのレジスタを解放することです。

PFC3 で使用可能なハードウェア ベースのレート リミッタは、次のとおりです。

- 入力および出力 ACL ブリッジド パケット
- uRPF チェックの失敗
- FIB 受信
- FIB 収集
- レイヤ 3 セキュリティ機能
- ICMP リダイレクト
- ICMP 到達不能（ACL 廃棄）
- ルートなし（FIB 不一致）
- VACL ログ
- TTL 失敗
- MTU 失敗
- マルチキャスト IPv4
- マルチキャスト IPv6

入出力 ACL ブリッジド パケット（ユニキャストのみ）

このレート リミッタは、入出力 ACL ブリッジの結果として MSFC に送信されたパケットをレート制限します。スイッチはこの機能を実現するため、TCAM ブリッジの結果を表す既存および新規の ACL TCAM エントリを、MSFC をポイントするレイヤ 3 リダイレクトの結果に変更します。TCAM エントリが、変更したレイヤ 3 リダイレクト レート制限の結果と一致するパケットは、ネットワーク管理者が CLI で設定した指示に従ってレート制限されます。入力値および出力値は、いずれも同一のレート リミッタ レジスタを共有するため、同じ値となります。ACL ブリッジの入出力レート制限をディセーブルにすると、レイヤ 3 リダイレクトによるレート制限の結果は、ブリッジの結果に変換されます。

入力または出力 ACL ブリッジド パケットのレート制限は、1 つのレート リミッタ レジスタを共有します。この機能をオンにすると、入力および出力 ACL にはいずれも、同じレート リミッタ値が使用されます。

バースト値は、1 度のバーストで許可されるパケット数を制限します。許可される個々のパケットは、それぞれ 1 つのトークンを使用します。1 つのパケットに対し 1 つのトークンが使用可能である必要があります。1 ミリ秒ごとに 1 つのトークンが生成されます。パケットが送られて来ないと、トークンは最大バースト値まで蓄積されます。たとえば、バースト値を 50 に設定している場合は、スイッチは最大 50 のトークンを蓄積でき、50 パケットのバーストを吸収できます。

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを 50000 pps（パケット/秒）に制限し、バースト値を 50 に制限します。

```
Router(config)# mls rate-limit unicast acl input 50000 50
```

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを、出力 ACL ブリッジの結果と同じレート（50000 pps、バースト値 50）に制限します。

```
Router(config)# mls rate-limit unicast acl output 50000 50
```

入力または出力のいずれかでレート リミッタの値が変更されると（両方がイネーブルになっている場合）、両方の値が新しい値に変更されます。次の例では、出力レートが 40000 pps に変更されます。

```
Router(config)# mls rate-limit unicast acl output 40000 50
```

show mls rate-limit コマンドを入力すると、ACL ブリッジド入力（ACL BRIDGED IN）および出力（ACL BRIDGED OUT）の値がどちらも 40000 pps に変わっていることを確認できます。

```
Router# show mls rate-limit
  Rate Limiter Type       Status      Packets/s   Burst
---------------------   ----------    ---------   -----
MCAST NON RPF           Off           -           -
MCAST DFLT ADJ          On            100000      100
MCAST DIRECT CON        Off           -           -
ACL BRIDGED IN          On            40000       50
ACL BRIDGED OUT         On            40000       50
IP FEATURES             Off
…
```

uRPF チェックの失敗

uRPF チェック失敗のレート リミッタを使用すると、uRPF チェックに失敗したために MSFC に送信する必要のあるパケットのレートを設定できます。uRPF チェックは、インターフェイスの受信したパケットが有効な送信元からのものであるかどうかを検証する機能です。これにより、偽装アドレスを使用するユーザからの DoS 攻撃の潜在的な脅威を最小にできます。uRPF チェックに失敗した偽装パケットは、MSFC に送信されることがあります。uRPF チェック レート リミッタを使用すると、uRPF チェックの失敗が発生した場合に、MSFC CPU にブリッジされる 1 秒あたりのパケット数をレート制限できます。

次の例では、uRPF チェックに失敗し、MSFC に送信されるパケットを、100000 pps およびバースト パケット 100 にレート制限します。

```
Router(config)# mls rate-limit unicast ip rpf-failure 100000 100
```

TTL 失敗

このレート リミッタは、Time to Live（TTL）チェックに失敗したために MSFC に送信されるパケットをレート制限します。次の例の **all** キーワードからもわかるように、このレート リミッタはマルチキャストおよびユニキャスト トラフィックの両方に適用されます。

（注）　TTL 失敗のレート リミッタは、IPv6 マルチキャストではサポートされません。

次の例では、TTL に失敗したパケットを 70000 pps、およびバースト値 150 にレート制限します。

```
Router(config)# mls rate-limit all ttl-failure 70000 150
```

ICMP 到達不能（ユニキャストのみ）

ICMP 到達不能攻撃では、攻撃対象の装置（この場合は MSFC）からは到達できない宛先アドレスを持つパケットを大量に送りつけることで、この装置を過負荷にします。ICMP 到達不能レート リミッタを使用すると、到達不能なアドレスを持ち、MSFC に送信されるパケットをレート制限できます。

次の例では、ACL 廃棄によって MSFC に送信されるパケットを、10000 pps および バースト値 100 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable acl-drop 10000 100
```

次の例では、FIB との不一致によって到達不能 ICMP メッセージの生成が必要となるパケットを、80000 pps および バースト値 70 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable no-route 80000 70
```

ICMP 到達不能（ルートなし）、ICMP 到達不能（ACL 廃棄）、IP エラー、および IP RPF 失敗の 4 つのレート リミッタは、同一のレート リミッタ レジスタを共有します。このいずれかのリミッタをイネーブルにすると、4 つのリミッタすべては同じ値を共有し、状況によっては同じ状態を共有します（ON/ON/ON など）。レート リミッタの内容を確認すると、このレジスタのメンバが別の機能の設定によってイネーブルにされている場合は、ステータスは ON ではなく ON-Sharing と表示されます。ただし、TTL 失敗のレート リミッタは例外です。この機能を手動でイネーブルにしている場合は、この値はレジスタ内の他のメンバと同じ値を共有します。

FIB（CEF）受信（ユニキャストのみ）

FIB 受信レート リミッタの機能は、宛先アドレスとして MSFC IP を保持するすべてのパケットをレート制限することです。レート リミッタは、正しいフレーム（good frame）と不正なフレーム（bad frame）を区別しません。

（注） CoPP を使用する場合は、FIB 受信レート リミッタをイネーブルにしないでください。FIB 受信レート リミッタは、CoPP ポリシーを上書きします。

次の例では、トラフィックを 25000 pps、およびバースト値 60 にレート制限します。

```
Router(config)# mls rate-limit unicast cef receive 25000 60
```

FIB 収集（ユニキャストのみ）

FIB 収集レート リミッタは ARP トラフィックを制限しません。しかし、アドレス解決（ARP）を必要とし、MSFC に送信されるトラフィックをレート制限する機能を備えます。この状況は、ポートに送られたトラフィックに含まれるホスト アドレスが、MSFC にローカル接続されているサブネット上のアドレスであり、この宛先ホストに対する ARP エントリが存在しない場合に発生します。この場合、この宛先ホストの MAC アドレスに対しては、直接接続されているサブネットが不明であるため、このサブネット上のどのホストからも回答がありません。したがって、[glean] 隣接が該当し、トラフィックは MSFC に直接送られ、ここで ARP 解決が行われます。このレート リミッタは、このような ARP 要求によって CPU を過負荷にする攻撃の可能性を制限します。

次の例では、MSFC に送信されるトラフィックを 20000 pps、およびバースト値 60 に制限します。

```
Router(config)# mls rate-limit unicast cef glean 20000 60
```

レイヤ 3 セキュリティ機能（ユニキャストのみ）

いくつかのセキュリティ機能では、パケットはまず MSFC に送信されてから処理されます。このようなセキュリティ機能では、MSFC に送信されるパケットの数をレート制限することで、過負荷の可能性を抑える必要があります。これは、認証プロキシ（auth-proxy）、IPSEC、検査などのセキュリティ機能です。

認証プロキシは、入力ユーザまたは出力ユーザ、またはその両方の認証に使用されます。通常これらのユーザはアクセス リストによってブロックされますが、認証プロキシを使用すると、ユーザはブラウザを開いてファイアウォールを通過し、IP アドレスに基づき Terminal Access Controller Access Control System Plus（TACACS+）または RADIUS サーバの認証を受けることができます。このサーバは追加のアクセス リスト エントリをスイッチに渡し、認証を受けたユーザの通過を許可します。これらの ACL はソフトウェア内で保存および処理されます。このため、認証プロキシを使用するユーザ数が多すぎると、MSFC が過負荷になるおそれがあります。このような場合にレート制限を行うと効果的です。

IPSec および検査も MSFC によって実行されるので、状況によってはレート制限が必要です。レイヤ 3 セキュリティ機能レート リミッタをイネーブルにすると、認証プロキシ、IPSec、および検証すべてが同時にイネーブルになります。

次の例では、セキュリティ機能を 100000 pps、およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit unicast ip features 100000 10
```

ICMP リダイレクト（ユニキャストのみ）

ICMP リダイレクト レート リミッタを使用すると、ICMP トラフィックをレート制限できます。たとえば、最適化されていないスイッチを経由してホストがパケットを送信すると、MSFC はこのホストに対し、送信パスを修正するように ICMP リダイレクト メッセージを送信します。このトラフィックが連続的に発生する場合、レート制限を行わないと、MSFC は ICMP リダイレクト メッセージを連続的に生成します。

次の例では、ICMP リダイレクトを 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 20000 20
```

VACL ログ（ユニキャストのみ）

VLAN-ACL ロギングの結果によって MSFC に送信されたパケットをレート制限すると、ロギング タスクによって CPU が過負荷になることを防止できます。VACL はハードウェア処理されますが、MSFC によるロギングが行われます。スイッチで VACL ロギングを設定しておくと、VACL で拒否された IP パケットに対するログ メッセージが生成されます。

次の例では、ロギング要求を 5000 pps（このレート リミッタの有効範囲は 10 ～ 5000 pps）に制限します。

```
Router(config)# mls rate-limit unicast acl vacl-log 5000
```

MTU 失敗

MTU 失敗のレート リミッタは TTL 失敗のレート リミッタと似ており、ユニキャストおよびマルチキャスト トラフィックの両方でサポートされます。MTU チェックに失敗したパケットは、MSFC CPU に送信されます。これにより、MSFC が過負荷になることがあります。

次の例では、MTU チェックに失敗し、MSFC に送信されるパケットを、10000 pps およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit all mtu 10000 10
```

レイヤ 2 マルチキャスト IGMP スヌーピング

Internet Group Management Protocol（IGMP）スヌーピング レート リミッタは、スーパーバイザ エンジン宛てのレイヤ 2 IGMP パケットの数を制限します。IGMP スヌーピングは、ホストとスーパーバイザ エンジン間の IGMP メッセージを待ち受けます。Catalyst 6500 シリーズ スイッチが truncated モードで動作している場合は、レイヤ 2 PDU レート リミッタはイネーブルにできません。ファブリック対応モジュールとファブリック非対応モジュールの両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの初めの 64 バイト）を送信します。

次の例では、IGMP スヌーピング トラフィックをレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

レイヤ 2 PDU

レイヤ 2 PDU レート リミッタを使用すると、MSFC CPU ではなくスーパーバイザ エンジン宛てに送信されたレイヤ 2 PDU プロトコル パケット（BPDU、DTP、PAgP、CDP、STP、および VTP パケット）の数をレート制限できます。Catalyst 6500 シリーズ スイッチが truncated モードで動作している場合は、レイヤ 2 PDU レート リミッタはイネーブルにできません。ファブリック対応モジュールとファブリック非対応モジュールの両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの初めの 64 バイト）を送信します。

次の例では、レイヤ 2 PDU を 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit layer2 pdu 20000 20
```

レイヤ 2 プロトコル トンネリング

このレート リミッタは、スーパーバイザ エンジン宛てのレイヤ 2 プロトコル トンネリング パケット（制御 PDU、CDP、STP、および VTP パケット）をレート制限します。これらのパケットはソフトウェアによってカプセル化（PDU 内の宛先 MAC アドレスを書き換え）されてから、専用のマルチキャスト アドレス（01-00-0c-cd-cd-d0）に転送されます。Catalyst 6500 シリーズ スイッチが truncated モードで動作している場合は、レイヤ 2 PDU レート リミッタはイネーブルにできません。ファブリック対応モジュールとファブリック非対応モジュールの両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの初めの 64 バイト）を送信します。

次の例では、レイヤ 2 プロトコル トンネリング パケットを 10000 pps、およびバースト パケット 10 にレート制限します。

```
Router(config)# mls rate-limit layer2 l2pt 10000 10
```

IP エラー

このレート リミッタは、IP チェックサム エラーおよび長さのエラーが生じたパケットを制限します。PFC3 に到達したパケットで、IP チェックサム エラーまたは長さの整合性エラーが発生している場合は、このパケットは追加処理のために MSFC に送信される必要があります。このように形式に誤りのあるパケットは、攻撃者によって DoS 攻撃の実行に悪用されることがありますが、ネットワーク管理者はこのようなパケットのレートを設定することで、制御パスを保護できます。

次の例では、IP エラーの生じたパケットを 1000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit unicast ip errors 1000 20
```

IPv4 マルチキャスト

このレート リミッタは、IPv4 マルチキャスト パケットを制限します。このレート リミッタでは、ハードウェア内のデータ パスから、ソフトウェア内のデータ パスまで送信されたパケットをレート制限できます。これを使用することで、ソフトウェア内の制御パスが輻輳することを防止し、設定したレートを超えたトラフィックを廃棄できます。IPv4 マルチキャスト レート リミッタは、設定可能な 3 つのレート リミッタから構成されます。FIB 不一致に対するレート リミッタ、マルチキャストで部分的にスイッチされるフローのレート リミッタ、およびマルチキャスト直接接続レート リミッタです。

FIB 不一致に対するレート リミッタを使用すると、mroute テーブル内のエントリと一致しないマルチキャスト トラフィックをレート制限できます。

部分的にスイッチされたフローに対するレート リミッタを使用すると、転送および複製のために MSFC3 宛てに送信されるフローをレート制限できます。マルチキャスト トラフィック フローにおいて、少なくとも 1 つの発信レイヤ 3 インターフェイスが多層的にスイッチングされ、少なくとも 1 つの発信インターフェイスが多層的にスイッチングされていない場合（ハードウェア スイッチの H ビットが設定されていない）は、このフローは部分的にスイッチングされたフロー、つまりパーシャル SC（パーシャル ショートカット）と見なされます。H ビット フラグが設定された発信インターフェイスはハードウェア内でスイッチングされ、残りのトラフィックは MSFC3 により、ソフトウェア内でスイッチングされます。このため、転送および複製のために MSFC3 に送信されるフローをレート制限することをお勧めします。レート制限をしないと、このフローによって CPU の稼動率が高くなる可能性があります。

マルチキャスト直接接続レート リミッタは、直接接続された送信元からのマルチキャスト パケットを制限します。

次の例では、マルチキャスト パケットを 30000 pps、およびバースト値 30 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 30
```

ip-option キーワード、および IP オプション レート リミッタは、PFC3B または PFC3BXL モードのみでサポートされます。

次の例では、uRPF チェックに失敗した IPv4 マルチキャスト パケットのレート制限を設定する方法を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
```

次の例では、マルチキャスト FIB 不一致パケットを 10000 pps、およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 10000 10
```

次の例では、パーシャル ショートカット フローを 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 partial 20000 20
```

次の例では、マルチキャスト パケットを 30000 pps、およびバースト値 20 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 20
```

次の例では、IGMP スヌーピング トラフィックをレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

IPv6 マルチキャスト

このレート リミッタは、IPv6 マルチキャスト パケットを制限します。表 36-2 は、IPv6 レート リミッタと各レート リミッタが対応するトラフィック クラスの一覧を示します。

表 36-2　IPv6 レート リミッタ

レート リミッタ	レート制限するトラフィック クラス
接続済み	直接接続された送信元トラフィック
デフォルト廃棄	* (*, G/m) SSM * (*, G/m) SSM non-rpf
ルート制御	* (*, FF02::X/128)
Starg ブリッジ	* (*, G/128) SM * (*, G) が存在する場合は SM 非 rpf トラフィック
Starg-M ブリッジ	* (*, G/m) SM * (*, FF/8) * (*, G) が存在しない場合は SM 非 rpf トラフィック

IPv6 マルチキャスト トラフィックのレート リミッタを設定するには、次のいずれかの方法を使用できます。

- レート リミッタをトラフィック クラスに直接関連付け - レートを選択して、このレートをレート リミッタに関連付けます。次の例では、1000 pps および 20 バースト パケットを選択して、このレートをデフォルト廃棄（**default-drop**）レート リミッタに関連付けます。

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- レート リミッタを、設定済みの別のレート リミッタとスタティックに共有 - 隣接関係に基づくレート リミッタが十分に確保できない場合は、すでに設定されたレート リミッタ（ターゲット レート リミッタ）とレート リミッタを共有できます。次の例では、ルート制御（**route-cntl**）レート リミッタを、デフォルト廃棄（**default-drop**）ターゲット レート リミッタと共有します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  ターゲット レート リミッタが未設定の場合は、ターゲット レート リミッタを別のレート リミッタと共有するには、ターゲット レート リミッタが設定されている必要があることを通知するメッセージが表示されます。

- レート リミッタをダイナミックに共有 - どのレート リミッタを共有すべきか判断しにくい場合は、**share auto** キーワードを使用して、ダイナミック共有をイネーブルにします。ダイナミック共有をイネーブルにすると、事前設定されたレート リミッタが選択され、このレート リミッタが指定のレート リミッタと共有されます。次の例では、ルート制御（route-cntrl）レート リミッタに対してダイナミック共有を選択します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

次の例では、直接接続された送信元からの IPv6 マルチキャスト パケットのレート制限を設定する方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
```

次の例では、レート リミッタをトラフィック クラスに直接関連付ける設定方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

次の例では、事前設定された別のレート リミッタとレート リミッタをスタティックに共有する方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

次の例では、ルート制御レート リミッタに対してダイナミック共有をイネーブルにします。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

DoS 攻撃から保護するためのデフォルト設定

表 36-3 は、PFC3 の各種のハードウェア ベース レート リミッタにおける、DoS 攻撃から保護するためのデフォルト設定を示します。

表 36-3　PFC3 のハードウェア ベース レート リミッタのデフォルト設定

レート リミッタ	デフォルト ステータス（ON/OFF）	デフォルト値
入力および出力 ACL ブリッジド パケット	OFF	
RPF 失敗	ON	100 pps、バースト パケット 10
FIB 受信	OFF	
FIB 収集	OFF	
レイヤ 3 セキュリティ機能	OFF	
ICMP リダイレクト	OFF	
ICMP 到達不能	ON	100 pps、バースト パケット 10
VACL ログ	ON	2000 pps、バースト パケット 10
TTL 失敗	OFF	
MTU 失敗	OFF	
レイヤ 2 PDU	OFF	
レイヤ 2 プロトコル トンネリング	OFF	
IP エラー	ON	100 pps、バースト パケット 10
マルチキャスト IGMP	OFF	
マルチキャスト FIB 不一致	ON	100000 pps、バースト パケット 100
マルチキャスト パーシャル SC	ON	100000 pps、バースト パケット 100
マルチキャスト直接接続	OFF	
マルチキャスト非 RPF	OFF	
マルチキャスト IPv6	ON	*packets-in-burst* を設定しない場合は、マルチキャスト関連のレート リミッタではデフォルト値 **100** がプログラミングされます。

DoS 攻撃からの保護における設定時の注意事項および制約事項

ここでは、次の設定における注意事項および制約事項について説明します。

PFC2

PFC2 を使用するシステムに対して DoS 攻撃からの保護を設定する場合は、次の注意事項および制約事項に従ってください。

- セキュリティ ACL を使用して DoS パケットを廃棄する場合は、次の点に注意します。
  - セキュリティ ACL には、廃棄するトラフィック フローを指定する必要があります。
  - セキュリティ ACL は、保護する必要があるすべての外部インターフェイスに設定する必要があります。複数のインターフェイスにセキュリティ ACL を設定するには、**interface range** コマンドを使用します。
- QoS ACL を使用してパケットをレート制限する場合は、次の点に注意します。
  - QoS ACL には、レート制限するトラフィック フローを指定する必要があります。
  - QoS ACL がすでに設定されているインターフェイスに、さらに QoS ACL を追加してパケットをレート制限する場合は、次のいずれかを実行できます。

    * レート制限する ACL を既存の QoS ACL と結合

    * DoS ACL と一致する個別のクラスを定義し、このクラスをポリシー マップに関連付け
  - QoS ACL は、保護する必要があるすべての外部インターフェイスに設定する必要があります。複数のインターフェイスに ACL を設定するには、interface range コマンドを使用します。
- CPU レート リミッタは、トラフィックの集約的な制限だけを行います。正しいパケットと不正なパケットは区別されません。
- FIB レート制限を使用する場合は、次の注意事項に従います。
  - FIB レート制限では、ハードウェア内でのブロードキャスト トラフィック、または一部のマルチキャスト トラフィックはレート制限されません。

    PFC3 は、個別のマルチキャスト レート リミッタを備えています。Supervisor Engine 2 は、個別のマルチキャスト レート リミッタを備えていません。
  - FIB レート制限では、正規のトラフィックと不正なトラフィックは区別されません（トンネル、Telnet など）。
  - FIB レート制限では、フローごとではなく、集約的なレート制限が適用されます。

PFC3

PFC3 を使用するシステムに対して DoS 攻撃からの保護を設定する場合は、CPU レート リミッタに関する次の注意事項および制約事項に従ってください。

（注）　CoPP に関する注意事項および制約事項については、「CoPP 設定時の注意事項および制約事項」（P.36-31）を参照してください。

- PFC3A を使用して構成したシステムでマルチキャストをイネーブルにしている場合は、以下のレート リミッタは使用しないでください。
  - TTL 失敗
  - MTU 失敗
- 以下のレート リミッタは、PFC3B または PFC3BXL モードのみでサポートされます。
  - ユニキャスト IP オプション
  - マルチキャスト IP オプション
- レイヤ 2 レート リミッタは以下のとおりです。
  - レイヤ 2 PDU
  - レイヤ 2 プロトコル トンネリング
  - レイヤ 2 マルチキャスト IGMP
- 8 つのレイヤ 3 レジスタ、および 2 つのレイヤ 2 レジスタを CPU レート リミッタとして使用できます。
- CoPP を使用している場合は、CEF 受信リミッタは使用しないでください。CEF 受信リミッタは、CoPP トラフィックを上書きします。
- レート リミッタは CoPP トラフィックを上書きします。
- 設定したレート制限は、個々の転送エンジンに適用されます（レイヤ 2 ハードウェア レート リミッタは例外的にグローバルに適用される）。
- レイヤ 2 レート リミッタは、truncated モードではサポートされません。
- 入力および出力 ACL ブリッジド パケット レート リミッタを使用する場合は、次の制約事項があります。
  - 入力および出力 ACL ブリッジド パケット レート リミッタは、ユニキャスト トラフィックのみで使用できます。
  - 入力および出力 ACL ブリッジド パケット レート リミッタは、1 つのレート リミッタ レジスタを共有します。ACL ブリッジ入出力レート リミッタをイネーブルにすると、入出力 ACL はどちらも同一のレート リミッタ値を共有します。
- ユニキャスト トラフィックをレート制限するには、**mls rate-limit unicast** コマンドを使用します。
- マルチキャスト トラフィックをレート制限するには、**mls rate-limit multicast** コマンドを使用します。
- レイヤ 2 マルチキャスト トラフィックをレート制限するには、**mls rate-limit multicast layer 2** コマンドを使用します。

パケット廃棄統計情報のモニタ

着信または送信トラフィックをインターフェイス上でキャプチャし、このトラフィックのコピーを外部インターフェイスに送信して、トラフィック アナライザでモニタできます。トラフィックをキャプチャして外部インターフェイスに転送するには、**monitor session** コマンドを使用します。

トラフィックをキャプチャする場合は、次の制約事項が適用されます。

- キャプチャした着信トラフィックはフィルタリングされません。
- キャプチャする着信トラフィックは、キャプチャの実行場所までの転送時にレート制限されません。

Monitor Session コマンドによる廃棄パケットのモニタ

次の例では、**monitor session** コマンドを使用してトラフィックをキャプチャし、外部インターフェイスに転送する方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 source vlan 44 both
Router(config)# monitor session 1 destination interface g9/1
Router(config)# end
Router#
2w0d: %SYS-5-CONFIG_I: Configured from console by console
```

次の例では、**show monitor session** コマンドを使用して、宛先ポートの場所を表示する方法を示します。

```
Router# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          44
Destination Ports: Gi9/1
Filter VLANs:      None
```

show tcam interface コマンドによる廃棄パケットのモニタ

PFC3B および PFC3BXL モードでは、ハードウェア内の ACL ヒット カウンタがサポートされます。**show tcam interface** コマンドを使用すると、ACL TCAM 内の各エントリを表示できます。

次の例では、**show tcam interface** コマンドを使用して、エントリがヒットした回数を表示します。

```
Router# show tcam interface fa5/2 acl in ip detail

---------------------------------------------------------------------------------------------------------------
DPort - Destination Port   SPort - Source Port        TCP-F - U -URG Pro   - Protocol
I     - Inverted LOU       TOS   - TOS Value                - A -ACK rtr   - Router
MRFM  - M -MPLS Packet     TN    - T -Tcp Control           - P -PSH COD   - C -Bank Care Flag
      - R -Recirc. Flag          - N -Non-cachable          - R -RST       - I -OrdIndep. Flag
      - F -Fragment Flag   CAP   - Capture Flag             - S -SYN       - D -Dynamic Flag
      - M -More Fragments  F-P   - FlowMask-Prior.          - F -FIN T     - V(Value)/M(Mask)/R(Result)
X     - XTAG               (*)   - Bank Priority
---------------------------------------------------------------------------------------------------------------
```

```
Interface: 1018   label: 1   lookup_type: 0
protocol: IP   packet-type: 0

+-+-----+---------------+---------------+---------------+---------------+-------+---+----+-+---+--+---+---+
|T|Index|  Dest Ip Addr | Source Ip Addr|     DPort     |     SPort     | TCP-F|Pro|MRFM|X|TOS|TN|COD|F-P|
+-+-----+---------------+---------------+---------------+---------------+------+---+----+-+---+--+---+---+
 V 18396         0.0.0.0         0.0.0.0       P=0             P=0       ------   0 ---- 0   0 -- --- 0-0
 M 18404         0.0.0.0         0.0.0.0         0               0               0 ---- 0   0
 R rslt: L3_DENY_RESULT                rtr_rslt: L3_DENY_RESULT


 V 36828         0.0.0.0         0.0.0.0       P=0             P=0        ------  0 ---- 0   0 -- --- 0-0
 M 36836         0.0.0.0         0.0.0.0         0               0               0 ---- 0   0
 R rslt: L3_DENY_RESULT (*)            rtr_rslt: L3_DENY_RESULT (*)
Router#
```

TTL または IP オプション カウンタを使用して、レイヤ 3 転送エンジンのパフォーマンスをモニタすることもできます。

次の例では、**show mls statistics** コマンドを使用して、レイヤ 3 転送エンジンに関連付けられたパケット統計情報およびエラーを表示します。

```
Router# show mls statistics

Statistics for Earl in Module 6

L2 Forwarding Engine
  Total packets Switched                : 25583421

L3 Forwarding Engine
  Total packets L3 Switched             : 25433414 @ 24 pps

  Total Packets Bridged                 : 937860
  Total Packets FIB Switched            : 23287640
  Total Packets ACL Routed              : 0
  Total Packets Netflow Switched        : 0
  Total Mcast Packets Switched/Routed   : 96727
  Total ip packets with TOS changed     : 2
  Total ip packets with COS changed     : 2
  Total non ip packets COS changed      : 0
  Total packets dropped by ACL          : 33
  Total packets dropped by Policing     : 0

Errors
  MAC/IP length inconsistencies         : 0
  Short IP packets received             : 0
  IP header checksum errors             : 0
  TTL failures                          : 0
<----------------- TTL counters
  MTU failures                          : 0
<------------------MTU failure counters

Total packets L3 Switched by all Modules: 25433414 @ 24 pps
```

VACL キャプチャによる廃棄パケットのモニタ

VACL キャプチャ機能を使用すると、キャプチャしたトラフィックを転送するように設定されたポートにトラフィックを転送できます。capture アクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。

VACL キャプチャを使用すると、各 VLAN からのトラフィックを別のインターフェイスに割り当てることができます。

VACL キャプチャでは、ある種類のトラフィック（たとえば HTTP）をあるインターフェイスに、別の種類のトラフィック（たとえば DNS）を別のインターフェイスに送信することはできません。また、VACL キャプチャ粒度は、ローカルにスイッチされたトラフィックのみに適用できます。トラフィックをリモート スイッチに転送した場合は、この粒度は保存できません。

次の例では、VACL キャプチャを使用してトラフィックをキャプチャし、ローカル インターフェイスに転送する方法を示します。

```
Router(config-if)# switchport capture
Router(config-if)# switchport capture allowed vlan add 100
```

レート リミッタ情報の表示

show mls rate-limit コマンドを使用すると、設定したレート リミッタに関する情報を表示できます。

show mls rate-limit usage コマンドを使用すると、特定の種類のレート リミッタが使用したハードウェア レジスタを表示できます。どの種類のレート リミッタからも使用されていないレジスタの場合は、出力結果には Free と表示されます。ある種類のレート リミッタによって使用されているレジスタの場合は Used と表示され、このレート リミッタの種類が表示されます。

コマンドの結果、レート制限ステータスは次のいずれかとして出力されます。

- 特定の条件に対するレートが設定されている場合は「On」
- この種類のレート リミッタが未設定であり、この条件に適合するパケットがレート制限されていない場合は「Off」
- ある特定の条件（手動設定したものではない条件）が、同一の共有グループに属する別のレート リミッタの設定によって影響を受ける場合は「On/Sharing」
- マルチキャスト パーシャル SC レート リミッタがディセーブルになっている場合は「-（ハイフン）」

コマンドの結果、レート制限共有については次の情報が出力されます。

- 共有がスタティックであるかダイナミックであるか
- グループのダイナミック共有コード

設定したレート リミッタの情報を表示するには、**show mls rate-limit** コマンドを使用します。

```
Router# show mls rate-limit
 Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group

   Rate Limiter Type       Status     Packets/s   Burst  Sharing
 ---------------------   ----------   ---------   -----  -------
         MCAST NON RPF   Off                -       -     -
        MCAST DFLT ADJ   On            100000     100  Not sharing
      MCAST DIRECT CON   Off                -       -     -
        ACL BRIDGED IN   Off                -       -     -
       ACL BRIDGED OUT   Off                -       -     -
           IP FEATURES   Off                -       -     -
          ACL VACL LOG   On              2000       1  Not sharing
           CEF RECEIVE   Off                -       -     -
             CEF GLEAN   Off                -       -     -
      MCAST PARTIAL SC   On            100000     100  Not sharing
        IP RPF FAILURE   On               100      10  Group:0 S
           TTL FAILURE   Off                -       -     -
 ICMP UNREAC. NO-ROUTE   On               100      10  Group:0 S
 ICMP UNREAC. ACL-DROP   On               100      10  Group:0 S
         ICMP REDIRECT   Off                -       -     -
           MTU FAILURE   Off                -       -     -
       MCAST IP OPTION   Off                -       -     -
       UCAST IP OPTION   Off                -       -     -
           LAYER_2 PDU   Off                -       -     -
            LAYER_2 PT   Off                -       -     -
             IP ERRORS   On                 100      10  Group:0 S
           CAPTURE PKT   Off                -       -     -
            MCAST IGMP   Off                -       -     -
 MCAST IPv6 DIRECT CON   Off                -       -     -
 MCAST IPv6 *G M BRIDG   Off                -       -     -
  MCAST IPv6 *G BRIDGE   Off                -       -     -
  MCAST IPv6 SG BRIDGE   Off                -       -     -
 MCAST IPv6 ROUTE CNTL   Off                -       -     -
  MCAST IPv6 DFLT DROP   Off                -       -     -
 MCAST IPv6 SECOND. DR   Off                -       -     -
Router#
```

ハードウェア レート リミッタの使用状況を表示するには、**show mls rate-limit usage** コマンドを使用します。

```
Router# show mls rate-limit usage
                            Rate Limiter Type     Packets/s   Burst
                          ----------------------  ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                           -           -       -
             RL# 1: Free                           -           -       -
             RL# 2: Free                           -           -       -
             RL# 3: Used
                                     MCAST DFLT ADJ      100000     100
             RL# 4: Free                           -           -       -
             RL# 5: Free                           -           -       -
             RL# 6: Used
                                   IP RPF FAILURE          100      10
                                ICMP UNREAC. NO-ROUTE      100      10
                                ICMP UNREAC. ACL-DROP      100      10
                                         IP ERRORS         100      10
             RL# 7: Used
                                    ACL VACL LOG          2000       1
             RL# 8: Rsvd for capture                -           -       -
```

```
Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
             RL#11: Free                        -          -       -
             RL#12: Free                        -          -       -
Router#
```

CoPP の機能概要

CoPP 機能を使用すると、不要なトラフィックや DoS トラフィックから MSFC を保護し、重要なコントロール プレーンおよび管理トラフィックを優先させることができるので、Catalyst 6500 シリーズ スイッチのセキュリティを強化できます。PFC3 および DFC3 は、CoPP のハードウェア サポートを行います。CoPP は、PFC3 のレート リミッタと連携して動作します。

（注）　Supervisor Engine 2 は CoPP をサポートしません。

PFC3 は、組み込みの [special case] レート リミッタをサポートします。このレート リミッタは、IP オプション、TTL および MTU の失敗、エラーの生じたパケット、マルチキャスト パケットといった ACL の分類に該当しない、特定のシナリオで使用できます。special-case レート リミッタをイネーブルにすると、このレート リミッタは基準に適合するパケットに対し、CoPP ポリシーを上書きします。

MSFC によって管理されるトラフィックは、次の 3 つの機能コンポーネント（*プレーン*）に分類されます。

- データ プレーン
- マネジメント プレーン
- コントロール プレーン

MSFC の管理するトラフィックのほとんどは、コントロール プレーンおよびマネジメント プレーンによって処理されます。CoPP を使用してコントロール プレーンおよびマネジメント プレーンを保護することで、ルーティングの安定性、到達可能性、および確実なパケット配信を維持できます。CoPP では、Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）から専用のコントロール プレーン設定を使用して、コントロール プレーン パケットに対するフィルタリングおよびレート制限機能を提供します。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルにされています。

CoPP 設定時の注意事項および制約事項

CoPP を設定する場合は、次の注意事項および制約事項に従ってください。

- Release12.2(18)SXE よりも前のリリースでは、PFC3 は MQC の class-default をハードウェアでサポートしていません。クラス デフォルトは、通常のクラス マップに置き換えられます。catch-all マップを定義すると、MQC class-default がハードウェアでサポートされます。
- マルチキャストに一致するクラスは、ハードウェアではなくソフトウェアに適用されます。
- CPP によるブロードキャスト パケット処理は、ハードウェアではサポートされません。ブロードキャスト DoS 攻撃からの保護を実現するには、ACL、トラフィック ストーム制御、および CPP ソフトウェア保護を組み合わせて使用します。
- CoPP は ARP ポリシーをサポートしません。ARP ポリシング メカニズムは、ARP ストームからの保護を実現します。
- CoPP は、デフォルトの非 IP クラス以外の非 IP クラスをサポートしません。非 IP トラフィックを廃棄するには、非 IP クラスの代わりに ACL を使用できます。また、RP CPU に到達する非 IP トラフィックを制限するには、デフォルトの非 IP CoPP クラスを使用できます。
- CoPP ポリシー ACL では、**log** キーワードは使用しないでください。
- PFC3A では、出力 QoS と CoPP を同時に設定することはできません。この状況では、CoPP はソフトウェア内で実行されます。出力 QoS と CoPP を同時に設定できないことを伝える警告メッセージが表示されます。
- 大規模な QoS 設定を使用すると、システムの TCAM 領域が足りなくなる可能性があります。この場合は、CoPP はソフトウェア内で実行されます。
- 他のインターフェイスに対する大規模な QoS 設定があると、領域が足りなくなる可能性があります。この場合は、CoPP がソフトウェア内で完全に実行され、パフォーマンス低下や CPU サイクル消費につながる可能性があります。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはスイッチへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、スイッチへのリモート アクセスが禁止され、コンソール接続が必要となる場合があります。
- PFC3 は、組み込みの special-case レート リミッタをサポートします。これは、ACL を使用できない状況（TTL、MTU、IP オプションなど）で便利です。special-case レート リミッタをイネーブルにする場合は、このレート リミッタが基準に適合するパケットに対し、CoPP ポリシーを上書きすることに注意してください。
- **mls qos** コマンドによって MMLS QoS をグローバルにイネーブル化しない限り、CoPP はハードウェアでイネーブル化されません。**mls qos** コマンドを入力しないと、CoPP はソフトウェア内だけで動作し、ハードウェアに対する機能を果たせなくなります。
- 出力 CoPP、およびサイレント モードはサポートされません。CoPP は入力だけでサポートされます。サービス ポリシー出力 CoPP は、コントロール パネル インターフェイスには適用できません。
- ハードウェア内の ACE ヒット カウンタは、ACL 論理のみに対応します。CPU トラフィックのトラブルシューティングおよび評価には、ソフトウェア ACL のヒット カウンタ、および **show access-list**、**show policy-map control-plane**、**show mls ip qos** コマンドが役立ちます。
- CoPP は転送エンジン単位で実行され、ソフトウェア CoPP は集約的に実行されます。
- CoPP によるマルチキャスト パケット処理は、ハードウェアではサポートされません。マルチキャスト DoS 攻撃からの保護を実現するには、ACL、マルチキャスト CPU レート リミッタ、および CoPP ソフトウェア保護を組み合わせて使用します。
- CoPP では、ACE に **log** キーワードを使用できません。

- CoPP はハードウェア QoS TCAM リソースを使用します。TCAM の利用率を確認するには、**show tcam utilization** コマンドを入力します。

CoPP の設定

CoPP では MQC を使用することで、トラフィックの分類基準を定義し、分類したトラフィックに対して設定可能なポリシー アクションを指定します。最初にクラス マップを定義して、分類の対象となるトラフィックを識別する必要があります。クラス マップは、特定のトラフィック クラスに対するパケットを定義します。トラフィックを分類したあとは、識別したトラフィックにポリシー アクションを適用するためのポリシー マップを作成できます。**control-plane** 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、CoPP サービス ポリシーをコントロール プレーンに直接付加できます。

トラフィック分類基準を定義する方法については、「トラフィック分類の定義」（P.36-34）を参照してください。

CoPP を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	MLS QoS をグローバルにイネーブル化します。
ステップ 2	`Router(config)# ip access-list extended` *access-list-name* `Router(config-ext-nacl)#` {**permit** | **deny**} *protocol* **source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]	トラフィックと一致する ACL を定義します。 • **permit** は、名前付き IP アクセス リストにパケットが適合する条件を設定します。 • **deny** は、名前付き IP アクセス リストがパケットを拒否する条件を設定します。 **（注）** ほとんどの場合は、重要なトラフィックとそうでないトラフィックの識別には ACL を設定する必要があります。
ステップ 3	`Router(config)# class-map` *traffic-class-name* `Router(config-cmap)# match` {**ip precedence**} |{**ip dscp**} | *access-group*	パケット分類基準を定義します。**match** ステートメントを使用して、クラスに関連付けるトラフィックを識別します。
ステップ 4	`Router(config)# policy-map` *service-policy-name* `Router(config-pmap)# class` *traffic-class-name* `Router(config-pmap-c)# police` {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]	サービス ポリシー マップを定義します。**class** *traffic-class-name* コマンドを使用して、サービス ポリシー マップにクラスを関連付けます。**police** ステートメントを使用して、サービス ポリシー マップにアクションを関連付けます。
ステップ 5	`Router(config)# control-plane` `Router(config-cp)#`	コントロール プレーンのコンフィギュレーション モードを有効にします。
ステップ 6	`Router(config-cp)# service-policy input` *service-policy-name*	QoS サービス ポリシーをコントロール プレーンに適用します。

パケット分類基準を定義する場合は、次の注意事項および制約事項に従ってください。

- 以降のクラスで設定されたフィルタリングおよびポリシングと一致することを避けるため、ポリシングは各クラスで設定します。CoPP では、police コマンドを含まないクラスにはフィルタリングを適用しません。police コマンドのないクラスは、どのトラフィックとも一致しません。
- 分類に使用する ACL は QoS ACL です。サポートされる QoS ACL は、IP 標準 ACL、拡張 ACL、および名前付き ACL です。IPv6 ACL はハードウェアではサポートされません。
- 次の一致タイプのみがサポートされます。
  - **ip precedence**
  - **ip dscp**
  - **access-group**
- ハードウェアでは、IP ACL だけがサポートされます。
- MAC ベースの一致は、ソフトウェアのみで行われます。
- 1 つの **match** コマンドを、1 つのクラス マップのみに入力できます。
- Release12.2(18)SXE よりも前のリリースでは、MQC クラスのデフォルトはサポートされません。

サービス ポリシーを定義する場合は、**police** ポリシー マップ アクションのみがサポートされます。

サービス ポリシーをコントロール プレーンに適用する場合は、**input** 方向のみがサポートされます。

CoPP のモニタ

サイト固有のポリシーを作成するには、**show policy-map control-plane** コマンドを入力することで、コントロール プレーン ポリシーの統計情報をモニタでき、CoPP のトラブルシューティングを行えます。このコマンドを使用すると、実際に適用されたポリシーについてのダイナミックな情報を表示できます。たとえば、ハードウェアおよびソフトウェア内において、設定されたポリシーに適合する、またはこれを超過するバイト数およびパケット数を表示できます。

show policy-map control-plane コマンドの出力結果は次のようになります。

```
Router# show policy-map control-plane
Control Plane Interface
  Service policy CoPP-normal
Hardware Counters:
class-map: CoPP-normal (match-all)
      Match: access-group 130
      police :
        96000 bps 3000 limit 3000 extended limit
      Earl in slot 3 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
```

```
Software Counters:
    Class-map: CoPP-normal (match-all) 0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      police:
        96000 bps, 3125 limit, 3125 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Router#
```

ハードウェア カウンタを表示して、ポリシーによって廃棄および転送されたバイト数を確認するには、**show mls qos ip** コマンドを入力します。

```
Router# show mls qos ip
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                             Id         Id
-------------------------------------------------------------------------------
CPP  5  In CoPP-normal    0    1   dscp  0         505408       83822272
CPP  9  In CoPP-normal    0    4   dscp  0              0              0
Router#
```

CoPP アクセス リストの情報を表示するには、access-lists coppacl-bgp コマンドを入力します。

```
Router#show access-lists coppacl-bgp
Extended IP access list coppacl-bgp
10 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp (4 matches)
20 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
30 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp (1 match)
40 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

トラフィック分類の定義

ここでは、CoPP トラフィックを分類する方法について説明します。

- 「トラフィック分類の概要」（P.36-34）
- 「トラフィック分類の注意事項」（P.36-36）
- 「CoPP トラフィック分類の基本的な ACL の例」（P.36-36）

トラフィック分類の概要

定義できるクラスの数に制限はありませんが、一般的にトラフィックは、相対的な重要度に基づくクラスに分類されます。次に、グループ分けの例を示します。

- Border Gateway Protocol（BGP）- BGP ルーティング プロトコルにおいて、隣接関係を維持するために重要なトラフィック。BGP キープ アライブ、ルーティング更新などです。BGP ルーティング プロトコルの維持は、ネットワーク内での接続、またはサービス プロバイダーとの接続を維持するうえで重要です。BGP を実行しないサイトでは、このクラスを使用する必要はありません。
- Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）- IGP ルーティング プロトコルを維持するうえで重要なトラフィック。たとえば Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などです。IGP ルーティング プロトコルの維持は、ネットワーク内の接続を維持するうえで重要です。

- 管理 - 日常業務で必要とされ、頻繁に使用される必須トラフィック。たとえば、リモート ネットワーク アクセスに使用するトラフィックや、Cisco IOS イメージの更新および管理トラフィックです。これには、Telnet、Secure Shell（SSH; セキュア シェル）、Network Time Protocol（NTP）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、Terminal Access Controller Access Control System（TACACS）、HTTP、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、File Transfer Protocol（FTP; ファイル転送プロトコル）などがあります。
- レポート - レポート目的で、ネットワーク パフォーマンスに関する統計情報の生成に使用されるトラフィック。たとえば、Cisco IOS IP サービス レベル アグリーメントを使用して、異なる DSCP 設定で ICMP を生成し、さまざまな QoS データ クラス内の応答時間をレポートできます。
- モニタ - スイッチのモニタに使用するトラフィック。このトラフィックは許可する必要がありますが、スイッチを危険にさらすことがあってはなりません。CoPP を使用すると、このトラフィックは許可されますが、低いレートに制限できます。たとえば、ICMP エコー要求（ping）、traceroute などです。
- クリティカルなアプリケーション - 特定のカスタマー環境に固有の、クリティカルなアプリケーション トラフィック。このクラスに分類するトラフィックは、ユーザに必要なアプリケーションの要件に合わせて、特別に調整する必要があります。マルチキャストを使用するカスタマーもいれば、IPSec または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用するカスタマーもいます。このトラフィックの例としては、GRE、Hot Standby Router Protocol（HSRP）、Virtual Router Redundancy Protocol（VRRP）、Session Initiation Protocol（SIP）、データ リンク スイッチング、Dynamic Host Configuration Protocol（DHCP）、Multicast Source Discovery Protocol（MSDP）、IGMP、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPsec などが挙げられます。
- レイヤ 2 プロトコル - ARP に使用されるトラフィック。ARP パケットが過剰に発生すると、MSFC リソースが独占され、他の重要なプロセスがリソース不足になってしまう可能性があります。CoPP を使用して ARP パケットをレート制限すると、このような状況を回避できます。現時点では、一致プロトコル分類基準を使用して明示的に分類可能な唯一のレイヤ 2 プロトコルが、ARP となります。
- 不要 - MSFC へのアクセスを無条件で廃棄および拒否する必要のある、不正な、または悪意あるトラフィックを明示的に指定します。この分類は、スイッチ宛ての既知のトラフィックを常に拒否する必要があり、デフォルト カテゴリに含まれないようにする場合に便利です。トラフィックを明示的に拒否した場合は、**show** コマンドを使用すると、拒否したトラフィックの概算統計情報を収集し、そのレートを見積もることができます。
- デフォルト - 他に分類されない、MSFC 宛ての残りのトラフィックすべてを収容。MQC はデフォルト クラスを備えているため、他のユーザ定義クラスでは明示的に識別されないトラフィックに適用する処理を指定できます。このトラフィックの MSFC へのアクセス レートは、大幅に制限されます。デフォルト分類を設定しておくと、統計情報をモニタして、通常であれば識別されないコントロール プレーン宛てトラフィックのレートを決定できます。このトラフィックを識別したあとは、追加の分析を行うことで該当カテゴリに分類できます。必要であれば、このトラフィックにも対応するように、他の CoPP ポリシー エントリを更新することもできます。

トラフィックの分類が完了すると、ACL は、ポリシーの定義に使用するトラフィック クラスを作成します。CoPP 分類に使用する基本的な ACL の例については、「CoPP トラフィック分類の基本的な ACL の例」（P.36-36）を参照してください。

トラフィック分類の注意事項

トラフィック分類を定義する場合は、次の注意事項および制約事項に従ってください。

- 実際の CoPP ポリシーを作成する前に、どのトラフィックをどのクラスに分類するかを識別しておく必要があります。トラフィックは相対的な重要度に基づき、9 つのクラスに分類されます。実際に必要となるクラス数はこれとは異なる可能性があり、各自のローカルな要件、およびセキュリティ ポリシーに基づき選択する必要があります。
- 双方向的に一致するポリシーを定義する必要はありません。ポリシーは入力のみに適用されるため、トラフィックは一方向（ネットワークから MSFC へ）のみで識別します。

CoPP トラフィック分類の基本的な ACL の例

ここでは、CoPP 分類の基本的な ACL の例を示します。各例では、一般的に必要とされるトラフィックを、以下の ACL によって識別します。

- ACL 120 – クリティカルなトラフィック
- ACL 121 – 重要なトラフィック
- ACL 122 – 通常のトラフィック
- ACL 123 – 不要なトラフィックを明示的に拒否
- ACL 124 – その他すべてのトラフィック

次の例では、クリティカルなトラフィックに対する ACL 120 を定義します。

```
Router(config)# access-list 120 remark CoPP ACL for critical traffic
```

次の例では、既知のピアからスイッチの BGP TCP ポートへの、BGP トラフィックを許可します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
```

次の例では、ピアの BGP ポートからこのスイッチへの BGP トラフィックを許可します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
Router(config)# access-list 120 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp
Router(config)# access-list 120 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

次の例では、重要なクラスに対する ACL 121 を定義します。

```
Router(config)# access-list 121 remark CoPP Important traffic
```

次の例では、TACACS ホストからのリターン トラフィックを許可します。

```
Router(config)# access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
```

次の例では、サブネットからスイッチへの SSH アクセスを許可します。

```
Router(config)# access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
```

次の例では、指定のサブネット内のホストからスイッチへの Telnet フル アクセスを許可し、残りのサブネットをポリシングします。

```
Router(config)# access-list 121 deny tcp host 10.86.183.3 any eq telnet
Router(config)# access-list 121 permit tcp 10.86.183.0 0.0.0.255 any eq telnet
```

次の例では、NMS ホストからスイッチへの SNMP アクセスを許可します。

```
Router(config)# access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
```

次の例では、既知のクロック ソースからの NTP パケットの受信をスイッチに許可します。

```
Router(config)# access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

次の例では、通常のトラフィック クラスに対する ACL 122 を定義します。

```
Router(config)# access-list 122 remark CoPP normal traffic
```

次の例では、スイッチから送信される traceroute トラフィックを許可します。

```
Router(config)# access-list 122 permit icmp any any ttl-exceeded
Router(config)# access-list 122 permit icmp any any port-unreachable
```

次の例では、ping を発行したスイッチへの応答を受信することを許可します。

```
Router(config)# access-list 122 permit icmp any any echo-reply
```

次の例では、スイッチへの ping の送信を許可します。

```
Router(config)# access-list 122 permit icmp any any echo
```

次の例では、不要なクラスに対する ACL 123 を定義します。

```
Router(config)# access-list 123 remark explicitly defined "undesirable" traffic
```

（注）　次の例では、ACL 123 は分類およびモニタのための許可エントリであり、トラフィックは CoPP ポリシーの結果に基づいて廃棄されます。

この例では、UDP 1434 宛てに送信され、ポリシングの対象となるすべてのトラフィックを許可します。

```
Router(config)# access-list 123 permit udp any any eq 1434
```

次の例では、他のすべてのトラフィックに対する ACL 124 を定義します。

```
Router(config)# access-list 124 remark rest of the IP traffic for CoPP
Router(config)# access-list 124 permit ip any any
```

sticky ARP の設定

sticky ARP は、ARP エントリ（IP アドレス、MAC アドレス、送信元 VLAN）が上書きされないように保証することで、MAC アドレスのスプーフィングを防止します。スイッチは、トラフィックをエンド デバイスまたは他のスイッチに転送する目的で、ARP エントリを維持します。ARP エントリは通常、定期的に更新されるか、または ARP ブロードキャスト受信時に修正されます。攻撃が開始されると、偽装した MAC アドレスと正規の IP アドレスを持つ ARP ブロードキャストが送信されます。この結果、スイッチは偽装した MAC アドレスによる正規の IP アドレスを学習し、トラフィックのこの MAC アドレスへの転送を開始します。sticky ARP をイネーブルにすると、スイッチは ARP エントリを学習し、ARP ブロードキャストから受信した変更は受け付けなくなります。ARP 設定を上書きしようとすると、エラー メッセージが発行されます。システム エラー メッセージの完全な詳細については、次の URL にある『*Catalyst 6500 Series Switch Cisco IOS System Message Guide*, Release 12.2SX 』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2sx/system/messages/122sxsms.html

（注）　sticky ARP の設定は、Release 12.2(18)SXF 以降のリリースでサポートされます。

レイヤ 3 インターフェイス上で sticky ARP を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	sticky ARP を適用するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip sticky-arp`	sticky ARP をイネーブルにします。
	`Router(config-if)# no ip sticky-arp ignore`	以前に設定した sticky ARP コマンドを削除します。
ステップ 3	`Router(config-if)# ip sticky-arp ignore`	sticky ARP をディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス 5/1 で sticky ARP をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# ip sticky-arp
Router(config-if)# end
Router#
```

CHAPTER 37

Dynamic Host Configuration Protocol（DHCP）スヌーピングの設定

この章では、Catalyst 6500 シリーズ スイッチに Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する手順について説明します。

（注） DHCP スヌーピング機能には、Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）および Release 12.2(18)SXE 以降のリリースが必要です。PFC2 は、DHCP スヌーピングをサポートしません。

この章で説明する主な内容は、次のとおりです。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

DHCP スヌーピングの概要

ここでは、DHCP スヌーピング機能について説明します。

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバ間のファイアウォールのように機能するセキュリティ機能です。DHCP スヌーピング機能では次の作業を行います。

- 信頼できない送信元から受信した DHCP メッセージを検証し、無効なメッセージをフィルタリングする。
- 信頼できる送信元および信頼できない送信元からの DHCP トラフィックのレートを制限する。
- DHCP スヌーピング バインディング データベースを構築し、維持する。このデータベースには、専用 IP アドレスを持つ信頼できないホストに関する情報が格納されます。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降 の要求を検証する。

Dynamic ARP Inspection（DAI; ダイナミック ARP 検査）などのその他のセキュリティ機能でも、DHCP スヌーピング バインディング データベースに格納されている情報を使用します。

DHCP スヌーピングは Virtual LAN（VLAN; 仮想 LAN）単位でイネーブルにします。デフォルトでは、すべての VLAN で非アクティブです。この機能は、1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

DHCP スヌーピング機能は、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）のソフトウェアに実装されています。そのため、イネーブルにされた VLAN のすべての DHCP メッセージは、PFC で代行受信され、MSFC に転送されて処理されます。

信頼できる送信元と信頼できない送信元

DHCP トラフィック機能は、トラフィックの送信元が信頼できるかできないかを判断します。信頼できない送信元は、トラフィック攻撃を開始したり、その他の悪意のある行為を行ったりする可能性があります。こうした攻撃を防ぐために、DHCP スヌーピング機能は、メッセージをフィルタリングし、信頼できない送信元からのトラフィックのレートを制限します。

企業ネットワークでは、その企業の管理制御下にあるデバイスは信頼できる送信元です。これらのデバイスには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは、信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダー環境では、サービス プロバイダー ネットワーク内にないデバイスは信頼できない送信元です（カスタマーのスイッチなど）。ホスト ポートは信頼できない送信元です。

Catalyst 6500 シリーズ スイッチでは、接続インターフェイスの信頼状態を設定することで、送信元を信頼できるものとして扱うことができます。

すべてのインターフェイスのデフォルトの信頼状態は untrusted です。DHCP サーバ インターフェイスを trusted に設定する必要があります。他のインターフェイスも、ネットワーク内のデバイス（スイッチやルータ）に接続している場合は、trusted に設定できます。通常、ホスト ポート インターフェイスは trusted に設定しません。

（注）　DHCP スヌーピング機能を適切に機能させるために、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続する必要があります。これは、信頼できない DHCP メッセージは信頼できるインターフェイスにのみ転送されるためです。

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 データベースは、DHCP スヌーピング バインディング テーブルとも呼ばれます。

DHCP スヌーピング機能は、代行受信した DHCP メッセージから抽出した情報を使用して、ダイナミックにデータベースを構築し、維持します。DHCP スヌーピングがイネーブルになっている VLAN にホストが関連付けられている場合、データベースには専用 IP アドレスを持つ信頼できない各ホストのエントリが格納されます。このデータベースには、信頼できるインターフェイスを介して接続されたホストのエントリは含まれません。

スイッチが特定の DHCP メッセージを受信すると、DHCP スヌーピングは機能はデータベースを更新します。たとえば、スイッチが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。IP アドレスのリース期限が過ぎたり、スイッチがホストから DHCPRELEASE メッセージを受信すると、この機能によってデータベース内のエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、専用 IP アドレス、リース期間、バインディングのタイプ、ホストに関連付けられた VLAN の番号およびインターフェイス情報が含まれています。

パケット検証

スイッチは、DHCP スヌーピングがイネーブルになっている VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。スイッチは、次のいずれかの条件が発生しない限り、DHCP パケットを転送します（次の条件が発生した場合、パケットは廃棄されます）。

- スイッチがネットワークまたはファイアウォール外部の DHCP サーバからパケット（DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY など）を受信した場合。
- スイッチが信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンになっている場合のみ実行されます。
- スイッチが、DHCP スヌーピング バインディング テーブル内にエントリがある信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。
- スイッチが、リレー エージェントの IP アドレス（0.0.0.0 以外）を保持する DHCP パケットを受信した場合。

Release 12.2(18)SXF1 よりも前のリリースでは、スイッチは信頼できないポートで受信された Option 82 情報を含む DHCP パケットを廃棄します。Release 12.2(18)SXF1 以降のリリースでは、信頼できない集約スイッチのポートに接続された信頼できるエッジ スイッチをサポートするため、信頼できないポートの機能で DHCP Option 82 をイネーブルにして、信頼できない集約スイッチのポートが Option 82 情報を含む DHCP パケットを受信するようにできます。集約スイッチに接続するエッジ スイッチのポートを、信頼できるポートとして設定します。

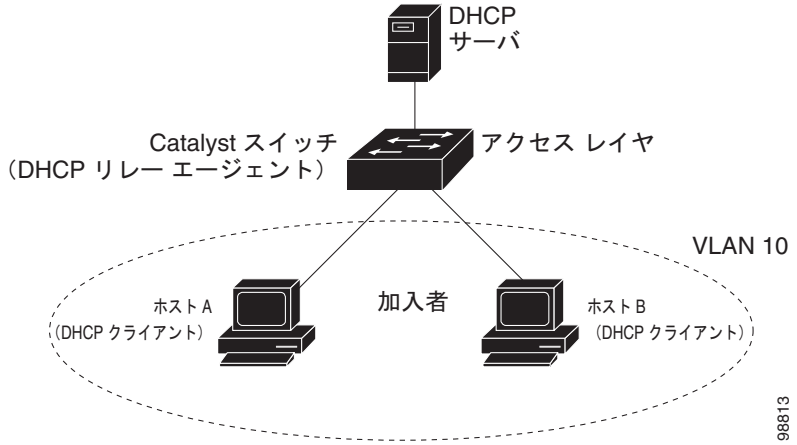
（注）　信頼できないポート機能で DHCP Option 82 がイネーブルである場合は、集約スイッチでダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査を使用して、信頼できない入力インターフェイスを保護します。

DHCP スヌーピングの 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 は多数の加入者に対し、IP アドレスの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、この装置をネットワークに接続するポートにスイッチ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。

図 37-1 は、メトロポリタン イーサネット ネットワーク内において、アクセス レイヤのスイッチに接続されている各加入者の IP アドレスを、一元的な DHCP サーバが割り当てる例を示します。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェントをヘルパー アドレスによって設定することで、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 37-1　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 スヌーピング情報の Option 82 をイネーブルにすると、次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、これを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、パケット内に Option 82 情報を追加します。Option 82 情報には、スイッチの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（回線 ID サブオプション）が含まれます。
- 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は、スイッチは DHCP パケット内にこの IP アドレスを追加します。
- 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 サーバは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、このリモート ID または回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの実装を行えます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる IP アドレスの数を制限するポリシーなどです。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中継されている場合は、DHCP サーバは応答をスイッチにユニキャストします。クライアントとサーバが同じサブネット上にある場合は、サーバはこの応答をブロードキャストします。スイッチはリモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データが挿入されてい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。

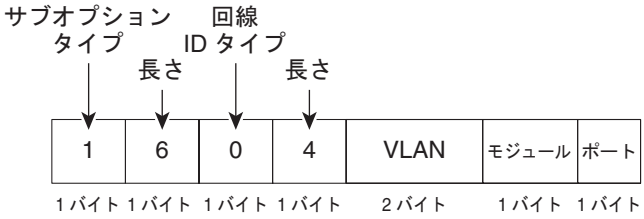
上記の一連のイベントが発生する間、図 37-2 に示す以下のフィールドの値は変更されません。

- 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
  - 回線 ID タイプの長さ

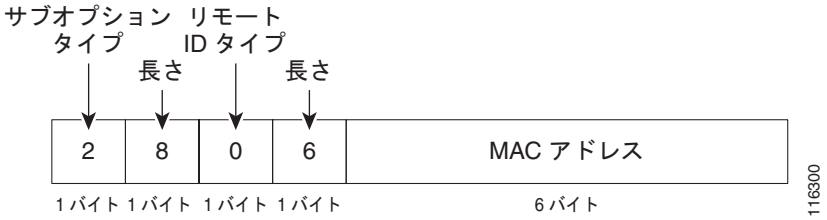
図 37-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化されている場合、および **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合です。回線 ID サブオプションの場合は、モジュール フィールドはモジュールのスロット番号となります。

図 37-2　　サブオプションのパケット形式

回線 ID サブオプション フレーム形式



リモート ID サブオプション フレーム形式



DHCP スヌーピング データベース エージェントの概要

リロード後もバインディングを維持するには、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。このエージェントを使用しないと、DHCP スヌーピングによって確立されたバインディングはリロード後に失われてしまい、同様に接続も失われます。

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。スイッチはリロード時にこのファイルを読み取り、バインディング用のデータベースを構築します。スイッチはデータベースが変更されるたびにこのファイルに書き込むことで、このファイルを最新に保ちます。

バインディングを保持するファイルの形式は、次のようになります。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

ファイル内の各エントリには、チェックサムを示すタグが付けられます。これは、ファイルが読み取られるたびに、エントリの検証に使用されます。1 行目の <initial-checksum> エントリは、最新の書き込みに関連する各エントリを、以前の書き込みに関連する各エントリから区別します。

次に、バインディング ファイルの例を示します。

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1                                    e5e1e733
1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1                                    4b3486ec
1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1                                   f0e02872
1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1                                   ac41adf9
1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1                                      34b3273e
END
```

各エントリは、IP アドレス、VLAN、MAC アドレス、リース期間（16 進数単位）、およびバインディングに関連付けられたインターフェイスを示します。各エントリの最後に示されるチェックサムは、ファイルの冒頭から、エントリに関連付けられたすべてのバイトの合計に基づいて計算されます。各エントリは、72 バイトのデータ、スペース、およびチェックサムの順で構成されます。

ブートアップ時、計算されたチェックサムと保存されたチェックサムが等しい場合は、スイッチはファイルから各エントリを読み取り、各バインディングを DHCP スヌーピング データベースに追加します。計算されたチェックサムが保存されたチェックサムと異なる場合は、ファイルから読み取られたこのエントリは無視され、このエントリ以降のすべてのエントリも無視されます。また、スイッチはファイルから読み取ったエントリのうち、リース期間が失効しているすべてのエントリも無視します。この場合は、リース期間としてすでに経過した期間が示されているので、スイッチはこの値に基づき判断します。エントリ内で参照されるインターフェイスが、システム上にすでに存在しない場合、ルータ ポートである場合、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場合も、このエントリは無視されます。

スイッチが新たなバインディングを学習した場合、または一部のバインディングを失った場合は、スイッチは変更された各エントリをスヌーピング データベースから抽出し、これらをファイルに書き込みます。より多くの変更を蓄積してから、実際の書き込みを一括して行えるように、この書き込みの実行には遅延時間を設定できます。個々の転送には、未完了の転送が中断されるまでの時間を示すタイムアウトが関連付けられます。このようなタイマーを、書き込み遅延および中断タイムアウトと呼びます。

DHCP スヌーピングのデフォルト設定

表 37-1 は、各 DHCP スヌーピング オプションのデフォルトの設定値を示します。

表 37-1　DHCP スヌーピングのデフォルト設定値

オプション	デフォルト値 / 状態
DHCP スヌーピング	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
信頼できないポート機能上の DHCP Option 82	ディセーブル
DHCP スヌーピング レート制限	なし
DHCP スヌーピング信頼状態	信頼しない
DHCP スヌーピング VLAN	ディセーブル

DHCP スヌーピング設定時の制約事項および注意事項

ここでは、DHCP スヌーピング設定時の制約事項および注意事項について説明します。

- 「DHCP スヌーピング設定時の制約事項」（P.37-7）
- 「DHCP スヌーピング設定時の注意事項」（P.37-8）
- 「DHCP スヌーピングの最小設定」（P.37-9）

DHCP スヌーピング設定時の制約事項

DHCP スヌーピングを設定する場合は、次の制約事項に注意してください。

- PFC2 は、DHCP スヌーピングをサポートしません。
- Release 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースには、最大 512 のバインディングが格納されます。データベースに 512 を超える DHCP バインディングを追加しようとすると、すべてのバインディングがデータベースから削除されます。
- Release 12.2(18)SXF5 以降のリリースでは、DHCP スヌーピング データベースには、8,000 以上のバインディングが格納されます。
- DHCP スヌーピングをイネーブルにすると、スイッチでは以下の Cisco IOS DHCP コマンドを使用できなくなります。
  - **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 option** 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

  これらのコマンドを入力すると、スイッチはエラー メッセージを返し、設定は適用されません。

DHCP スヌーピング設定時の注意事項

DHCP スヌーピングを設定する場合は、次の注意事項に従ってください。

- 少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにし、スイッチで DHCP をグローバルにイネーブルにするまで、DHCP スヌーピングは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には、DHCP サーバおよび DHCP リレー エージェントとして機能する装置を、事前に設定およびイネーブルにしておく必要があります。
- DHCP サーバの設定については、次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』の「Configuring DHCP」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm
- レイヤ 2 LAN 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、このポートを信頼できるポートとして設定します。
- レイヤ 2 LAN 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、このポートを信頼できないポートとして設定します。
- DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。
  - DHCP スヌーピングをイネーブルにすると、プライマリ VLAN の設定はすべて、関連付けられたセカンダリ VLAN に伝播します。
  - プライマリ VLAN で DHCP スヌーピングを設定してから、関連付けられたセカンダリ VLAN で DHCP スヌーピングを別の値で設定すると、セカンダリ VLAN の設定は無効になります。
  - プライマリ VLAN で DHCP スヌーピングが設定されていない場合に、関連付けられたセカンダリ VLAN で DHCP スヌーピングを設定すると、設定はセカンダリ VLAN のみで有効になります。
  - セカンダリ VLAN 上で DHCP スヌーピングを手動設定すると、次のメッセージが表示されます。

    ```
    DHCP Snooping configuration may not take effect on secondary vlan XXX
    ```

  - **show ip dhcp snooping** コマンドを実行すると、DHCP スヌーピングがイネーブルにされたすべての VLAN（プライマリおよびセカンダリを含む）が表示されます。

DHCP スヌーピングの最小設定

DHCP スヌーピング機能の最小設定手順は次のとおりです。

1. DHCP サーバを定義し、設定します。

   DHCP サーバの設定については、次の URL にある『*Cisco IOS IP and IP Routing Configuration Guide*』の「Configuring DHCP」を参照してください。

   http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

2. 少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにします。

   デフォルトでは、DHCP スヌーピングはすべての VLAN で非アクティブです。「VLAN 上での DHCP スヌーピングのイネーブル化」（P.37-13）を参照してください。

3. DHCP サーバが信頼できるインターフェイスを通じて接続されていることを確認します。

   デフォルトでは、すべてのインターフェイスの信頼状態は untrusted です。「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.37-14）を参照してください。

4. DHCP スヌーピング データベース エージェントを設定します。

   この手順により、再起動またはスイッチオーバー後にデータベース エントリが復元されるようになります。「DHCP スヌーピング データベース エージェントの設定」（P.37-16）を参照してください。

5. DHCP スヌーピングをグローバルにイネーブルにします。

   DHCP スヌーピングは、この手順を完了するまで有効になりません。「DHCP スヌーピングのグローバルなイネーブル化」（P.37-10）を参照してください。

DHCP リレーをスイッチで設定する場合、次の追加ステップが必要です。

1. DHCP リレー エージェントの IP アドレスを定義し、設定します。

   DHCP サーバが DHCP クライアントとは別のサブネット内にある場合、サーバ IP アドレスをクライアント側 VLAN のヘルパー アドレス フィールドに設定します。

2. 信頼できないポートに DHCP Option 82 を設定します。

   「信頼できないポート機能上での DHCP Option 82 のイネーブル化」（P.37-11）を参照してください。

DHCP スヌーピングの設定

ここでは、DHCP スヌーピングを設定する手順について説明します。

DHCP スヌーピングのグローバルなイネーブル化

（注）　最後の設定手順としてこのコマンドを設定します（またはスケジュールされているメンテナンス期間中に DHCP 機能をイネーブルにします）。DHCP スヌーピングをグローバルにイネーブル化すると、各ポートを設定しない限り、スイッチは DHCP 要求を廃棄するためです。

DHCP スヌーピングをグローバルにイネーブル化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。
	`Router(config)# no ip dhcp snooping`	DHCP スヌーピングをディセーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping | include Switch`	設定を確認します。

次に、DHCP スヌーピングをグローバルにイネーブル化する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# do show ip dhcp snooping | include Switch
Switch DHCP snooping is enabled
Router(config)#
```

（注）　DHCP スヌーピングをディセーブルにし、DAI をイネーブルにすると、ARP テーブル内のすべての ARP エントリが存在しない DHCP データベースと照合されるため、スイッチはすべてのホストをシャット ダウンします。DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用して ARP パケットの許可および拒否を行います。

DHCP Option 82 データ挿入のイネーブル化

DHCP Option 82 データ挿入をイネーブル化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping information option`	DHCP Option 82 データ挿入をイネーブルにします。
	`Router(config)# no ip dhcp snooping information option`	DHCP Option 82 データ挿入をディセーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping | include 82`	設定を確認します。

次に、DHCP Option 82 データ挿入をディセーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is disabled
Router#(config)
```

次に、DHCP Option 82 データ挿入をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option
Router(config)# do show ip dhcp snooping | include 82
Insertion of option 82 is enabled
Router#(config)
```

信頼できないポート機能上での DHCP Option 82 のイネーブル化

（注）　信頼できないポート機能で DHCP Option 82 をイネーブルにした場合、スイッチは信頼できないポートで受信された Option 82 情報を含む DHCP パケットを廃棄しません。任意の信頼できない装置が接続された集約スイッチでは、**ip dhcp snooping information option allowed-untrusted** コマンドを入力しないでください。

Release 12.2(18)SXF1 以降のリリースの場合、信頼できないポートで Option 82 情報を含む DHCP パケットを受信できるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping information option allow-untrusted`	（任意）信頼できないポートで Option 82 情報を含む着信 DHCP パケットを受信できるようにします。 デフォルト設定は、ディセーブルです。
	`Router(config)# no ip dhcp snooping information option allow-untrusted`	信頼できないポート機能上で DHCP Option 82 をディセーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping`	設定を確認します。

次に、信頼できないポート機能で DHCP Option 82 をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping information option allow-untrusted
Router#(config)
```

DHCP スヌーピングの MAC アドレス検証のイネーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルにすると、信頼できないポートで受信した DHCP パケット内の送信元 MAC アドレスとクライアント ハードウェア アドレスが一致するかどうかが検証されます。送信元 MAC アドレスはパケットに関連付けられたレイヤ 2 フィールドで、クライアント ハードウェア アドレスは DHCP パケット内のレイヤ 3 フィールドです。

DHCP スヌーピングの MAC アドレス検証をイネーブル化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。
	`Router(config)# no ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をディセーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping | include hwaddr`	設定を確認します。

次に、DHCP スヌーピングの MAC アドレス検証をディセーブルにする例を示します。

```
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is disabled
Router(config)#
```

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)# do show ip dhcp snooping | include hwaddr
Verification of hwaddr field is enabled
Router(config)#
```

VLAN 上での DHCP スヌーピングのイネーブル化

デフォルトでは、DHCP スネーピング機能はすべての VLAN で非アクティブです。DHCP スネーピング機能 は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

VLAN でイネーブルにすると、DHCP スヌーピング機能によって MFC3 の VACL テーブル内に 4 つのエントリが作成されます。これらのエントリにより、PFC3 がこの VLAN 上のすべての DHCP メッセージを代行受信し、MSFC に送信します。DHCP スヌーピング機能は MSFC のソフトウェアに実装されています。

VLAN 上で DHCP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping vlan {{vlan_ID [vlan_ID]} | {vlan_range}`	VLAN または VLAN 範囲に対して DHCP スヌーピングをイネーブルにします。
	`Router(config)# no ip dhcp snooping`	DHCP スヌーピングをディセーブルにします。
ステップ 2	`Router(config)# do show ip dhcp snooping`	設定を確認します。

DHCP スヌーピングは 1 つの VLAN、または特定の VLAN 範囲に対して設定できます。

- 1 つの VLAN に対して設定するには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲に対して設定するには、開始 VLAN 番号と終了 VLAN 番号を入力するか、または一組の VLAN 番号をダッシュ（-）でつなげて指定します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10 12
Router(config)#
```

次に、別の方法で VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12
```

次に、別の方法で VLAN 10 ～ 12 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10,11,12
```

次に、VLAN 10 ～ 12、および VLAN 15 で DHCP スヌーピングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-12,15
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following Interfaces:
```

```
Insertion of option 82 is enabled
Verification of hwaddr field is enabled
Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
Router#
```

レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定

レイヤ 2 LAN インターフェイス上で DHCP 信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {type[1] slot/port | port-channel number}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスのみを選択してください。
ステップ 2	`Router(config-if)# ip dhcp snooping trust`	インターフェイスを trusted として設定します。
	`Router(config-if)# no ip dhcp snooping trust`	デフォルトの信頼状態（untrusted）に戻します。
ステップ 3	`Router(config-if)# do show ip dhcp snooping | begin pps`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
FastEthernet5/12           yes         unlimited
Router#
```

次に、ファスト イーサネット ポート 5/12 を信頼できないポートとして設定する例を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
FastEthernet5/12           no          unlimited
Router#
```

レイヤ 2 LAN インターフェイスでの DHCP スヌーピング レート制限の設定

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {`*type*[1] *slot/port* | **port-channel** *number*`}`	設定するインターフェイスを選択します。 （注）　**switchport** コマンドで設定した LAN ポート、またはレイヤ 2 ポートチャネル インターフェイスのみを選択してください。
ステップ 2	`Router(config-if)# ip dhcp snooping limit rate` *rate*	DHCP パケットのレート制限を設定します。
ステップ 3	`Router(config-if)# no ip dhcp snooping limit rate`	DHCP パケットのレート制限をディセーブルにします。
ステップ 4	`Router(config-if)# do show ip dhcp snooping | begin pps`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

レイヤ 2 LAN インターフェイス上で DHCP スヌーピングのレート制限を設定する場合は、次の点に注意してください。

- 信頼できないインターフェイスでのレートは、100 pps（パケット / 秒）以下に制限することを推奨します。
- 信頼できるインターフェイスにレート制限を設定する場合は、DHCP スヌーピングをイネーブルにしている VLAN を複数収容するトランク ポートでは、レート制限を高い値に設定することを推奨します。
- DHCP スヌーピングでは、レート制限を超過したポートは errdisable ステートとなります。

次に、ファスト イーサネット ポート 5/12 を、DHCP パケットのレート制限によって 100 pps に制限する例を示します。

```
Router# configure terminal
Router(config)# interface FastEthernet 5/12
Router(config-if)# ip dhcp snooping limit rate 100
Router(config-if)# do show ip dhcp snooping | begin pps
Interface                      Trusted     Rate limit (pps)
------------------------       -------     ----------------
FastEthernet5/12               no          100
Router#
```

DHCP スヌーピング データベース エージェントの設定

DHCP スヌーピング データベース エージェントを設定するには、次の 1 つまたは複数の作業を行ってください。

コマンド	目的
`Router(config)# ip dhcp snooping database { _url | write-delay seconds | timeout seconds }`	（必須）データベース エージェント（またはファイル）の URL、および関連するタイムアウト値を設定します。
`Router(config)# no ip dhcp snooping database [write-delay | timeout]`	設定を消去します。
`Router# show ip dhcp snooping database [detail]`	（任意）データベース エージェントの現在の動作状態、および転送に関連する統計情報を表示します。
`Router# clear ip dhcp snooping database statistics`	（任意）データベース エージェントに関連する統計情報を消去します。
`Router# renew ip dhcp snooping database [validation none] [url]`	（任意）指定の URL にあるファイルから、エントリの読み取りを要求します。
`Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds`	（任意）バインディングをスヌーピング データベースに追加します。
`Router# no ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname`	（任意）スヌーピング データベースからバインディングを削除します。

DHCP スヌーピング データベース エージェントを設定する場合は、次の点に注意してください。

- Release 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースには、最大 512 のバインディングが格納されます。データベースに 512 を超える DHCP バインディングを追加しようとすると、すべてのバインディングがデータベースから削除されます。
- Release 12.2(18)SXF5 以降のリリースでは、DHCP スヌーピング データベースには、8,000 以上のバインディングが格納されます。
- スイッチの記憶装置の記憶領域が消費されることを避けるため、ファイルは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上に保存します。
- スイッチオーバーが発生した場合、TFTP からアクセス可能なリモート ロケーションにファイルが保存されていれば、新たにアクティブになったスーパーバイザ エンジンはこのバインディング リストを使用できます。
- ネットワーク ベースの URL（TFTP、File Transfer Protocol（FTP; 簡易転送プロトコル）など）では、スイッチが一連のバインディングを初めて書き込む前に、設定した URL に空のファイルを作成しておく必要があります。

データベース エージェントの設定例

ここでは、データベース エージェントの設定例を紹介します。

例 1：データベース エージェントのイネーブル化

次に、指定の場所にバインディングを保存するように DHCP スヌーピング データベース エージェントを設定し、この設定内容と動作状態を表示する例を示します。

```
Router# configure terminal
Router(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Router(config)# end
Router# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0

Router#
```

出力結果の最初の 3 行は、設定した URL、および関連するタイマー設定値を表します。次の 3 行は、動作状態のほか、書き込み遅延時間および中断タイマーが経過するまでに残された時間を表します。

出力結果にはこのほか、スタートアップ時の失敗として、スタートアップ時の読み取りまたはファイル作成の試みに失敗した回数が表示されます。

（注）　TFTP サーバ上に一時ファイルを作成するには、**touch** コマンドを使用して、TFTP サーバのデーモン ディレクトリ内に作成します。一部の UNIX 実装では、ファイルには完全な読み取りおよび書き込みアクセス許可（777）を設定する必要があります。

DHCP スヌーピング バインディングは、MAC アドレスと VLAN の組み合わせに重点を置いています。リモート ファイル内のエントリが、スイッチがすでにバインディングを持つ MAC アドレスと VLAN の組み合わせを表す場合は、リモート ファイルの読み取り時にこのエントリは無視されます。このような状態を、*バインディング コリジョン*と呼びます。

ファイル内のエントリに示されたリース期間が、ファイルの読み取り時にすでに経過している場合は、このエントリは無効になります。期限切れリース カウンタは、このような状況によって無視されたバインディングの数を示します。無効なインターフェイス カウンタは、読み取りが行われた時点で、エントリが参照するインターフェイスがシステム内にすでに存在しない場合、ルータである場合、または DHCP スヌーピングにおいて信頼できるインターフェイス（存在する場合）である場合に無視されたバインディングの数を示します。サポートされない VLAN は、エントリの示す VLAN がシステム上でサポートされない場合に無視されたエントリの数を示します。解析の失敗カウンタは、ファイル内のエントリの意味をスイッチが解析できなかった場合に無視されたエントリの数を示します。

スイッチは、このように無視されたバインディングに対し、2 種類のカウンタを維持します。1 つは、上記の条件が 1 つ以上該当するために無視された 1 つ以上のバインディングを持つ、個々の読み取りに対するカウンタです。このようなカウンタは「Last ignored bindings counters」として表示されます。「Total ignored bindings counters」は、スイッチのブートアップ後、すべての読み取りによって無視されたバインディングの合計数を示します。これらの 2 種類のカウンタは、**clear** コマンドによって消去されます。合計カウンタのセットは、最後に消去した時点からの無視されたバインディングの累積数と見なすことができます。

例 2：TFTP ファイルからのバインディング エントリの読み取り

TFTP ファイルからエントリを手動で読み取るには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show ip dhcp snooping database`	DHCP スヌーピング データベース エージェントの統計情報を表示します。
ステップ 2	`Router# renew ip dhcp snoop data` *url*	スイッチに、指定の URL からファイルを読み取るように指示します。
ステップ 3	`Router# show ip dhcp snoop data`	読み取りのステータスを表示します。
ステップ 4	`Router# show ip dhcp snoop bind`	バインディングの読み取りが適切に行われたかどうかを確認します。

次に、tftp://10.1.1.1/directory/file からエントリを手動で読み取る例を示します。

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router# renew ip dhcp snoop data tftp://10.1.1.1/directory/file
Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !
[OK - 457 bytes]
Database downloaded successfully.

Router#
00:01:29: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Read
succeeded.
Router# show ip dhcp snoop data
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : 15:24:34 UTC Sun Jul 8 2001
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        1   Failed Transfers :        0
Successful Reads     :        1   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Router#
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:05   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:02   1.1.1.1          49810       dhcp-snooping  512   GigabitEthernet1/1
00:01:00:01:00:04   1.1.1.1          49810       dhcp-snooping  1536  GigabitEthernet1/1
00:01:00:01:00:03   1.1.1.1          49810       dhcp-snooping  1024  GigabitEthernet1/1
00:01:00:01:00:01   1.1.1.1          49810       dhcp-snooping  1     GigabitEthernet1/1
Router# clear ip dhcp snoop bind
Router# show ip dhcp snoop bind
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Router#
```

例 3：DHCP スヌーピング データベースへの情報の追加

DHCP スヌーピング データベースにバインディングを手動で追加するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show ip dhcp snooping binding`	DHCP スヌーピング データベースを表示します。
ステップ 2	`Router# ip dhcp snooping binding binding_id vlan vlan_id interface interface expiry lease_time`	**ip dhcp snooping** EXEC コマンドを使用して、バインディングを追加します。
ステップ 3	`Router# show ip dhcp snooping binding`	DHCP スヌーピング データベースをチェックします。

次に、DHCP スヌーピング データベースにバインディングを手動で追加する例を示します。

```
Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Router#
Router# ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gi1/1 expiry 1000

Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          992         dhcp-snooping  1     GigabitEthernet1/1
Router#
```

バインディング テーブルの表示

個々のスイッチが持つ DHCP スヌーピング バインディング テーブルは、信頼できないポートに対応するバインディング エントリを保持します。このテーブルには、信頼できるポートと相互接続するホストについての情報は含まれません。相互接続する各スイッチは、それぞれ独自の DHCP スヌーピング バインディング テーブルを持つためです。

次に、スイッチの DHCP スヌーピング バインディング情報を表示する例を示します。

```
Router# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6943        dhcp-snooping  10    FastEthernet6/10
```

表 37-2 では、**show ip dhcp snooping binding** コマンドの出力結果における各フィールドについて説明します。

表 37-2　show ip dhcp snooping binding コマンドの出力結果

フィールド	説明
MAC Address	クライアント ハードウェアの MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアント IP アドレス
Lease (seconds)	IP アドレスのリース期間
Type	バインディング タイプ。DHCP スヌーピングによって学習されたダイナミック バインディングか、またはスタティックに設定されたバインディングです。
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続されるインターフェイス

CHAPTER 38

ダイナミック ARP 検査の設定

この章では、Catalyst 6500 シリーズ スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP 検査）を設定する方法について説明します。Release 12.2(18)SXE 以降のリリースでは、PFC3 は DAI をサポートします。PFC2 は、DAI をサポートしません。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

DAI の概要

ここでは、DAI によって ARP スプーフィング攻撃を防止する方法について説明します。

ARP の概要

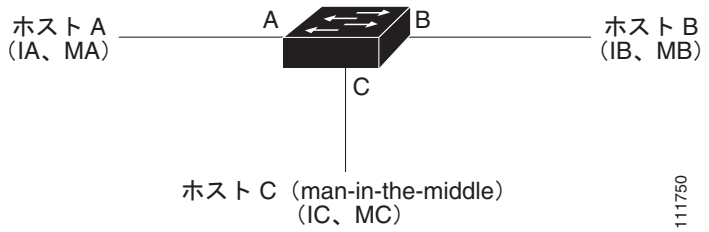
ARP では、IP アドレスを MAC（メディア アクセス制御）アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとする場合、ホスト B の ARP キャッシュにホスト A の MAC アドレスが存在しないとします。ホスト B は、ホスト A の IP アドレスに関連付けられた MAC アドレスを取得するために、ブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内の全ホストがこの ARP 要求を受信し、ホスト A が自身の MAC アドレスで応答します。

ARP スプーフィング攻撃の概要

ARP スプーフィング攻撃と ARP キャッシュ ポイズニングは、ARP 要求を受信していない場合でも ARP によってホストが無償応答できるため発生する可能性があります。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。攻撃が開始されると、攻撃を受けた機器からのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARP スプーフィング攻撃では、サブネットに接続されたシステムの ARP キャッシュをポイズニング（汚染）し、このサブネット上の他のホスト宛てのトラフィックを代行受信することで、レイヤ 2 ネットワークに接続されたホスト、スイッチ、およびルータを攻撃します。図 38-1 は、ARP キャッシュ ポイズニングの例を示します。

図 38-1　ARP キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してスイッチに接続されています。すべてのホストは同一サブネットに属します。カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A は IP アドレス [IA]、および MAC アドレス [MA] を使用します。ホスト A が IP レイヤ上でホスト B と通信する場合は、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを尋ねる ARP 要求をブロードキャストします。スイッチとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を持つホストのバインディングによって偽装した ARP 応答をブロードキャストすることで、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングできます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的なトポロジです。

DAI および ARP スプーフィング攻撃の概要

DAI は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。この機能により、一部の man-in-the-middle 攻撃からネットワークを保護できます。

DAI を使用することで、有効な ARP 要求および応答だけが中継されることを保証できます。スイッチの動作は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットは廃棄します。

DAI は信頼できるデータベースに保存された有効な IP アドレスおよび MAC アドレス バインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、DHCP スヌーピング バインディング データベースと呼びます。このデータベースは、VLAN およびスイッチ上で Dynamic Host Configuration Protocol（DHCP）スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。信頼できるインターフェイス上で ARP パケットを受信した場合は、スイッチはこのパケットを検査せずに転送します。信頼できないインターフェイスでは、スイッチは有効性を確認できたパケットのみを転送します。

DAI では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ定義の Access Control List（ACL; アクセス制御リスト）に照合することで ARP パケットを検証できます（「DAI フィルタリングのための ARP ACL の適用」（P.38-10）を参照）。スイッチは、廃棄されたパケットを記録します（「廃棄パケットのロギング」（P.38-5）を参照）。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットを廃棄するのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットを廃棄するのかを設定できます（「その他の検証のイネーブル化」（P.38-12）を参照）。

インターフェイスの信頼状態とネットワーク セキュリティ

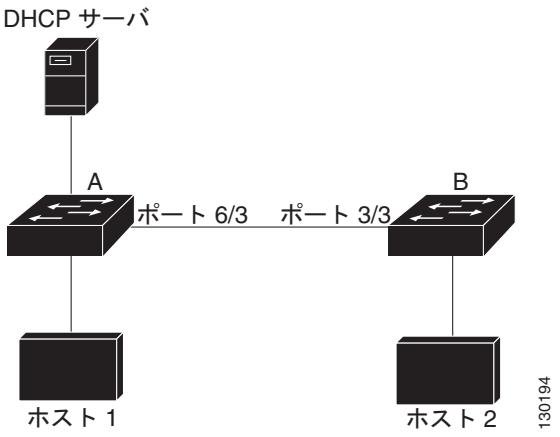
DAI は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク設定では、ホスト ポートに接続されているすべてのスイッチ ポートを信頼できないポートとして、スイッチに接続されているすべてのスイッチ ポートは信頼できるポートとして設定します。この設定では、特定スイッチからネットワークに送信されるすべての ARP パケットは、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

注意　信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 38-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 およびホスト 2 を含む VLAN 上で DAI を実行していると仮定します。ホスト 1 とホスト 2 がスイッチ A に接続されている DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP/MAC アドレスをバインドします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B では廃棄されます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 38-2　　DAI をイネーブルにした VLAN での ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A が DAI を実行していなければ、ホスト 1 はスイッチ B（スイッチ間のリンクが信頼可能として設定されている場合はホスト 2 も同様）の ARP キャッシュを簡単にポイズニングできます。この状況は、スイッチ B が DAI を実行している場合でも起こりえます。

DAI は、DAI を実行するスイッチに接続された、信頼できないインターフェイス上のホストが、ネットワーク内の他のホストの ARP キャッシュをポイズニングしないように保証します。しかし、ネットワークのその他の場所にあるホストが、DAI を実行するスイッチに接続されたホストのキャッシュをポイズニングする可能性は防止できません。

VLAN 内の一部のスイッチが DAI を実行し、他のスイッチは DAI を実行していない状況では、これらのスイッチに接続されたインターフェイスを信頼できないインターフェイスとして設定します。ただし、DAI が設定されていないスイッチからのパケットのバインディングを検証するには、DAI を実行するスイッチ上で ARP ACL を設定します。こうしたバインディングを判断できない場合は、レイヤ 3 において、DAI を実行するスイッチを DAI を実行しないスイッチから切り離します。設定の詳細については、「例 2：1 つのスイッチが DAI をサポートする場合」（P.38-22）を参照してください。

（注） DHCP サーバとネットワークのセットアップ方法によっては、VLAN 内のすべてのスイッチで、特定の ARP パケットを検証できない場合もあります。

ARP パケットのレート制限

スイッチは、DAI 有効性検査を実行することで着信 ARP パケットをレート制限して、Denial of Service（DoS; サービス拒絶）攻撃を防止します。デフォルトでは、信頼できないインターフェイスのレートは 15 pps（パケット/秒）です。信頼できるインターフェイスは、レート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト期間が経過すると、この状態から自動的に回復するようになります。

設定の詳細については、「ARP パケットのレート制限の設定」（P.38-11）を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

DAI では DHCP スヌーピング バインディング データベースを使用して、有効な IP アドレスおよび MAC アドレスのバインディング一覧を維持します。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL のほうが優先されます。ACL は、**ip arp inspection filter** グローバル コンフィギュレーション コマンドを使用してスイッチを設定した場合に限り、スイッチに適用されます。スイッチはまず、ARP パケットを、ユーザが設定した ARP ACL と照合します。ARP パケットが ARP ACL によって拒否される場合は、DHCP スヌーピングによって書き込まれた有効なバインディングがデータベース内に存在する場合であっても、スイッチはこのパケットを拒否します。

廃棄パケットのロギング

スイッチはパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージが生成されたあとは、スイッチはこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用すると、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定できます。ログ記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「DAI ログ機能の設定」（P.38-14）を参照してください。

DAI のデフォルト設定

表 38-1 に、DAI のデフォルト設定を示します。

表 38-1　DAI のデフォルト設定

機能	デフォルト設定
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	信頼できないインターフェイスでは、レートを 15 pps に制限。ネットワークがレイヤ 2 スイッチド ネットワークであり、ホストが 1 秒間に 15 の新規ホストに接続することが前提です。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットがログ記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

DAI 設定時の注意事項および制約事項

DAI を設定する場合は、次の注意事項および制約事項に従ってください。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されたホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI 検査が有効なドメインを、DAI 検査の行われないドメインから切り離します。これにより、DAI をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス バインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスをダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。詳細については、第 37 章「Dynamic Host Configuration Protocol（DHCP）スヌーピングの設定」を参照してください。
- DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可および拒否を行います。
- DAI は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされます。
- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポート チャネルの信頼状態を変更すると、スイッチはチャネルを構成するすべての物理ポートに対し、新たにこの信頼状態を設定します。
- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。
- 受信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートは、各ポートの集約値を考慮し、DAI をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用すると、レートを無制限として設定できます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN へのサービス拒絶攻撃を招く可能性があります。

DAI の設定

ここでは、DAI の設定手順について説明します。

VLAN での DAI のイネーブル化

VLAN で DAI をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip arp inspection vlan {vlan_ID | vlan_range}`	VLAN で DAI をイネーブルにします（デフォルトではディセーブル）。
	`Router(config)# no ip arp inspection vlan {vlan_ID | vlan_range}`	VLAN で DAI をディセーブルにします。
ステップ 3	`Router(config-if)# do show ip arp inspection vlan {vlan_ID | vlan_range} | begin Vlan`	設定を確認します。

DAI は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

- 1 つの VLAN でイネーブルにするには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲でイネーブルにするには、一組の VLAN 番号をダッシュ（-）でつなげて指定します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12
```

次に、VLAN 10 ～ 12 で DAI をイネーブルにするもう 1 つの方法を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10,11,12
```

次に、VLAN 10 ～ 12、および VLAN 15 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
Vlan      Configuration    Operation   ACL Match          Static ACL
 ----      -------------    ---------   ---------          ----------
   10      Enabled          Inactive
   11      Enabled          Inactive
   12      Enabled          Inactive
   15      Enabled          Inactive

 Vlan      ACL Logging      DHCP Logging
 ----      -----------      ------------
   10      Deny             Deny
   11      Deny             Deny
   12      Deny             Deny
   15      Deny             Deny
```

DAI インターフェイスの信頼状態の設定

スイッチは、信頼できるインターフェイスで受信した ARP パケットを転送しますが、そのパケットをチェックすることはしません。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求および ARP 応答を代行受信します。スイッチは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、または適切な宛先にパケットを転送します。スイッチは無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたログ設定に基づき、ログ バッファに廃棄パケットを記録します。詳細については、「DAI ログ機能の設定」（P.38-14）を参照してください。

DAI インターフェイスの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {`*type*[1] *slot/port* | **port-channel** *number*`}`	別のスイッチに接続されている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。
ステップ 3	`Router(config-if)# ip arp inspection trust`	スイッチ間の接続を、trusted として設定します（デフォルトでは untrusted）。
	`Router(config)# no ip arp inspection trust`	スイッチ間の接続を、untrusted として設定します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	DAI の設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# ip arp inspection trust
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/12
Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa5/12           Trusted              None               N/A
```

DAI フィルタリングのための ARP ACL の適用

（注）　**arp access-list** コマンドの詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

ARP ACL を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router# ip arp inspection filter` *arp_acl_name* **vlan** {*vlan_ID* | *vlan_range*} [**static**]	ARP ACL を VLAN に適用します。
ステップ 3	`Router(config)# do show ip arp inspection vlan` {*vlan_ID* | *vlan_range*}	設定を確認します。

ARP ACL を適用する場合は、次の点に注意してください。

- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲を指定するには、複数組の VLAN 番号をダッシュ（-）でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。
- （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 内のすべてのコマンドに一致しないパケットは廃棄されます。DHCP バインディングは使用されません。

  このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 内のどのコマンドとも一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。
- IP アドレスおよび MAC アドレスのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合のみに許可されます。

次に、example_arp_acl という名前の ARP ACL を、VLAN 10 ～ 12、および VLAN 15 に適用する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection filter example_arp_acl vlan 10-12,15
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Inactive    example_arp_acl   No
   11     Enabled          Inactive    example_arp_acl   No
   12     Enabled          Inactive    example_arp_acl   No
   15     Enabled          Inactive    example_arp_acl   No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
   11     Deny             Deny
   12     Deny             Deny
   15     Deny             Deny
```

ARP パケットのレート制限の設定

DAI をイネーブルにすると、スイッチは ARP パケットの有効性検査を実行します。これにより、スイッチは ARP パケットのサービス拒絶攻撃を受けやすくなります。ARP パケットをレート制限することで、ARP パケットのサービス拒絶攻撃を防止できます。

ARP パケットのレート制限をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {`*type*[1] *slot/port* | **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	`Router(config-if)# ip arp inspection limit {rate` *pps* `[burst interval` *seconds*`] | none}`	（任意）ARP パケットのレート制限を設定します。
	`Router(config-if)# no ip arp inspection limit`	ARP パケットのレート制限設定を解除します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ARP パケットのレート制限を設定する場合は、次の点に注意してください。

- デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。
- **rate** *pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。
- **rate none** キーワードは、処理できる着信 ARP パケットのレートに上限がないことを指定します。
- （任意）**burst interval** *seconds*（デフォルトは 1）には、インターフェイスをモニタして高レートの ARP パケットの有無を確認するための、連続するインターバルを秒単位で指定します。有効な範囲は 1 ～ 15 です。
- 着信 ARP パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ポートは、errdisable ステートの回復がイネーブルにされるまで、errdisable ステートを維持します。errdisable ステートの回復をイネーブルにすると、指定のタイムアウト時間が経過した時点で、ポートは errdisable ステートから回復します。
- インターフェイスのレート制限値を設定しない限り、インターフェイスの信頼状態を変更すると、このレート制限値も、設定した信頼状態に対応するデフォルト値に変更されます。レート制限値を設定すると、信頼状態を変更した場合でも、インターフェイスはこのレート制限値を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限値に戻ります。
- トランク ポートおよび EtherChannel ポートで受信される ARP パケットのレート制限を設定するうえでの注意事項については、「DAI 設定時の注意事項および制約事項」（P.38-7）を参照してください。

次に、ファスト イーサネット ポート 5/14 に ARP パケットのレート制限を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/14
Router(config-if)# ip arp inspection limit rate 20 burst interval 2
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/14
 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa5/14           Untrusted               20                  2
```

DAI errdisable ステート回復のイネーブル化

DAI の errdisable ステート回復をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# errdisable recovery cause arp-inspection`	（任意）DAI の errdisable ステート回復をイネーブルにします（デフォルトはディセーブル）。
	`Router(config-if)# no errdisable recovery cause arp-inspection`	DAI の errdisable ステート回復をディセーブルにします。
ステップ 3	`Router(config)# do show errdisable recovery | include Reason|---|arp-`	設定を確認します。

次に、DAI の errdisable ステート回復をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# errdisable recovery cause arp-inspection
Router(config)# do show errdisable recovery | include Reason|---|arp-
ErrDisable Reason    Timer Status
-----------------    --------------
arp-inspection       Enabled
```

その他の検証のイネーブル化

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証をイネーブルにすることができます。

追加検証をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip arp inspection validate {[dst-mac] [ip] [src-mac]}`	（任意）追加検証をイネーブルにします（デフォルトはなし）。
	`Router(config)# no ip arp inspection validate {[dst-mac] [ip] [src-mac]}`	追加検証をディセーブルにします。
ステップ 3	`Router(config)# do show ip arp inspection | include abled$`	設定を確認します。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。
- 各 **ip arp inspection validate** コマンドは、それまでに指定したコマンドの設定を上書きします。**ip arp inspection validate** コマンドによって **src** および **dst mac** 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証のみをイネーブルにした場合は、2 つめのコマンドの結果によって **src** および **dst mac** 検証がディセーブルになります。

- 次の追加検証を実行できます。
  - **dst-mac** - イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。
  - **ip** - ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内のみで検査されます。
  - **src-mac** - イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較して検査します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

次に、src-mac 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

次に、dst-mac 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、ip 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled
```

次に、src-mac および dst-mac 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、src-mac、dst-mac、および ip 追加検証をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection validate src-mac dst-mac ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
```

DAI ログ機能の設定

ここでは DAI ログ機能について説明します。

DAI ログ機能の概要

DAI はパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージが生成されたあとは、DAI はこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

1 つのログ バッファ エントリによって、複数のパケットを表現できます。たとえば、同じ ARP パラメータを持つ同一 VLAN 上で、1 つのインターフェイスが多数のパケットを受信した場合は、DAI のログ バッファではこれらのパケットが 1 つのエントリとして結合され、このエントリに対して 1 つのシステム メッセージが生成されます。

ログ バッファでオーバーフローが生じた場合は、1 つのログ イベントがログ バッファ内に収まらなかったことを意味し、**show ip arp inspection log** イネーブル EXEC コマンドによる出力が影響を受けます。この場合は、パケット数と時間のみが表示され、あとはデータの代わりに 2 つのダッシュ（--）が表示されます。このエントリに対しては、その他の統計情報は表示されません。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip arp inspection log-buffer entries` *number*	DAI のログ バッファ サイズを設定します（有効範囲は 0 ～ 1024）。
	`Router(config)# no ip arp inspection log-buffer entries`	デフォルトのバッファ サイズ（32）に戻します。
ステップ 3	`Router(config)# do show ip arp inspection log | include Size`	設定を確認します。

次に、DAI ログ バッファを 64 メッセージに設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer entries 64
Router(config)# do show ip arp inspection log | include Size
Total Log Buffer Size : 64
```

DAI のログ システム メッセージの設定

DAI のログ システム メッセージを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip arp inspection log-buffer logs` *number_of_messages* `interval` *length_in_seconds*	DAI のログ バッファ サイズを設定します。
	`Router(config)# no ip arp inspection log-buffer logs`	デフォルトのシステム メッセージ設定に戻します。
ステップ 3	`Router(config)# do show ip arp inspection log`	設定を確認します。

DAI のログ システム メッセージを設定する場合は、次の点に注意してください。

- **logs** *number_of_messages* の有効範囲は 0 ～ 1024 です（デフォルトは 5）。0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。
- **interval** *length_in_seconds* の有効範囲は 0 秒 ～ 86400 秒（1 日）です（デフォルトは 1）。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。インターバル値を 0 に設定すると、ログ値 0 は上書きされます。
- システム メッセージは、*length_in_seconds* 秒あたり *number_of_messages* 個の割合で送信されます。

次に、2 秒あたり 12 個メッセージが送信されるように DAI のログ レートを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 12 interval 2
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 12 entries per 2 seconds.
```

次に、60 秒あたり 20 個のメッセージが送信されるように DAI のログ レートを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 20 interval 60
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 20 entries per 60 seconds.
```

DAI のログ フィルタリングの設定

DAI のログ フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip arp inspection vlan` *vlan_range* `logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}`	各 VLAN に対するログ フィルタリングを設定します。
ステップ 3	`Router(config)# do show running-config | include ip arp inspection vlan` *vlan_range*	設定を確認します。

DAI のログ フィルタリングを設定する場合は、次の点に注意してください。

- デフォルトでは、拒否されたすべてのパケットがログ記録されます。
- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲を指定するには、複数組の VLAN 番号をダッシュ（-）でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。
- **acl-match matchlog** - DAI ACL の設定に基づきパケットをログ記録します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト設定コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットがログ記録されます。
- **acl-match none** - ACL と一致したパケットをログ記録しません。
- **dhcp-bindings all** - DHCP バインディングと一致したすべてのパケットがログ記録されます。
- **dhcp-bindings none** - DHCP バインディングと一致したパケットはログ記録されません。
- **dhcp-bindings permit** - DHCP バインディングによって許可されたパケットがログ記録されます。

次に、VLAN 100 の DAI ログ フィルタリングを、ACL と一致したパケットをログ記録しないように設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection vlan 100 logging acl-match none
Router(config)# do show running-config | include ip arp inspection vlan 100
ip arp inspection vlan 100 logging acl-match none
```

DAI 情報の表示

DAI 情報を表示するには、表 38-2 に示す各イネーブル EXEC コマンドを使用します。

表 38-2　DAI 情報を表示するためのコマンド

コマンド	説明
show arp access-list [*acl_name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [*interface_id*]	指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対して、ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan_range*	指定の VLAN に対し、DAI の設定内容および動作状態を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN のみの情報が表示されます。

DAI 統計情報を消去または表示するには、表 38-3 に示す各イネーブル EXEC コマンドを使用します。

表 38-3　DAI 統計情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection statistics	DAI 統計情報を消去します。
show ip arp inspection statistics [**vlan** *vlan_range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可または拒否されたパケット、DHCP によって許可または拒否されたパケットの統計情報を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN のみの情報が表示されます。

show ip arp inspection statistics コマンドでは、スイッチは信頼できる DAI ポートにおいて、個々の ARP 要求および応答パケットに対して転送されたパケット数を増分します。スイッチは送信元 MAC、宛先 MAC、または IP 検証の結果拒否された各パケットに対し、ACL によって許可されたかまたは DHCP によって許可されたパケットの数を 1 つ増やします。また、スイッチは、該当する失敗回数の値も 1 つ増やします。

DAI ログ情報を消去または表示するには、表 38-4 に示す各イネーブル EXEC コマンドを使用します。

表 38-4　DAI ログ情報を消去または表示するためのコマンド

コマンド	説明
clear ip arp inspection log	DAI のログ バッファを消去します。
show ip arp inspection log	DAI ログ バッファの設定および内容を表示します。

DAI の設定例

ここでは、次の例について説明します。

例 1：2 つのスイッチが DAI をサポートする場合

この手順は、2 つのスイッチが DAI 機能をサポートする場合の DAI の設定方法を示します。図 38-2（P.38-4）に示すように、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。両方のスイッチは、各ホストが属する VLAN 1 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されています。方法のホストは、同一の DHCP サーバから IP アドレスを取得します。スイッチ A はホスト 1 およびホスト 2 のバインディングを持ち、スイッチ B はホスト 2 のバインディングを持ちます。スイッチ A のファスト イーサネット ポート 6/3 は、スイッチ B のファスト イーサネット ポート 3/3 に接続されています。

（注）

- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス バインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスをダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。詳細については、第 37 章「Dynamic Host Configuration Protocol（DHCP）スヌーピングの設定」を参照してください。
- この構成は、DHCP サーバがスイッチ A から別の場所に移動されてしまうと機能しません。
- この構成によってセキュリティが損なわれないようにするには、スイッチ A のファスト イーサネット ポート 6/3、およびスイッチ B のファスト イーサネット ポート 3/3 を、信頼できるポートとして設定します。

スイッチ A の設定

スイッチ A において DAI をイネーブルにし、ファスト イーサネット ポート 6/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　スイッチ A およびスイッチ B 間の接続を確認します。

```
スイッチA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
スイッチB          Fas 6/3           177         R S I     WS-C6506  Fas 3/3
スイッチA#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
スイッチA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチA(config)# ip arp inspection vlan 1
スイッチA(config)# end
スイッチA# show ip arp inspection vlan 1
```

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
スイッチA#
```

ステップ 3　ファスト イーサネット ポート 6/3 を、信頼できるポートとして設定します。

```
スイッチA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチA(config)# interface fastethernet 6/3
スイッチA(config-if)# ip arp inspection trust
スイッチA(config-if)# end
スイッチA# show ip arp inspection interfaces fastethernet 6/3

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted              None
スイッチA#
```

ステップ 4　バインディングを確認します。

```
スイッチA# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:00:02:00:02   1.1.1.2          4993        dhcp-snooping  1     FastEthernet6/4
スイッチA#
```

ステップ 5　DAI がパケットを処理する前、および後の統計情報を調べます。

```
スイッチA# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                 0                        0
スイッチA#
```

このあと、ホスト 1 が IP アドレス 1.1.1.2 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
スイッチA# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0
```

```
 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
スイッチA#
```

ホスト 1 がこのあと、IP アドレス 1.1.1.3 を持つ ARP 要求を送信しようとすると、このパケットは廃棄され、エラー メッセージがログ記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa6/4, vlan
1.([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])
スイッチA# show ip arp inspection statistics vlan 1
スイッチA#
```

この場合に表示される統計情報は次のようになります。

```
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              2              2              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
スイッチA#
```

スイッチ B の設定

スイッチ B において DAI をイネーブルにし、ファスト イーサネット ポート 3/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　接続を確認します。

```
スイッチA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
スイッチB          Fas 3/3           120         R S I     WS-C6506  Fas 6/3
スイッチB#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
スイッチB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチB(config)# ip arp inspection vlan 1
スイッチB(config)# end
スイッチB# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active
```

```
 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
スイッチB#
```

ステップ 3　ファスト イーサネット ポート 3/3 を、信頼できるポートとして設定します。

```
スイッチB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチB(config)# interface fastethernet 3/3
スイッチB(config-if)# ip arp inspection trust
スイッチB(config-if)# end
スイッチB# show ip arp inspection interfaces

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted              15
 Gi1/2            Untrusted              15
 Gi3/1            Untrusted              15
 Gi3/2            Untrusted              15
 Fa3/3            Trusted               None
 Fa3/4            Untrusted              15
 Fa3/5            Untrusted              15
 Fa3/6            Untrusted              15
 Fa3/7            Untrusted              15

<output truncated>
スイッチB#
```

ステップ 4　DHCP スヌーピング バインディングのリストを確認します。

```
スイッチB# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:00:01:00:01   1.1.1.1          4995        dhcp-snooping  1     FastEthernet3/4
スイッチB#
```

ステップ 5　DAI がパケットを処理する前、および後の統計情報を調べます。

```
スイッチB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1             0              0              0             0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
スイッチB#
```

ホスト 2 がこのあと、IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報も適切に更新されます。

```
スイッチB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1             1              0              0             0
```

```
 Vlan    DHCP Permits    ACL Permits   Source MAC Failures
 ----    ------------    -----------   -------------------
    1               1              0                     0

 Vlan    Dest MAC Failures   IP Validation Failures
 ----    -----------------   ----------------------
    1                    0                       0
スイッチB#
```

ホスト 2 が IP アドレス 1.1.1.2 を持つ ARP 要求を送信しようとすると、この要求は廃棄され、システム メッセージがログ記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/4, vlan
1.([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri May 23 2003])
スイッチB#
```

この場合に表示される統計情報は次のようになります。

```
スイッチB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1               1              1              1              0

 Vlan    DHCP Permits    ACL Permits   Source MAC Failures
 ----    ------------    -----------   -------------------
    1               1              0                     0

 Vlan    Dest MAC Failures   IP Validation Failures
 ----    -----------------   ----------------------
    1                    0                       0
スイッチB#
```

例 2：1 つのスイッチが DAI をサポートする場合

この手順では、スイッチ に示す図 38-2（P.38-4）B が、DAI および DHCP スヌーピングをサポートしていない場合に DAI を設定する方法を示します。

スイッチ B が DAI および DHCP スヌーピングをサポートしていない場合は、スイッチ A のファスト イーサネット ポート 6/3 を信頼できるポートとして設定すると、セキュリティ ホールが生じます。これは、スイッチ A およびホスト 1 が、スイッチ B またはホスト 2 によって攻撃される可能性があるためです。

この可能性を排除するには、スイッチ A のファスト イーサネット ポート 6/3 を信頼できないポートとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない場合は、スイッチ A に ACL 設定を適用できなくなるため、レイヤ 3 でスイッチ B からスイッチ A を切り離す必要があります。これらのスイッチ間では、ルータを使用してパケットをルーティングします。

スイッチ A に対して ARP ACL をセットアップするには、次の作業を行います。

ステップ 1　IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を許可するアクセス リストを設定して、設定内容を確認します。

```
スイッチA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチA(config)# arp access-list H2
スイッチA(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
スイッチA(config-arp-nacl)# end
スイッチA# show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 0001.0001.0001
```

ステップ 2　VLAN 1 に ACL を適用して、設定を確認します。

```
スイッチA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチA(config)# ip arp inspection filter H2 vlan 1
スイッチA(config)# end
スイッチA#

スイッチA# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      H2                No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
スイッチA#
```

ステップ 3　ファスト イーサネット ポート 6/3 を信頼できないポートとして設定し、設定内容を確認します。

```
スイッチA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチA(config)# interface fastethernet 6/3
スイッチA(config-if)# no ip arp inspection trust
スイッチA(config-if)# end
Switch# show ip arp inspection interfaces fastethernet 6/3

 Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Untrusted               15

Switch#
```

ホスト 2 がスイッチ A のファスト イーサネット ポート 6/3 から 5 つの ARP 要求を送信し、1 つの get 要求がスイッチ A によって許可された場合は、統計情報は次のように適切に更新されます。

```
Switch# show ip arp inspection statistics vlan 1
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              5              0              0              0
Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              5                    0
Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
Switch#
```

CHAPTER 39

トラフィック ストーム制御の設定

この章では、Catalyst 6500 シリーズ スイッチに、トラフィック ストーム制御機能を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

トラフィック ストーム制御の概要

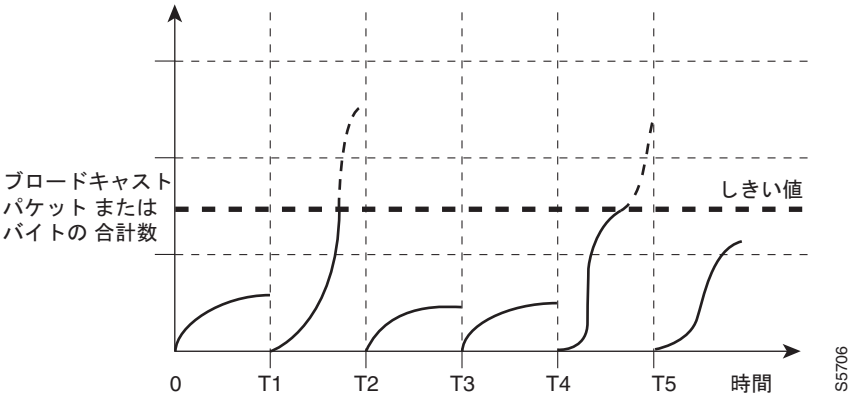
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、LAN ポートが、物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャスト トラフィック ストームによって中断されるのを防ぎます。

トラフィック ストーム制御（トラフィック抑制）は着信トラフィック レベルを、1 秒ごとのトラフィック ストーム制御でモニタします。そのインターバルの中で、トラフィック レベルを、設定したトラフィック ストーム制御レベルと比較します。トラフィック ストーム制御レベルは、ポートの利用可能な帯域幅全体に対するパーセンテージです。各ポートには、すべてのタイプのトラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）用に使用されている単一のトラフィック ストーム制御レベルがあります。

トラフィック ストーム制御は、1 秒ごとのトラフィック ストーム制御で、トラフィック ストーム制御をイネーブルにする各トラフィック タイプのレベルをモニタします。1 つのインターバルの中で、トラフィック ストーム制御がイネーブルにされている入力トラフィックが、ポートで設定されているトラフィック ストーム制御レベルに達する場合、トラフィック ストーム制御は、そのトラフィック ストーム制御インターバルが終了するまでトラフィックを廃棄します。

図 39-1 に、指定したインターバルでの LAN インターフェイス上のブロードキャスト トラフィック パターンを示します。この例では、T1 と T2 の時間の間と T4 と T5 の間でトラフィック ストーム制御が発生しています。これらのインターバルの間で、ブロードキャスト トラフィックの総量が設定されたスレッシュホールドを超過しています。

図 39-1　　ブロードキャスト抑制



トラフィック ストーム制御スレッシュホールドの数値と時間インターバルの組み合わせにより、トラフィック ストーム制御アルゴリズムがさまざまなレベルの粒度で機能します。スレッシュホールドが高くなると、より多くのパケットを通過させることができます。

Catalyst 6500 シリーズ スイッチのトラフィック ストーム制御は、ハードウェアに実装されています。トラフィック ストーム制御回路は、LAN インターフェイスからスイッチング バスに送信されるパケットをモニタします。パケット宛先アドレスの個別/グループ ビットを使用して、トラフィック ストーム制御回路はパケットがユニキャストかブロードキャストかを判断し、現在のパケット カウントを 1 秒間隔で追跡し続けて、スレッシュホールドに達すると、後続のパケットをフィルタ アウトします。

ハードウェア トラフィック ストーム制御では帯域ベースの方式を使用してトラフィックを測定しているので、制御されたトラフィックで利用可能な帯域幅全体に対するパーセンテージの設定が最も重要な実装要因となります。パケットは一定間隔で着信しないので、制御されたトラフィック アクティビティを 1 秒間隔で測定することは、トラフィック ストーム制御の動作に影響する可能性があります。

次に、トラフィック ストーム制御動作の例を示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにし、ブロードキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャスト トラフィックを廃棄します。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、そのブロードキャストとマルチキャスト トラフィックの合計が 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックを廃棄します。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、ブロードキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックを廃棄します。
- ブロードキャストおよびマルチキャスト トラフィック ストーム制御をイネーブルにし、マルチキャスト トラフィックが 1 秒間のトラフィック ストーム制御の間に制御レベルを超える場合、トラフィック ストーム制御はそのトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャストおよびマルチキャスト トラフィックを廃棄します。

トラフィック ストーム制御のデフォルト設定

トラフィック ストーム制御は、デフォルトではディセーブルに設定されています。

トラフィック ストーム制御に関する注意事項および制約事項

トラフィック ストーム制御を設定する場合は、次の注意事項および制約事項に従ってください。

- 次のスイッチング モジュールは、トラフィック ストーム制御をサポートしません。
  - WS-X6148A-GE-45AF
  - WS-X6148A-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6148-GE-TX
  - WS-X6148V-GE-TX
  - WS-X6548-GE-45AF
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
- スイッチは、マルチキャストとユニキャストのトラフィック ストーム制御を、ギガビットおよび 10 ギガビット イーサネット LAN ポートでサポートします。ほとんどのファスト イーサネット スイッチング モジュールは、マルチキャストとユニキャストのトラフィック ストーム制御をサポートしませんが、WS-X6148A-RJ-45 と WS-X6148-SFP はサポートします。
- スイッチは、上記のモジュールを除く、すべての LAN ポートでブロードキャスト トラフィック ストーム制御をサポートします。
- BPDU を除き、トラフィック ストーム制御は、制御トラフィックとデータトラフィックを区別しません。
- マルチキャスト抑制をイネーブルにすると、以下のモジュールでマルチキャスト抑制スレッシュホールドが超過した場合に、トラフィック ストーム制御によって BPDU が抑制されます。
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX
  - WS-X6748-GE-TX
  - WS-X6704-10GE
  - WS-SUP32-GE-3B
  - WS-SUP32-10GE-3B

  上記のモジュールでマルチキャスト抑制をイネーブルにする場合は、BPDU を受信する必要がある STP 保護されたポートには、トラフィック ストーム制御を設定しないでください。

  上記のモジュール以外では、BPDU はトラフィック ストーム制御によって抑制されません。

トラフィック ストーム制御のイネーブル化

トラフィック ストーム制御をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**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 2	Router(config-if)# **storm-control broadcast level** *level*[*.level*]	インターフェイス上のブロードキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
	Router(config-if)# **no storm-control broadcast level**	インターフェイス上のブロードキャスト トラフィック ストーム制御をディセーブルにします。
ステップ 3	Router(config-if)# **storm-control multicast level** *level*[*.level*] （注）　**storm-control multicast** コマンドは、ギガビット イーサネット インターフェイスでのみサポートされています。	インターフェイス上のマルチキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
	Router(config-if)# **no storm-control multicast level**	インターフェイス上のマルチキャスト トラフィック ストーム制御をディセーブルにします。
ステップ 4	Router(config-if)# **storm-control unicast level** *level*[*.level*] （注）　**storm-control unicast** コマンドは、ギガビット イーサネット インターフェイスでのみサポートされています。	インターフェイス上のユニキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
	Router(config-if)# **no storm-control unicast level**	インターフェイス上のユニキャスト トラフィック ストーム制御をディセーブルにします。
ステップ 5	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 6	Router# **show running-config** *interface*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

トラフィック ストーム制御レベルを設定する場合、次の点に注意してください。

- トラフィック ストーム制御は、EtherChannel（ポート チャネル インターフェイス）に設定できます。
- トラフィック ストーム制御を、EtherChannel のメンバであるポートに設定しないでください。トラフィック ストーム制御を EtherChannel のメンバとして設定されているポートに設定すると、そのポートは中断状態になります。
- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。

- 次のモジュールでは、次のレベルですべてのトラフィックが抑制されます。
  - WS-X6704-10GE：0.33% 以下
  - WS-X6724-SFP 10Mbps ポート：0.33% 以下
  - WS-X6748-SFP 100Mbps ポート：0.03% 以下
  - WS-X6748-GE-TX 100Mbps ポート：0.03% 以下
  - WS-X6716-10G-3C / 3CXL オーバーサブスクリプション モード：0.29% 以下

ハードウェアの制限および方式によってサイズの異なるパケットがカウントされるため、レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズにより、実際に実行されるレベルは、設定レベルと数 % 程度異なる場合があります。

次に、ギガビット イーサネット インターフェイス 3/16 でマルチキャスト トラフィック ストーム制御をイネーブルにして、トラフィック ストーム制御レベルを 70.5% に設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control multicast level 70.5
Router(config-if)# end
```

次に、1 つのモード用に設定されているトラフィック ストーム制御レベルがギガビット イーサネット インターフェイス 4/10 上にすでに設定されている他のすべてのモードに影響する例を示します。

```
Router# show run inter gig4/10
Building configuration...

Current configuration : 176 bytes
!
Router# interface GigabitEthernet4/10
Router# switchport
Router# switchport mode access
Router# storm-control broadcast level 70.00
Router# storm-control multicast level 70.00
Router# spanning-tree portfast edge
Router# end

Router# configure terminal
Router(config)# interface gigabitethernet 4/10
Router(config-if)# storm-control unicast level 20
Router(config-if)# end

Router# show interfaces gig4/10 counters storm-control

Port      UcastSupp %     McastSupp %     BcastSupp %  TotalSuppDiscards
Gi4/10      20.00           20.00           20.00              0

Router#
```

トラフィック ストーム制御設定の表示

トラフィック ストーム制御情報を表示するには、表 39-1 に記載されているコマンドを使用します。

表 39-1　トラフィック ストーム制御のステータスと設定の表示用コマンド

コマンド	目的
Router# **show interfaces** [{*type*[1] *slot/port*} | {**port-channel** *number*}] **switchport**	すべてのレイヤ 2 LAN ポートまたは特定のレイヤ 2 LAN ポートの管理および動作ステータスを表示します。
Router# **show interfaces** [{*type*[1] *slot/port*} | {**port-channel** *number*}] **counters storm-control** Router# **show interfaces counters storm-control** [**module** *slot_number*]	すべてのインターフェイス上、または指定のインターフェイス上で、3 つのトラフィック ストーム制御モードすべてで廃棄される合計パケット数を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

（注）　**show interfaces** [{*interface_type slot/port*} | {**port-channel** *number*}] **counters** コマンドは、廃棄数を表示しません。廃棄数を表示するには、**storm-control** キーワードを使用する必要があります。

CHAPTER 40

不明なユニキャスト / マルチキャスト フラッディングのブロック

この章では、不明なユニキャスト フラッディングのブロック（UUFB）機能と不明なマルチキャスト フラッディングのブロック（UMFB）機能を Catalyst 6500 シリーズ スイッチ上で設定する方法について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

UUFB および UMFB の概要

デフォルトでは、不明なユニキャスト/マルチキャスト トラフィックは、VLAN 上のすべてのレイヤ 2 ポートにフラッディングされます。UUFB 機能および UMFB 機能を使用してこのトラフィックを防止または制限すれば、この動作を防止することができます。UUFB 機能と UMFB 機能は、特定のポートでの不明なユニキャスト/マルチキャスト フラッディングをブロックし、そのポート上に存在するとわかっている MAC アドレスを持つ出力トラフィックだけを許可します。UUFB 機能と UMFB 機能は、Private VLAN（PVLAN）ポートも含め、**switchport** コマンドで設定したすべてのポートでサポートされます。

（注） VLAN のノンレシーバー（ルータ）ポートに **switchport block multicast** コマンドを入力すると、ルーティング プロトコルが中断される場合があります。このコマンドは、ARP 機能や、224.0.0.0/24 の範囲内のローカル サブネットワーク マルチキャスト制御グループを使用するその他のプロトコル（Network Time Protocol（NTP）など）も中断する場合があります。

UUFB の設定

UUFB または UFMB を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface {{`*type*[1] *slot/port*`} | {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	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチング用に設定します。
ステップ 4	`Router(config-if)# switchport block {unicast | multicast}`	ポート上での不明ユニキャスト フラッディングのブロックまたは不明マルチキャスト フラッディングのブロックをイネーブルにします。
ステップ 5	`Router(config-if)# do show interfaces [`*type*[1] *slot/port*`] switchport | include Unknown`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/12 に対して UUFB 設定をし、この内容を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport block unicast
Router(config-if)# do show interface fastethernet 5/12 switchport | include Unknown
不明ユニキャストのブロック：イネーブル
```

CHAPTER 41

PFC QoS の設定

この章では、Catalyst 6500 シリーズ スイッチの Policy Feature Card（PFC; ポリシー フィーチャ カード）および Distributed Forwarding Card（DFC）に実装された Quality of Service（QoS; サービス品質）機能を設定する方法について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。
- http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html QoS および MPLS の詳細については、第 42 章「PFC3BXL または PFC3B モード MPLS QoS の設定」を参照してください。
- Catalyst 6500 シリーズ スイッチの QoS（PFC QoS）では、Cisco IOS の Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）をいくつか使用します。PFC QoS はハードウェアに実装されているため、一部の MQC 構文だけがサポートされます。
- PFC3 は、Network-Based Application Recognition（NBAR）をサポートしていません。
- Supervisor Engine 2、PFC2、および Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を使用すると、レイヤ 3 インターフェイスに、PFC QoS の代わりに NBAR を設定できます。
  - PFC2 は、NBAR を設定したポートで、入力 Access Control List（ACL; アクセス制御リスト）をハードウェアでサポートします。
  - PFC QoS がイネーブルの場合、NBAR を設定しているポートを通過するトラフィックは、入力キュー、出力キューおよび廃棄スレッシュホールドを通過します。
  - PFC QoS がイネーブルの場合、MSFC2 は、NBAR トラフィック内の出力 IP precedence と等しくなるように出力 Class of Service（CoS; サービス クラス）を設定します。
  - 入力キューの通過後、すべてのトラフィックは、NBAR を設定したインターフェイス上の MSFC2 ソフトウェアで処理されます。
  - NBAR を設定するには、次のマニュアルを参照してください。
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

この章で説明する内容は、次のとおりです。

PFC QoS の機能概要

「PFC QoS」という用語は、Catalyst 6500 シリーズ スイッチに実装された QoS を意味します。PFC QoS は PFC やすべての DFC のほか、さまざまなスイッチ コンポーネントに実装されます。ここでは、PFC QoS の機能について説明します。

PFC QoS によってサポートされるポート タイプ

PFC は、FlexWAN モジュール ポートに対して QoS を提供しません。FlexWAN モジュール の QoS 機能については、次の資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm

すべてのリリースで、PFC QoS は *LAN ポート*をサポートします。LAN ポートとは、4 ポート ギガビット イーサネット WAN（GBIC）モジュール（OSM-4GE-WAN および OSM-2+4GE-WAN+）を除く、イーサネット スイッチング モジュール上のイーサネット ポートです。一部の Optical Services Module（OSM; オプティカル サービス モジュール）は、WAN ポートのほかに 4 つのイーサネット LAN ポートを備えています。

Release 12.2(17b)SXA 以降のリリースでは、PFC QoS はオプティカル サービス モジュール（OSM）ポートをサポートします。*OSM ポート*とは、OSM 上の WAN ポートです。その他の OSM QoS 機能については、次の資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

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、適度なタイミングで配信される可能性はどのトラフィックでも同等です。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等です。

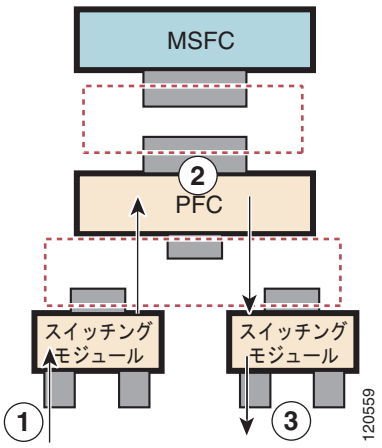
QoS を実装すると、ネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できます。QoS 機能は、ネットワーク トラフィックを選択（分類）し、プライオリティを示す QoS ラベルを割り当て、使用します。これにより、パケットは設定されたリソース使用制限に従い（トラフィックのポリシングとマーキング）、リソースの競合が生じた場合に輻輳回避が行われます。

PFC QoS 分類、ポリシング、マーキング、および輻輳回避は、PFC、DFC、および LAN スイッチング モジュール ポートの Application Specific Integrated Circuit（ASIC; 特定用途向け IC）のハードウェアに実装されます。

（注）　Catalyst 6500 シリーズ スイッチでは、レイヤ 3 またはレイヤ 2 でハードウェアによってスイッチングされたトラフィックに対し、一部の MQC 機能（Committed Access Rate（CAR; 専用アクセス レート）など）がサポートされません。キューイングはポートの ASIC に実装されるため、Catalyst 6500 シリーズ スイッチでは、MQC によって設定したキューイングはサポートされません。

図 41-1 は、Catalyst 6500 シリーズ スイッチにおける QoS 処理の概要を示します。

図 41-1　PFC QoS 機能による処理の概要



各 PFC QoS 機能は、次の順序で適用されます。

1. 入力ポートの PFC QoS 機能：
   - ポートの信頼状態 - PFC QoS における*信頼*とは、有効なポートとして受け入れられ、初期内部 DSCP 値の基準として使用されることを意味します。デフォルトではポートは信頼されず（untrusted）、初期内部 DSCP 値は 0 に設定されます。各ポートは、受信する CoS、IP precedence、または DSCP を信頼するように設定できます。
   - レイヤ 2 の CoS 再マーキング - PFC QoS は、レイヤ 2 CoS の再マーキングを適用します。この機能では、次の状況において、受信フレームにポートの CoS 値がマークされます。
     — トラフィックの形式が ISL、802.1Q、または 802.1p フレームではない場合
     — ポートが非信頼ポートとして設定されている場合
     OSM ATM および POS ポートでは、PFC QoS は入力 CoS を常に 0 に設定します。
   - 輻輳回避 - イーサネット LAN ポートを CoS または DSCP を信頼するように設定している場合は、QoS はレイヤ 2 CoS 値またはレイヤ 3 DSCP 値に基づきトラフィックを分類し、入力キューに割り当てることで、輻輳回避を行います。レイヤ 3 DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートだけで有効です。
2. PFC および DFC QoS 機能：
   - 内部 DSCP - PFC および DFC 上で、QoS はすべてのトラフィックに内部 DSCP 値を関連付け、システム内で処理できるように分類します。トラフィックの信頼状態に基づいて生成される初期内部 DSCP 値、および最終内部 DSCP 値が存在します。最終内部 DSCP は、初期値と同じである場合も、MQC ポリシー マップによって別の値に設定される場合もあります。
   - MQC ポリシー マップ - MQC ポリシー マップでは、次の 1 つまたは複数の処理が実行されます。
     — トラフィックの信頼状態の変更（内部 DSCP 値を別の QoS ラベルに基づいて設定）
     — 初期内部 DSCP 値の設定（信頼できないポートからのトラフィックに限る）
     — トラフィックのマーキング
     — トラフィックのポリシング

3. 出力イーサネット LAN ポートの QoS 機能：
   - 最終内部 DSCP によるレイヤ 3 DSCP マーキング（PFC2 では標準、PFC3 ではオプション）
   - 最終内部 DSCP からのマッピングによるレイヤ 2 CoS マーキング
   - レイヤ 2 CoS ベース、およびレイヤ 3 DSCP ベースの輻輳回避 （レイヤ 3 DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートだけで有効）

次の図は、QoS とスイッチ コンポーネント間の関係の詳細を示します。

- 図 41-2, PFC3 でのトラフィック フローおよび PFC QoS 機能
- 図 41-3, PFC2 でのトラフィック フローおよび PFC QoS 機能
- 図 41-4, PFC QoS 機能とコンポーネントの概要

図 41-2 は、PFC3 でのトラフィック フローと PFC QoS 機能を示します。

図 41-2　PFC3 でのトラフィック フローおよび PFC QoS 機能

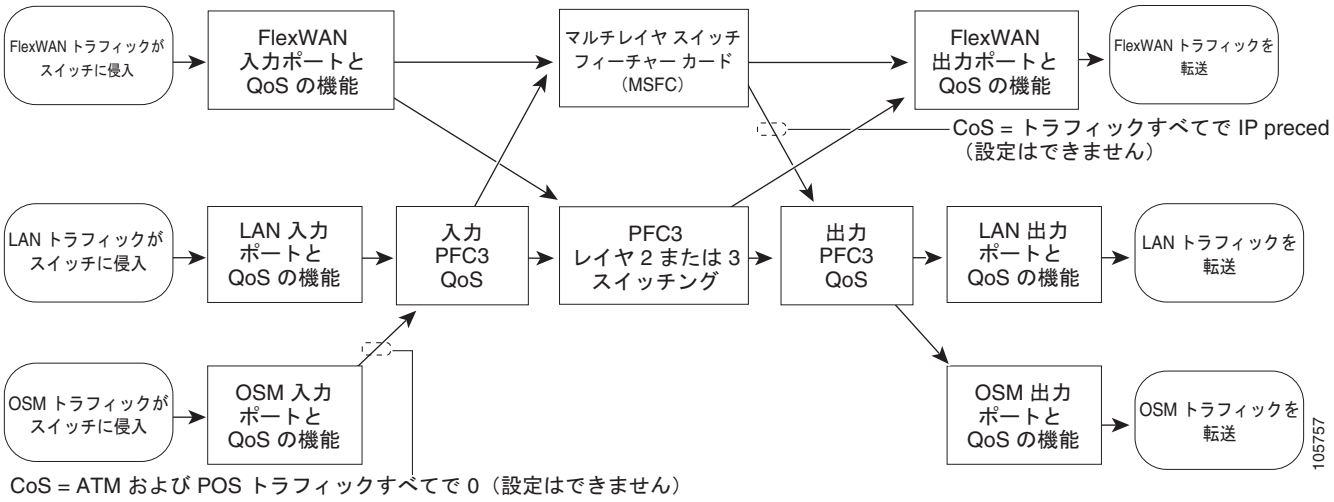


図 41-2 は、PFC3 の PFC QoS 機能間のトラフィック フローを示します。

- トラフィックは、どのタイプのポートからも入力および出力が可能です。
- DFC は、スイッチング モジュール上にローカルに PFC QoS を実装します。
- FlexWAN モジュール トラフィックの場合：
  - 入力 FlexWAN QoS 機能は、FlexWAN 入力トラフィックに適用できます。
  - 入力 FlexWAN トラフィックは、PFC3 によってレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
  - 出力 PFC QoS は、FlexWAN 入力トラフィックには適用されません。
  - 出力 FlexWAN QoS は、FlexWAN 出力トラフィックに適用できます。
- LAN ポート トラフィックの場合：
  - 入力 LAN ポート QoS 機能は、LAN ポート入力トラフィックに適用できます。
  - 入力 PFC QoS は、LAN ポート入力トラフィックに適用できます。
  - 入力 LAN ポート トラフィックは、PFC3 によってレイヤ 2 またはレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
  - 出力 PFC QoS および出力 LAN ポート QoS は、LAN ポート出力トラフィックに適用できます。

- OSM トラフィックの場合：
  - 入力 OSM ポート QoS 機能は、OSM ポート入力トラフィックに適用できます。
  - 入力 PFC3 QoS は、OSM ポート入力トラフィックに適用できます。
  - 入力 OSM ポート トラフィックは、PFC3 によってレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
  - 出力 PFC3 QoS および出力 OSM ポート QoS は、OSM ポート出力トラフィックに適用できます。

図 41-3 は、PFC2 でのトラフィック フローと PFC QoS 機能を示します。

図 41-3　PFC2 でのトラフィック フローおよび PFC QoS 機能

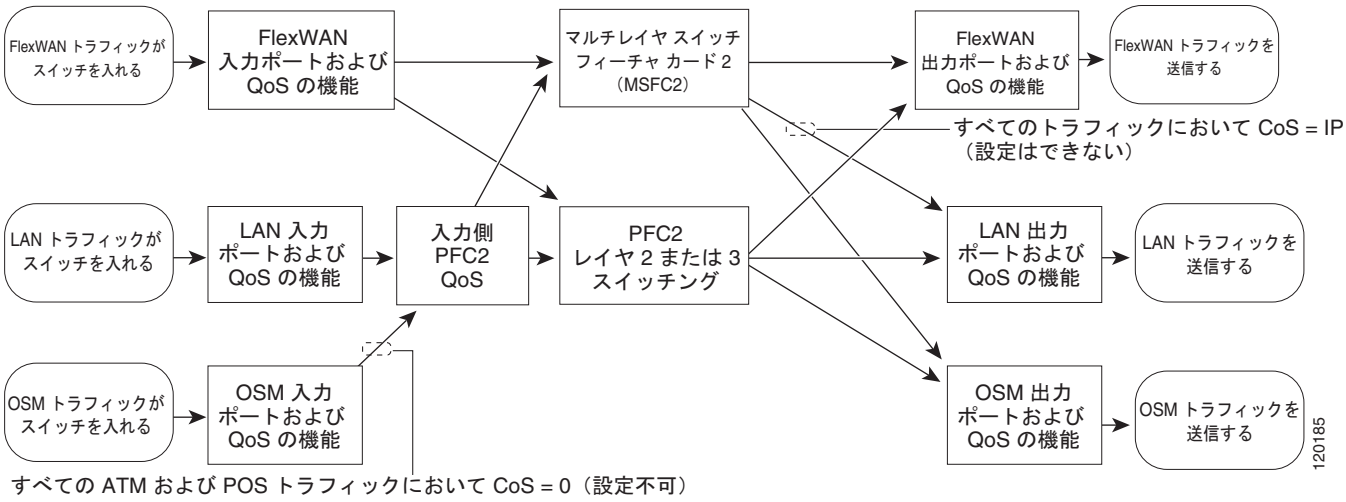
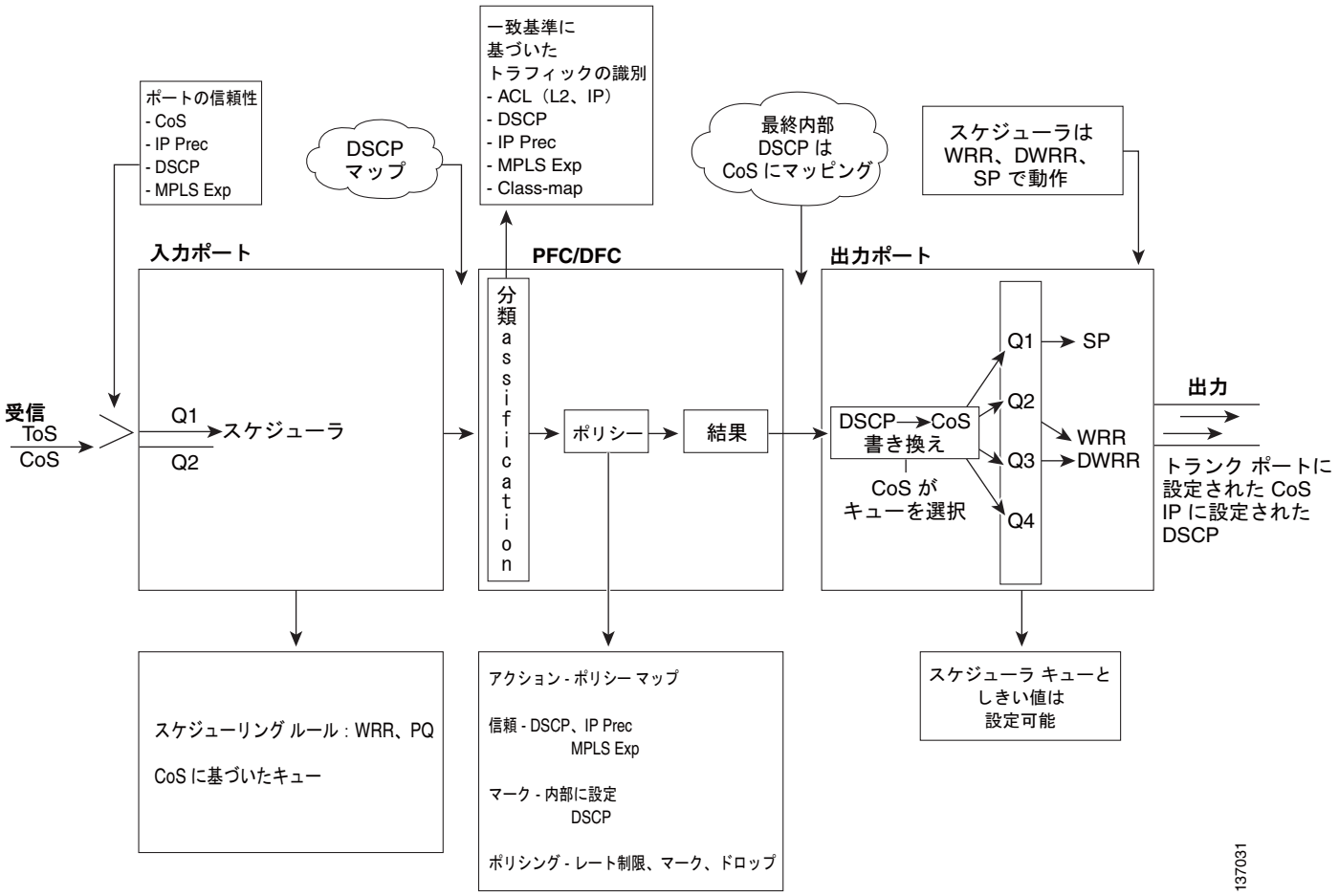


図 41-3 は、PFC2 での PFC QoS 機能間のトラフィック フローを示します。

- トラフィックは、どのタイプのポートからも入力および出力が可能です。
- DFC は、スイッチング モジュール上にローカルに PFC QoS を実装します。
- FlexWAN モジュール トラフィックの場合：
  - 入力 FlexWAN QoS 機能は、FlexWAN 入力トラフィックに適用できます。
  - 入力 FlexWAN トラフィックは、PFC2 によってレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 FlexWAN QoS は、FlexWAN 出力トラフィックに適用できます。
- LAN ポート トラフィックの場合：
  - 入力 LAN ポート QoS 機能は、LAN ポート入力トラフィックに適用できます。
  - 入力 LAN ポート トラフィックは、PFC2 によってレイヤ 2 またはレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 LAN ポート QoS は、LAN ポート出力トラフィックに適用できます。

- OSM トラフィックの場合：
  - OSM ポート QoS 機能は、OSM ポート入力トラフィックに適用できます。
  - 入力 PFC2 QoS は、OSM ポート入力トラフィックに適用できます。
  - OSM ポート入力トラフィックは、PFC2 によってレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 OSM ポート QoS は、OSM ポート出力トラフィックに適用できます。

図 41-4　PFC QoS 機能とコンポーネントの概要



コンポーネントの概要

ここでは、PFC QoS の決定とプロセスにおける、次の各コンポーネントの役割について詳しく説明します。

- 「入力 LAN ポートの PFC QoS 機能」（P.41-7）
- 「PFC および DFC の QoS 機能」（P.41-10）
- 「PFC QoS の出力ポート機能」（P.41-13）

入力 LAN ポートの PFC QoS 機能

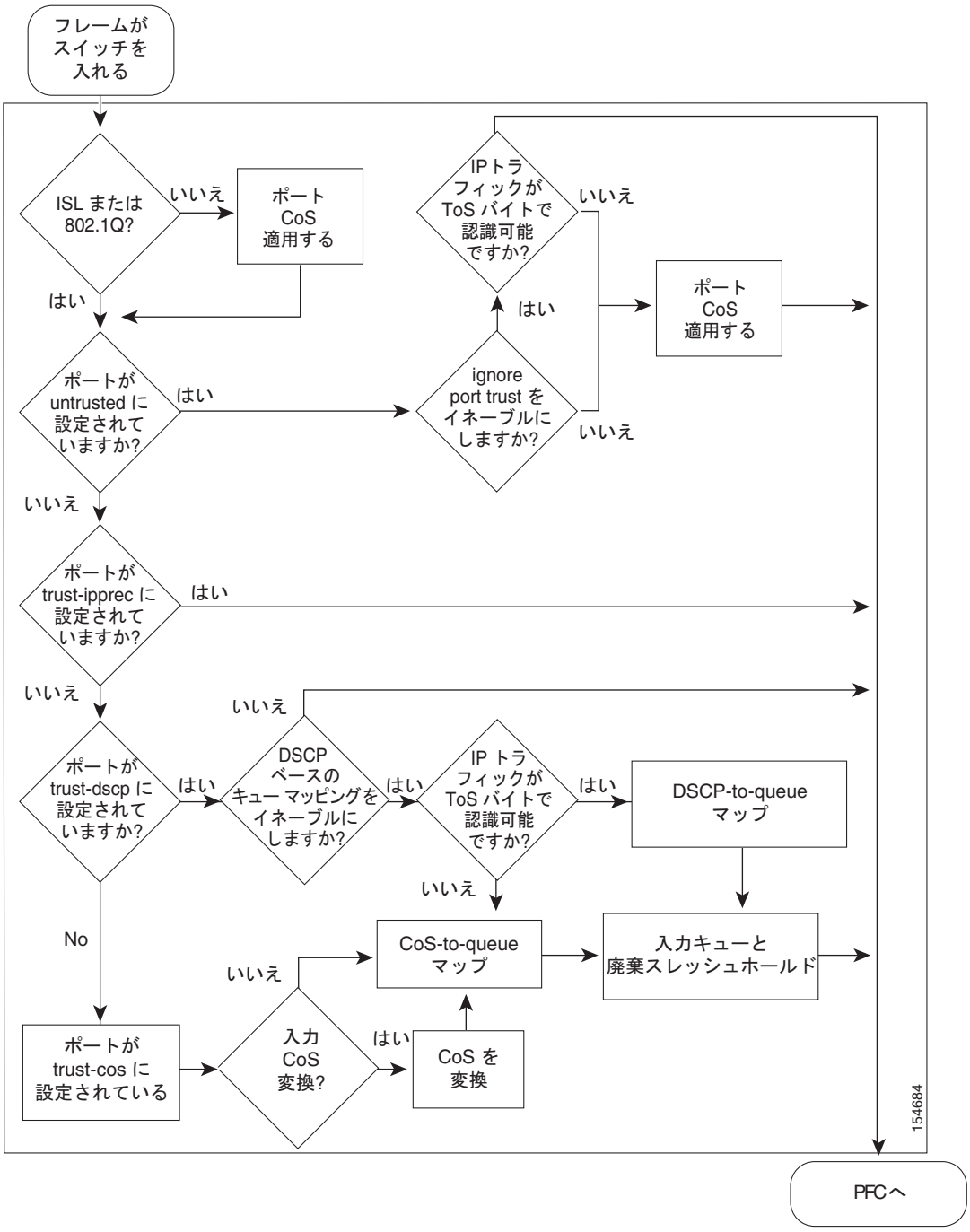
ここでは、入力ポートの QoS 機能の概要について説明します。

- 「入力 LAN ポート PFC QoS 機能のフローチャート」（P.41-7）
- 「ポートの信頼状態」（P.41-9）
- 「入力側の輻輳回避」（P.41-9）

入力 LAN ポート PFC QoS 機能のフローチャート

図 41-5 は、入力 LAN ポートの PFC QoS 機能間のトラフィック フローを示します。

図 41-5　入力 LAN ポートの PFC QoS 機能



（注）

- 入力 CoS 変換は、802.1Q トンネル ポートだけでサポートされます。
- Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能がサポートされます。
- DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートだけでサポートされます。

ポートの信頼状態

PFC QoS における*信頼*とは、有効なポートとして受け入れられ、初期内部 DSCP 値の基準として使用されることを意味します。ポートは、信頼できないポート（untrusted）として設定することも、次の QoS 値を信頼するように設定することもできます。

- レイヤ 2 CoS
  - CoS を信頼するように設定されたポートを、信頼できる CoS ポートと呼びます。
  - 信頼できる CoS ポートから受信するトラフィック、またはポリシー マップによって CoS を信頼するように設定されたトラフィックを、信頼できる CoS トラフィックと呼びます。

（注）　すべてのトラフィックに CoS 値が含まれるわけではありません。CoS 値を伝送するのは、ISL、802.1Q、および 802.1P トラフィックだけです。PFC QoS は、CoS 値を伝送しないすべてのトラフィックに対し、ポートの CoS 値を適用します。信頼できないポートでは、PFC QoS はすべてのトラフィックにポートの CoS 値を適用し、受信したすべての CoS 値を上書きします。

- IP precedence
  - IP precedence を信頼するように設定されたポートを、信頼できる IP precedence ポートと呼びます。
  - 信頼できる IP precedence ポートから受信するトラフィック、またはポリシー マップによって IP precedence を信頼するように設定されたトラフィックを、信頼できる IP precedence トラフィックと呼びます。
- DSCP
  - DSCP を信頼するように設定されたポートを、信頼できる DSCP ポートと呼びます。
  - 信頼できる DSCP ポートから受信するトラフィック、またはポリシー マップによって DSCP を信頼するように設定されたトラフィックを、信頼できる DSCP トラフィックと呼びます。

信頼できないポートから受信したトラフィックを、信頼できないトラフィックと呼びます。

入力側の輻輳回避

PFC QoS は、信頼できる CoS ポートに輻輳回避を実装します。信頼できる CoS ポートでは、QoS はレイヤ 2 の CoS 値に基づきトラフィックを分類して入力キューに割り当て、輻輳回避を行います。Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE の信頼できる DSCP ポートを設定して、受信する DSCP 値を使用して輻輳回避を行うことができます。入力側の輻輳回避の詳細については、「信頼できる CoS LAN 入力ポートでの分類とマーキング」（P.41-18）を参照してください。

PFC および DFC の QoS 機能

ここでは、PFC および DFC の QoS 関連事項について説明します。

サポートされるポリシー フィーチャ カード（PFC）

ポリシー フィーチャ カード（PFC）は、スーパーバイザ エンジンに搭載されるドータカードです。PFC は、他の機能とともに QoS 機能を提供します。Catalyst 6500 シリーズ スイッチでは、次の PFC がサポートされます。

- PFC2（Supervisor Engine 2）
- PFC3A（Supervisor Engine 720）
- PFC3B（Supervisor Engine 720 および Supervisor Engine 32）
- PFC3BXL（Supervisor Engine 720）

サポートされる Distributed Forwarding Card（DFC）

PFC は QoS ポリシーのコピーを Distributed Forwarding Card（DFC）に送信することで、QoS ポリシーがローカルにサポートされるようにします。これにより、DFC では、PFC がサポートしているものと同じ QoS 機能をサポートできるようになります。

Catalyst 6500 シリーズ スイッチでは、次の DFC がサポートされます。

- WS-F6K-DFC（Supervisor Engine 2 とともに dCEF256 および CEF256 モジュールで使用）
- WS-F6K-DFC3A、WS-F6K-DFC3B、WS-F6K-DFC3BXL（Supervisor Engine 720 とともに dCEF256 および CEF256 モジュールで使用）
- WS-F6700-DFC3A、WS-F6700-DFC3B、WS-F6700-DFC3BXL（Supervisor Engine 720 とともに CEF720 モジュールで使用）

PFC および DFC の QoS 機能リストおよびフローチャート

表 41-1 は、PFC および DFC の各バージョンでサポートされる QoS 機能の一覧を示します。

表 41-1　PFC および DFC でサポートされる QoS 機能

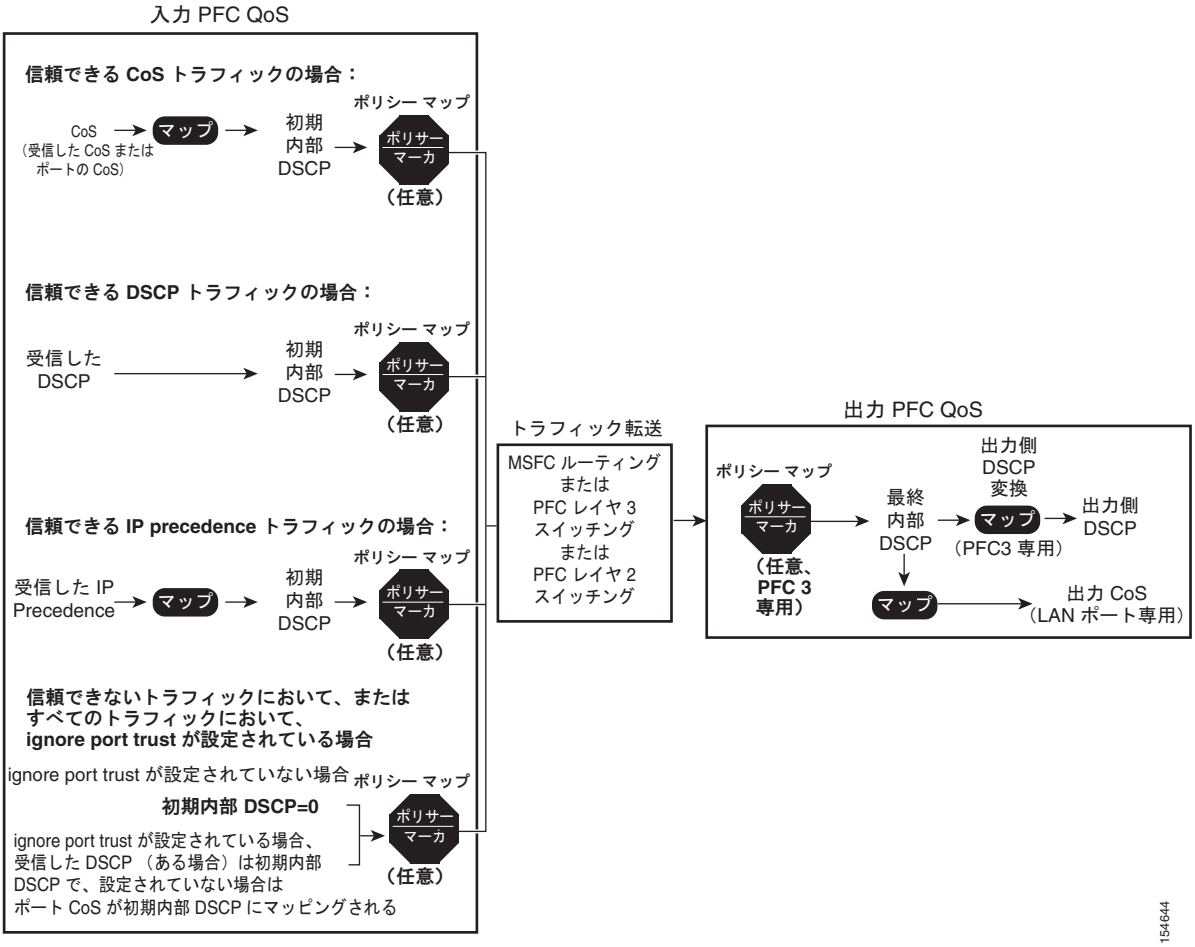
機能	PFC2/DFC	PFC3A/DFC 3A	PFC3B/DFC 3B	PFC3BXL/DFC3 BXL
DFC のサポート	あり	あり	あり	あり
フローの粒度	完全なフロー	送信元 宛先	送信元 宛先	送信元 宛先
QoS ACL	IP、IPX、MAC	IP、MAC	IP、MAC	IP、MAC
DSCP の透過性 （注）　DSCP の透過性をイネーブルにすると、出力 Type of Service（ToS; サービス タイプ）の書き換えがディセーブルになります。	なし	任意	任意	任意

表 41-1　PFC および DFC でサポートされる QoS 機能 （続き）

機能	PFC2/DFC	PFC3A/DFC 3A	PFC3B/DFC 3B	PFC3BXL/DFC3 BXL
出力 ToS の書き換え	必須	任意	任意	任意
ポリシング：				
入力集約ポリサー	あり	あり	あり	あり
出力集約ポリサー	なし	あり	あり	あり
集約ポリサーの数	1022	1022	1022	1022
マイクロフロー ポリサー	64 レート	64 レート	64 レート	64 レート
マイクロフロー ポリサーあたりのフロー数	32,000	64,000	110,000	240,000
ポリサーによる統計の計測単位	パケット	バイト	バイト	バイト
ポリサー処理の基準	レイヤ 3 の長さ	レイヤ 2 の長さ	レイヤ 2 の長さ	レイヤ 2 の長さ

図 41-6 は、PFC および DFC 上の QoS 機能間のトラフィック フローを示します。

図 41-6　PFC および DFC の QoS 機能



（注）　DSCP 透過性機能を使用すると、オプションで出力 DSCP 値をレイヤ 3 ToS バイトに書き込むことができます。

内部 DSCP 値

PFC QoS は処理中、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティを、内部 DSCP 値で表します。

初期内部 DSCP 値

PFC では何らかのマーキングまたはポリシングが行われる前に、PFC QoS によって、次のように初期内部 DSCP 値が導出されます。

- 信頼できないトラフィックにおいて、ignore port trust がイネーブルになっていない場合は、タグ付きおよびタグなしの両方のトラフィックに対し、初期内部 DSCP 値が 0 に設定されます。
- 信頼できないトラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
  - 認識可能な ToS バイトが含まれないトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる CoS トラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。

    （注）　信頼できる CoS トラフィックにおいて、ignore port trust がイネーブルにされている場合は、受信したタグ付き IP トラフィック内の CoS 値は使用されません。

  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる IP precedence トラフィックの場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した IP precedence 値を初期内部 DSCP 値にマッピングします。
  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる DSCP トラフィックの場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。

信頼できる CoS トラフィックおよび信頼できる IP precedence トラフィックの場合は、PFC QoS は設定可能なマップを使用して、3 ビット値である CoS または IP precedence から、6 ビットの初期内部 DSCP 値を導出します。

最終内部 DSCP 値

PFC でのポリシー マーキングおよびポリシングでは、初期内部 DSCP 値が最終内部 DSCP 値に変更されることがあります。この値は、これ以降に適用されるすべての QoS 機能で使用されます。

ポートベースの PFC QoS、および VLAN ベースの PFC QoS

各入力 LAN ポートは、物理ポート ベースの PFC QoS（デフォルト）または VLAN ベースの PFC QoS のいずれかに対応するように設定し、選択したインターフェイスにポリシー マップを付加できます。

ポート ベースの PFC QoS を設定するポートの場合、次のように入力 LAN ポートにポリシー マップを付加します。

- 非トランク入力 LAN ポートをポート ベースの PFC QoS 用に設定すると、そのポートを通じて受信するすべてのトラフィックに、ポートに付加されたポリシー マップが適用されます。
- トランク入力 LAN ポートをポート ベースの PFC QoS 用に設定すると、そのポートを通じて受信するすべての VLAN トラフィックに、ポートに付加されたポリシー マップが適用されます。

非トランク入力 LAN ポートを VLAN ベースの PFC QoS 用に設定すると、そのポートを通じて受信するトラフィックに、ポートの VLAN に付加されたポリシー マップが適用されます。

トランク入力 LAN ポートを VLAN ベースの PFC QoS 用に設定すると、そのポートを通じて受信するトラフィックに、トラフィックの VLAN に付加されたポリシー マップが適用されます。

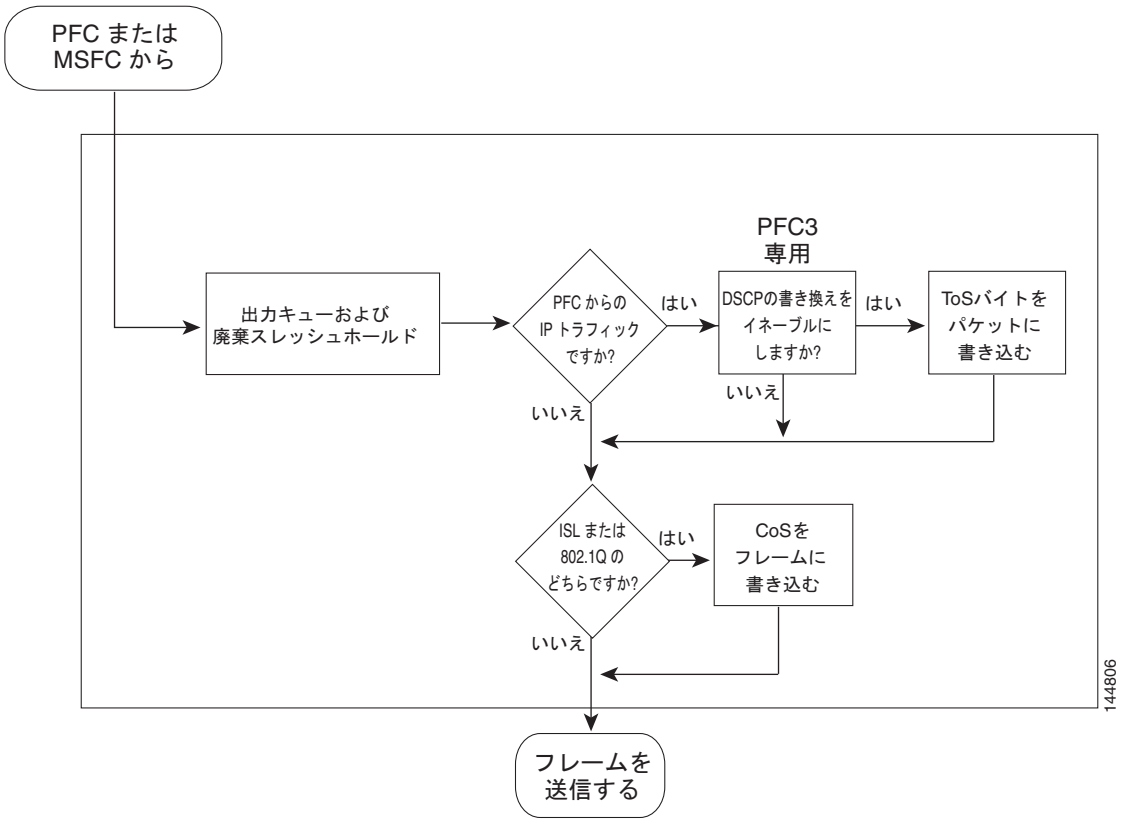
PFC QoS の出力ポート機能

ここでは、PFC QoS の出力ポート機能について説明します。

PFC QoS の出力 LAN ポート機能のフローチャート

図 41-7 は、出力 LAN ポートでの QoS 機能間のトラフィック フローを示します。

図 41-7　出力 LAN ポートでのスケジューリング、輻輳回避、およびマーキング



出力 CoS 値

すべての出力トラフィックについて、PFC QoS は設定変更可能なマップを使用して、トラフィックと関連付けられた最終内部 DSCP 値から CoS 値を導出します。導出された CoS 値は出力 LAN ポートに送られます。この値は分類および輻輳回避に使用されるほか、ISL フレームおよび 802.1Q フレームに書き込まれます。

（注）　Release 12.2(18)SXF5 以降のリリースでは、出力 LAN ポートでの分類と輻輳回避に最終内部 DSCP 値が使用されるように、WS-X6708-10GE ポートを設定することができます（「DSCP ベースのキューマッピングの設定」（P.41-108）を参照）。

PFC3 による出力 DSCP の変換

PFC3 の場合、内部 DSCP 値が出力 ToS バイトに書き込まれる前に内部 DSCP 値を変換するには、最大 15 個の出力 DSCP 変換マップを設定できます。出力 DSCP 変換マップは、PFC QoS がサポートする任意のインターフェイスに付加できます。

（注）
- 出力 DSCP 変換を設定する場合は、PFC QoS による、変換された DSCP 値に基づく出力 CoS 値の導出は行われません。
- PFC2 は出力 DSCP 変換をサポートしません。

出力 ToS バイト

DSCP 透過性をイネーブルにしている場合を除き、PFC QoS は最終内部 DSCP 値または変換された DSCP 値を基に、出力 IP トラフィックの ToS バイトを作成します。この ToS バイトは出力ポートに送られ、IP パケット内に書き込まれます。信頼できる DSCP トラフィック、および信頼できない IP トラフィックの場合、ToS バイトには、受信した ToS バイトの元の最下位 2 ビットが含まれます。

内部 DSCP 値または変換された DSCP 値には、IP precedence 値と同じ機能があります（「IP precedence 値と DSCP 値」（P.41-60）を参照）。

出力 PFC QoS インターフェイス

出力ポリシー マップをレイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）に付加することで、ポリシー マップを出力トラフィックに適用できます。

（注）
- 出力ポリシーはマイクロフロー ポリシングをサポートしません。
- PFC3 では、マイクロフロー ポリシングを ARP トラフィックに適用できません。
- 出力ポリシーでは信頼状態を設定できません。

再マーキングされた DSCP に対する出力 ACL のサポート

（注）　再マーキングされた DSCP に対する出力 ACL のサポートは、パケット再循環とも呼ばれます。

PFC3 を使用すると、Release 12.2(18)SXE 以降のリリースで、再マーキングされた DSCP を出力 ACL によってサポートできます。これにより、入力 PFC QoS によって行われた IP precedence または DSCP のポリシングまたはマーキングの変更を使用して、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングが実行されるように設定できます。

再マーキングされた DSCP に対する出力 ACL のサポートがないと、出力 QoS フィルタリングには、受信した IP precedence または DSCP の値が使用されます。ポリシングまたはマーキングの結果として入力 PFC QoS によって行われた、IP precedence または DSCP の変更は使用されません。

PFC3 は、出力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）において、レイヤ 3 でスイッチングおよびルーティングされたトラフィックだけに対して出力 PFC QoS を提供します。

再マーキングされた DSCP に対する出力 ACL サポートは、入力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）上で設定します。

再マーキングされた DSCP に対する出力 ACL サポートを設定したインターフェイス上では、PFC3 は QoS フィルタリングされた各 IP パケットを 2 回ずつ処理します。1 回目は入力 PFC QoS を適用し、2 回目は出力 PFC QoS を適用します。

注意　再マーキングされた DSCP に対する出力 ACL サポートを設定したスイッチが PFC3A モードで動作している場合は、PFC3 はトラフィックを処理して入力 PFC QoS を適用する際、入力 PFC QoS フィルタリングおよび入力 PFC QoS を適用し、入力インターフェイスに設定されたすべての出力 QoS フィルタリングおよび出力 PFC QoS を不正に適用します。この結果、再マーキングされた DSCP に対する出力 ACL サポートがイネーブルになっているインターフェイス上で QoS フィルタリングが設定された場合に、予期しない動作が発生します。この問題は、他の PFC3 モードでは発生しません。

入力 PFC QoS によってパケットが処理され、すべてのポリシングまたはマーキング変更が行われると、このパケットは出力 PFCQoS によって処理される前に、すべての設定済みレイヤ 2 機能（VACL など）によって入力インターフェイス上で再び処理されます。

再マーキングされた DSCP に対する出力 ACL サポートが設定されたインターフェイスで、入力 QoS によって変更された IP precedence または DSCP 値がレイヤ 2 機能と一致すると、一致するパケットはレイヤ 2 機能によってリダイレクトまたは廃棄されます。これにより、このパケットが出力 QoS によって処理されることを防ぎます。

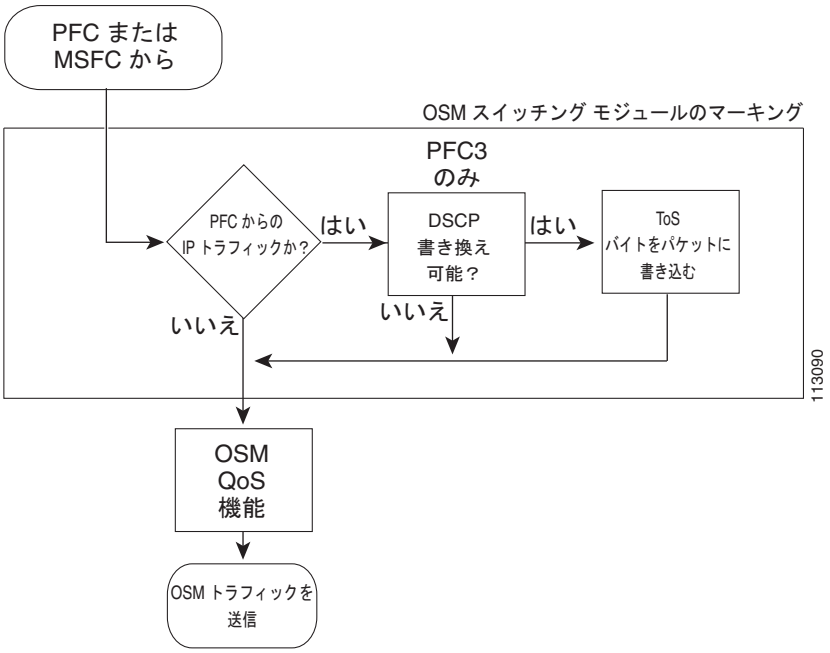
入力 PFC QoS によってパケットが処理され、すべてのポリシングまたはマーキング変更が行われると、このパケットは出力 PFC QoS によって処理される前に、すべての設定済みレイヤ 3 機能（たとえば入力 Cisco IOS ACL、Policy-Based Routing（PBR; ポリシー ベース ルーティング）など）によって入力インターフェイス上で再び処理されます。

再マーキングされた DSCP に対する出力 ACL サポートが設定されたインターフェイスにレイヤ 3 機能を設定している場合は、入力 PFC QoS によって処理されたパケットはこのレイヤ 3 機能によってリダイレクトまたは廃棄されることがあります。これにより、このパケットが出力 PFC QoS によって処理されることを防ぎます。

出力 OSM ポートでのマーキング

入力 PFC QoS により、OSM 出力 QoS 機能で使用される DSCP 値が設定されます（図 41-8 を参照）。

図 41-8　出力 OSM ポートでのマーキング



分類とマーキングの概要

ここでは、Catalyst 6500 シリーズ スイッチにおいて分類とマーキングが行われる場所、およびその方法について説明します。

- 「信頼できる入力ポートおよび信頼できない入力ポートでの分類とマーキング」（P.41-17）
- 「入力 OSM ポートでの分類とマーキング」（P.41-19）
- 「サービス ポリシーおよびポリシー マップによる PFC での分類およびマーキング」（P.41-19）
- 「MSFC での分類およびマーキング」（P.41-20）

信頼できる入力ポートおよび信頼できない入力ポートでの分類とマーキング

入力ポートの信頼状態によって、そのポートが受信したレイヤ 2 フレームをどのようにマーキング、スケジューリング、および分類するか、また、輻輳回避を実行するかどうかが決まります。ポートの信頼状態には、次の種類があります。

- untrusted（デフォルト）
- trust IP precedence
- trust DSCP
- trust CoS

すべてのリリースにおいて、入力 LAN ポートでの分類、マーキング、および輻輳回避ではレイヤ 2 CoS 値が使用可能であり、レイヤ 3 の IP precedence 値または DSCP 値は設定されません。

Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートを設定して、入力 LAN ポートでの分類と輻輳回避に、受信した DSCP 値を使用することができます（「DSCP ベースのキュー マッピングの設定」（P.41-108）を参照）。

Release 12.2(18)SXF5 よりも前のリリースでは、入力 LAN ポートの分類、マーキング、および輻輳回避には、レイヤ 2 CoS 値だけが使用されます。

ここでは、信頼できる入力ポートおよび信頼できない入力ポートでの、分類およびマーキングについて説明します。

- 「信頼できない入力ポートでの分類とマーキング」（P.41-17）
- 「信頼できる入力ポートでの分類とマーキング」（P.41-17）

信頼できない入力ポートでの分類とマーキング

PFC QoS のレイヤ 2 再マーキングでは、信頼できないポートから受信したすべてのフレームに、ポートの CoS 値がマークされます（デフォルト値は 0）。

信頼できない入力トラフィックに適用されたポート CoS 値を初期内部 DSCP 値にマッピングするには、入力トラフィックと一致する、信頼できる CoS ポリシー マップを設定します。

信頼できる入力ポートでの分類とマーキング

ポートを信頼可能として設定する場合は、そのポートが、有効な QoS ラベルを伝送するトラフィックを受信する場合だけにしてください。QoS は受信した QoS ラベルを、初期内部 DSCP 値の基準値として使用します。スイッチに入力後のトラフィックには、ポリシー マップによって、別の信頼状態を適用できます。たとえば、信頼できる CoS ポートからスイッチに入力されたトラフィックに対し、ポリシー マップを使用して、IP precedence または DSCP を信頼するように設定できます。これにより、ポートで信頼された QoS ラベルではなく、この信頼値が初期内部 DSCP 値の基準値として使用されます。

ここでは、信頼できる入力ポートでの分類およびマーキングについて説明します。

- 「信頼できる CoS LAN 入力ポートでの分類とマーキング」（P.41-18）
- 「信頼できる IP Precedence 入力ポートでの分類とマーキング」（P.41-18）
- 「信頼できる入力 DSCP ポートでの分類とマーキング」（P.41-18）

信頼できる CoS LAN 入力ポートでの分類とマーキング

CoS を信頼するように LAN ポートを設定する場合は、そのポートが、有効なレイヤ 2 CoS を伝送するトラフィックを受信する場合だけにしてください。

信頼できる入力 LAN ポートから ISL フレームがスイッチに入ると、PFC QoS は [User] フィールドの最下位 3 ビットを CoS 値として受け取ります。信頼できる入力 LAN ポートから 802.1Q フレームがスイッチに入ると、PFC QoS はユーザ プライオリティ ビットを CoS 値として受け取ります。PFC QoS のレイヤ 2 再マーキングでは、タグなしフレームで受信したすべてのトラフィックが、入力ポートの CoS 値でマーキングされます。

CoS を信頼するように設定したポートでは、PFC QoS によって次の処理が行われます。

- タグ付きの信頼できる CoS トラフィックによって受信した CoS 値は、初期内部 DSCP 値にマッピングされます。
- タグなしの信頼できるトラフィックに適用された入力ポート CoS 値は、初期内部 DSCP 値にマッピングされます。
- PFC QoS では、CoS ベースの入力キューおよびスレッシュホールドをイネーブルにすることで、輻輳回避を行うことができます。入力キューおよびスレッシュホールドの詳細については、「ポートベースのキュー タイプの概要」（P.41-24）を参照してください。

信頼できる IP Precedence 入力ポートでの分類とマーキング

IP precedence を信頼するようにポートを設定する場合は、そのポートが、有効なレイヤ 3 IP precedence を伝送するトラフィックを受信する場合だけにしてください。信頼できる IP precedence ポートからのトラフィックに対し、PFC QoS は受信した IP precedence 値を初期内部 DSCP 値にマッピングします。入力ポートのキューおよびスレッシュホールドでは、レイヤ 2 CoS が使用されます。したがって PFC QoS は、IP precedence を信頼するように設定されているポートでは、入力ポートの輻輳回避を行いません。PFC は、IP precedence を信頼するように設定されている入力ポートでは、トラフィックのマーキングを行いません。

信頼できる入力 DSCP ポートでの分類とマーキング

DSCP を信頼するようにポートを設定する場合は、そのポートが、有効なレイヤ 3 DSCP を伝送するトラフィックを受信する場合だけにしてください。

Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで DSCP ベースの入力キューおよびスレッシュホールドをイネーブルにすることで、輻輳回避を実行できます（「DSCP ベースのキュー マッピングの設定」（P.41-108）を参照）。

Release 12.2(18)SXF5 よりも前のリリースでは、入力ポートキューおよびスレッシュホールドでは、レイヤ 2 CoS しか使用されません。したがって、DSCP を信頼するように設定されたポートでは、PFC QoS によるポートの輻輳回避は行われません。

信頼できる DSCP ポートからのトラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。受信する DSCP を信頼するように設定された入力ポートでは、PFC QoS によるトラフィックのマーキングは行われません。

入力 OSM ポートでの分類とマーキング

PFC QoS は、入力 OSM ポートから受信したすべてのトラフィックに、0 の CoS を関連付けます。入力 OSM ポートの信頼状態を設定し、この信頼状態を、PFC が IP precedence 値または DSCP 値、および CoS 値を設定するときに使用させることができます。各入力 OSM ポートの信頼状態を、次のように設定できます。

- untrusted（デフォルト）
- trust IP precedence
- trust DSCP
- trust CoS（POS および ATM OSM ポートではポートの CoS 値を設定できないため、POS および ATM OSM ポートの CoS 値は常に 0）

サービス ポリシーおよびポリシー マップによる PFC での分類およびマーキング

PFC QoS は、サービス ポリシーによる分類およびマーキングをサポートします。これは、次のインターフェイス タイプに 1 つのポリシー マップを付加することで、入力 PFC QoS を適用します。

- 各入力ポート（FlexWAN インターフェイスを除く）
- 各 EtherChannel ポートチャネル インターフェイス
- 各 VLAN インターフェイス

PFC3 では、各レイヤ 3 インターフェイス（FlexWAN インターフェイスを除く）に 1 つのポリシー マップを付加することで、出力 PFC QoS を適用できます。

各ポリシー マップには、複数のポリシー マップ クラスを含めることができます。インターフェイスにより処理されたトラフィックのタイプごとに、個別のポリシー マップ クラスを設定できます。ポリシー マップ クラスのフィルタリングを設定するには、次の 2 つの方法があります。

- アクセス制御リスト（ACL）
- IP precedence および DSCP 値に対するクラス マップの **match** コマンド

ポリシー マップ クラスでは、次のオプション コマンドを使用してアクションを指定します。

- ポリシー マップ **set** コマンド - 信頼できないトラフィックの場合、または ignore port trust をイネーブルにしている場合は、PFC QoS は最終内部 DSCP 値として、設定済みの IP precedence 値または DSCP 値を使用できます。IP precedence および DSCP のビット値については、「IP precedence 値と DSCP 値」（P.41-60）を参照してください。
- ポリシー マップ クラス **trust** コマンド - PFC QoS は一致する入力トラフィックに対し、ポリシー マップ クラスの信頼状態を適用します。この信頼値は、ポートで信頼された QoS ラベル（存在する場合）の代わりに、初期内部 DSCP 値の基準値として使用されます。ポリシー マップでは、CoS、IP precedence、または DSCP を信頼するように設定できます。

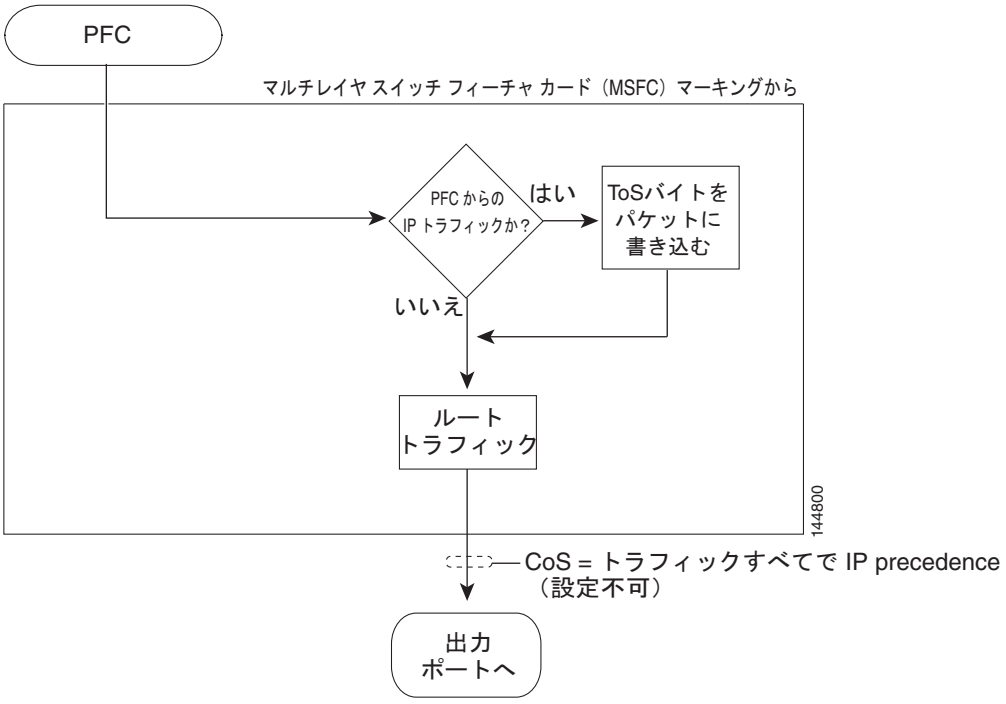
  （注） 信頼できる CoS ポリシー マップでは、信頼できないポートからのトラフィックで受信した CoS を元に戻すことはできません。信頼できないポートからのトラフィックには、常にポートの CoS 値が含まれます。

- 集約ポリサーおよびマイクロフロー ポリサー - PFC QoS ではポリサーを使用して、適合するトラフィックと適合しないトラフィックの両方について、マーキングまたは廃棄のいずれかを実行できます。

MSFC での分類およびマーキング

PFC QoS は MSFC に対し、IP トラフィックを最終内部 DSCP 値とともに送信します。MSFC から出力ポートへ送信されるすべてのトラフィックにおいて、CoS は IP precedence と同じ値です。

図 41-9　　PFC2/PFC3 および MSFC2/MSFC2A/MSFC3 によるマーキング



（注） PFC でレイヤ 3 スイッチングされるトラフィックは MSFC を通過せず、PFC によって割り当てられる CoS 値を維持します。

ポリサー

ここでは、各ポリサーについて説明します。

- 「ポリサーの概要」（P.41-20）
- 「集約ポリサー」（P.41-21）
- 「マイクロフロー ポリサー」（P.41-22）

ポリサーの概要

ポリシングを使用すると、QoS 設定で定義されたトラフィック転送ルールに適合するように、着信および送信トラフィックをレート制限できます。システムにおいてトラフィックが転送される方法を定義した設定済みルールは、契約と呼ばれます。この契約に適合しないトラフィックは、低い DSCP 値にマーク ダウンされるか、または廃棄されます。

ポリシングでは、不適合パケットはバッファに保存されません。したがって、ポリシングが送信遅延に影響することはありません。逆に、トラフィック シェーピングでは不適合トラフィックをバッファに保存することで、トラフィック バーストを緩和します （PFC QoS はシェーピングをサポートしません）。

PFC2 は入力 PFC QoS だけをサポートしますが、これには入力ポリシングが含まれます。PFC3 は入力および出力 PFC QoS の両方をサポートし、これには入力および出力ポリシングが含まれます。トラフィック シェーピングは、一部の WAN モジュールでサポートされます。OSM および FlexWAN モジュールでのトラフィック シェーピングの詳細については、次の URL にある OSM および FlexWAN 関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/index.htm

（注）　ポリサーは、ポート単位または VLAN 単位で入力トラフィックに適用されます。PFC3 の出力トラフィックに対するポリシングは、VLAN 単位だけで行われます。

次の処理を行うポリサーを作成できます。

- トラフィックのマーキング
- 帯域幅利用の制限およびトラフィックのマーキング

集約ポリサー

PFC QoS は、1 つの集約ポリサーで指定される帯域幅限度を、一致するトラフィックのすべてのフローに対して累積方式で適用します。たとえば、VLAN 1 および VLAN 3 上のすべての Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）トラフィック フローの帯域幅として、1 Mbps を許可するように集約ポリサーを設定すると、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローは、合計 1 Mbps となるように制限されます。

- ポリシー マップ クラスのインターフェイス別集約ポリサーは、**police** コマンドを使用して定義します。インターフェイス別集約ポリサーを複数の入力ポートに付加すると、各入力ポート上の一致するトラフィックが個別にポリシングされます。
- 名前付き集約ポリサーは、**mls qos aggregate-policer** コマンドを使用して作成します。名前付き集約ポリサーを複数の入力ポートに付加すると、そのポリサーが付加された全入力ポートからの一致するトラフィックがポリシングされます。
- 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチ仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

マイクロフロー ポリサー

PFC QoS は、マイクロフロー ポリサーで指定される帯域幅限度を、一致するトラフィックの各フローに対して個別に適用します。たとえば、VLAN 1 および VLAN 3 で TFTP トラフィックを 1 Mbps に制限するようにマイクロフロー ポリサーを設定すると、VLAN 1 の各フローに 1 Mbps が、VLAN 3 の各フローに 1 Mbps がそれぞれ許可されます。VLAN 1 に 3 つのフローが含まれ、VLAN 3 に 4 つのフローが含まれる場合は、マイクロフロー ポリサーはこの各フローにそれぞれ 1 Mbps を許可します。

マイクロフロー ポリサーの帯域幅限度を適用するように、PFC QoS を次のように設定できます。

- マイクロフロー ポリサーは、最大 63 通りのレート/バースト パラメータの組み合わせを使用して作成できます。
- ポリシー マップ クラスのマイクロフロー ポリサーは、**police flow** コマンドを使用して作成します。
- 送信元アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより宛先アドレスに関係なく、特定の送信元アドレスからのすべてのトラフィックにマイクロフロー ポリサーを適用します。
- 宛先アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより送信元アドレスに関係なく、特定の宛先アドレスへのすべてのトラフィックにマイクロフロー ポリサーを適用します。
- MAC レイヤ マイクロフロー ポリシングの場合、PFC QoS はプロトコルおよび送信元と宛先の MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、Ethertype が違っていても、同じフローの一部であると見なします。PFC3 では、IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
- PFC2 では、IPX トラフィックをフィルタリングするように IPX ACL を設定できます。IPX マイクロフロー ポリシングの場合、PFC QoS は、送信元ノードまたは送信元ソケットが異なるトラフィックを含め、同じ送信元ネットワーク、宛先ネットワーク、および宛先ノードを持つ IPX トラフィックは同じフローの一部であると見なします。
- デフォルトでは、マイクロフロー ポリサーは MSFC がルーティングするトラフィックだけに影響します。それ以外のトラフィック（ブリッジ グループのトラフィックも含む）のマイクロフロー ポリシングをイネーブルにするには、**mls qos bridged** コマンドを使用します。PFC2 では、ルーティングされたトラフィックに対してブリッジ マイクロフロー ポリシングもイネーブルにする必要があります。
- PFC3 では、マイクロフロー ポリシングを ARP トラフィックに適用できません。
- マイクロフロー ポリシングを IPv6 マルチキャスト トラフィックに適用できません。

各ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方を含めると、単独の帯域利用率と、他のフローと合算された帯域利用率に基づいて、フローのポリシングを行うことができます。

（注） トラフィックに集約ポリシングとマイクロフロー ポリシングを実行する場合、集約ポリサーおよびマイクロフロー ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。

たとえば、グループの個々のメンバに適した帯域幅限度を設定してマイクロフロー ポリサーを作成し、さらに、グループ全体として適切な帯域幅限度を設定して名前付き集約ポリサーを作成できます。グループのトラフィックと一致するポリシー マップ クラスに、この両方のポリサーを含めます。この組み合わせは、個々のフローには別々に作用し、グループには集約的に作用します。

ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方が含まれている場合、PFC QoS はどちらかのポリサーに基づいて不適合なステータスに対応し、そのポリサーの指定に従って、新しい DSCP 値を適用するか、またはパケットを廃棄します。両方のポリサーから不適合なステータスが戻された場合には、どちらかのポリサーでパケットの廃棄が指定されていれば、パケットは廃棄されます。指定されていない場合は、マークダウンされた DSCP 値が適用されます。

（注）　矛盾した結果が生じないように、同一の集約ポリサーでポリシングするすべてのトラフィックで、信頼状態が同じであることを確認してください。

PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。帯域幅利用限度は、Committed Information Rate（CIR; 認定情報速度）で指定します。より高い Peak Information Rate（PIR; 最大情報レート）も指定できます。レートを超過するパケットは、「不適合」と見なされます。

ポリサーごとに、不適合なパケットを廃棄するか、または新しい DSCP 値を適用するかを指定します（新しい DSCP 値を適用することを「マークダウン」といいます）。不適合なパケットは、元のプライオリティを維持しないので、適合するパケットが消費した帯域幅の一部としてはカウントされません。

PIR を設定する場合、PIR に不適合な場合のアクションは、CIR に不適合な場合のアクションよりも厳しいものになります。たとえば、CIR に不適合な場合のアクションがトラフィックをマークダウンするというアクションである場合、PIR に不適合な場合のアクションは、トラフィックを送信するというアクションにはできません。

PFC QoS はあらゆるポリサーで、設定変更可能なグローバル テーブルを使用して、内部 DSCP 値をマークダウンされた DSCP 値にマッピングします。マークダウンが発生すると、PFC QoS はこのテーブルからマークダウンされた DSCP 値を取得します。ユーザが個々のポリサーでマークダウン後の DSCP 値を指定することはできません。

（注）

- **conform-action transmit** キーワードによるポリシングは、一致するトラフィックの入力 LAN ポート信頼状態（trust DSCP、または **trust** ポリシー マップ クラス コマンドで定義された信頼状態）よりも優先されます。
- デフォルトでは、マークダウン テーブルは、マークダウンが起こらないように設定されています。つまり、マークダウンされた DSCP 値は、元の DSCP 値と同じです。マークダウンをイネーブルにするには、ネットワークに合わせてテーブルを適切に設定します。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

ポートベースのキュー タイプの概要

ポートベースのキュー タイプは、ポートを制御する ASIC によって決定されます。ここでは、Catalyst 6500 シリーズ スイッチの LAN モジュールによってサポートされるキュー タイプ、廃棄スレッシュホールド、およびバッファについて説明します。

入力および出力バッファとレイヤ 2 CoS ベース キュー

イーサネット LAN モジュール ポートの ASIC は、固定数のキューに分割されるバッファを備えています。輻輳回避をイネーブルにすると、PFC QoS はトラフィックのレイヤ 2 CoS 値を使用して、トラフィックを各キューに割り当てます。バッファとキューは、スイッチを通過するフレームを一時的に保管します。PFC QoS はポートの ASIC メモリを、各ポートの各キューに対するバッファとして割り当てます。

Catalyst 6500 シリーズ スイッチの LAN モジュールは、次のキュー タイプをサポートします。

- 標準キュー
- 完全優先キュー

Catalyst 6500 シリーズ スイッチの LAN モジュールは、キュー間で次のスケジューリング アルゴリズムをサポートします。

- Shaped Round Robin（SRR; シェイプド ラウンド ロビン）- SRR を使用すると、1 つのキューは、割り当てられた帯域幅だけの使用が許可されます。
- Deficit Weighted Round Robin（DWRR）- より高いプライオリティのキュー内のトラフィックによってプライオリティを低く設定されている、転送中のすべてのキューを追跡し、次回のラウンドでこの差分を補います。
- Weighted Round-Robin（WRR; 重み付きラウンドロビン）- WRR は、各キューに対して帯域幅を明示的に予約しません。各キューに割り当てられる帯域幅の量は、ユーザが設定できます。キューに割り当てられる割合（重み）は、このキューに割り当てられる帯域幅の量を定義します。
- 完全優先キューイング - 遅延に影響されやすいデータ（音声など）を、他のキュー内のパケットがキューから取り出される前にキューから取り出します。これにより、遅延に影響されやすいデータが、他のトラフィックより優先的に処理されます。スイッチは、完全優先キュー内のトラフィックを処理してから、標準キューを処理します。スイッチは標準キュー内のパケットを送信したあとで、完全優先キュー内のトラフィックを調べます。スイッチは完全優先キュー内でトラフィックを検出すると、標準キューの処理を中断し、先に完全優先キュー内のすべてのトラフィックを処理してから、標準キューに戻ります。

Catalyst 6500 シリーズ スイッチの LAN モジュールは、輻輳回避を実行する際、キュー内で次のタイプのスレッシュホールドを使用します。

- Weighted Random Early Detection（WRED; 重み付きランダム早期検出）- WRED 廃棄スレッシュホールドを設定したポートでは、バッファの輻輳を回避する目的のランダムな確率に基づき、特定の QoS ラベルを持つフレームがキューへの入力を許可されます。特定の QoS ラベルを持つフレームがキューへの入力を許可、または廃棄される確率は、この QoS ラベルに割り当てられた重みとスレッシュホールドに依存します。

  たとえば、スレッシュホールドが 2 のキュー 1 に CoS 2 が割り当てられ、スレッシュホールド 2 のレベルが 40%（ロー）および 80%（ハイ）であるとします。この場合、CoS 2 を持つフレームは、キュー 1 が 40% 以上占有されるまでは廃棄されません。キューの深さが 80% に近づくにつれ、CoS 2 を持つフレームは、キューへの入力が許可される確率よりも、廃棄される確率のほうが高くなります。キューの占有率が 80% を超えると、キューの占有率が 80% 未満となるまで、CoS 2 フレームはすべて廃棄されます。キュー レベルがロー スレッシュホールドとハイ スレッシュホールドの中間にある場合に、スイッチによって廃棄されるフレームは、フロー単位や FIFO 形式ではなく、ランダムに選択されます。この方法は、バックオフや転送ウィンドウ サイズの調整によって、定期的なパケット廃棄に適応することが可能な、TCP などのプロトコルに適します。

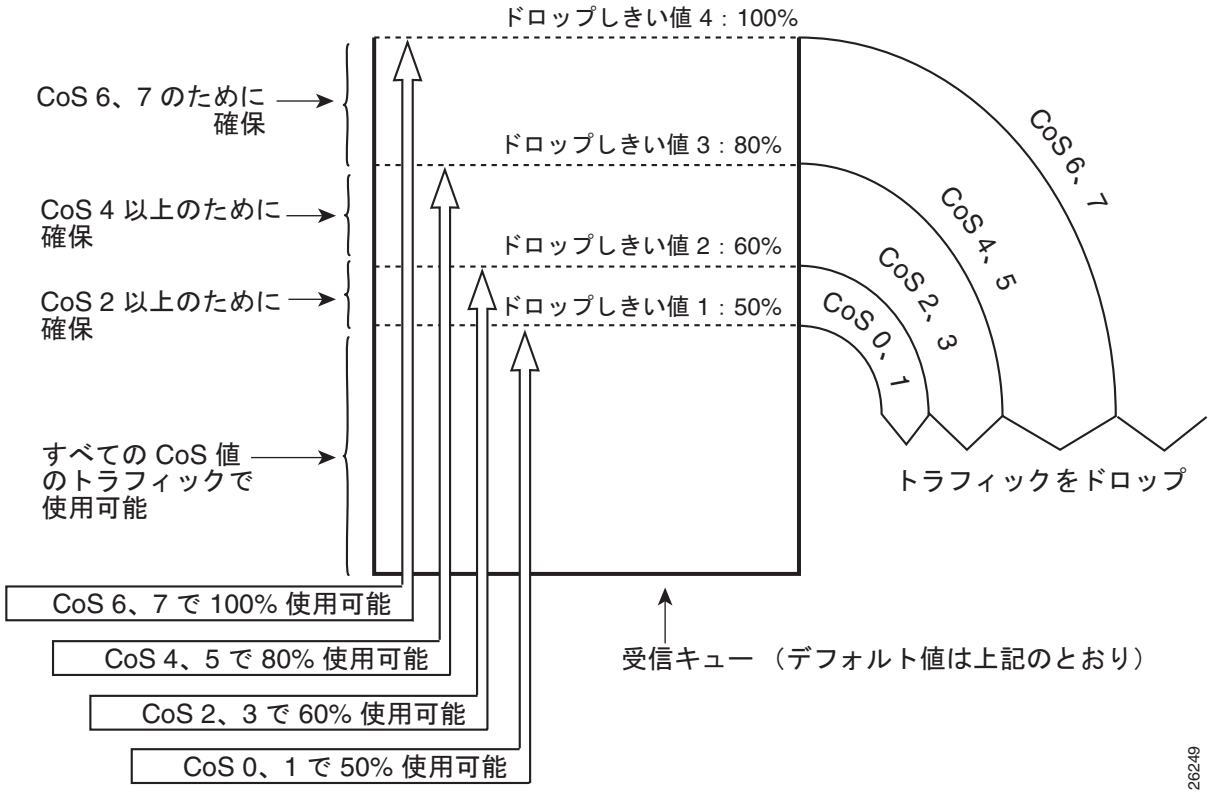
- テール廃棄スレッシュホールド - テール廃棄スレッシュホールドを設定したポートでは、特定の QoS ラベルを持つフレームは、この QoS ラベルに関連付けられた廃棄スレッシュホールドが超過するまで、キューへの入力を許可されます。同じ QoS ラベルを持つ以降のフレームは、スレッシュホールドの超過状態が解消するまで廃棄されます。たとえば、スレッシュホールドが 2 のキュー 1 に CoS 1 が割り当てられ、スレッシュホールド 2 の水準が 60% であるとします。この場合、CoS 1 を持つフレームは、キュー 1 が 60% 占有されるまでは廃棄されません。以降のすべての CoS 1 フレームは、キューの占有率が 60 % 未満になるまで廃棄されます。一部のポート タイプでは、テール廃棄スレッシュホールドおよび WRED 廃棄スレッシュホールドの両方を使用するように標準受信キューを設定するには、CoS 値をキューにマッピングするか、またはキューおよびスレッシュホールドにマッピングします。スイッチでは、キューにだけマッピングされている CoS 値を伝送するトラフィックには、テール廃棄スレッシュホールドが使用されます。キューおよびスレッシュホールドにマッピングされている CoS 値を伝送するトラフィックには、WRED 廃棄スレッシュホールドが使用されます。同じタイプの LAN ポートは、すべて同じ廃棄スレッシュホールドの設定を使用します。

（注）　Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで、DSCP ベースのキューおよびスレッシュホールドをイネーブルにできます（「DSCP ベースのキュー マッピングの設定」（P.41-108）を参照）。

複数のキューを組み合わせ、各キューにスケジューリング アルゴリズムを関連付けることで、スイッチでの輻輳回避を実行できます。

図 41-10 に、**1q4t** 入力 LAN ポートの廃棄スレッシュホールドを示します。他の設定でも、廃棄スレッシュホールドは同様に機能します。

図 41-10　受信キューの廃棄スレッシュホールド



入力キューのタイプ

LAN ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **1q2t** は、1 つの設定変更可能なテール廃棄スレッシュホールドおよび 1 つの設定変更できないテール廃棄スレッシュホールドがある、1 つの標準キューを意味します。
- **1q4t** は、4 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キューを意味します。
- **1q8t** は、8 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キューを意味します。
- **2q8t** は、それぞれ 8 つの設定変更可能なテール廃棄スレッシュホールドがある 2 つの標準キューを意味します。
- **8q4t** は、それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 4 つのスレッシュホールドがある、8 つの標準キューを意味します。
- **8q8t** は、それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 8 つのスレッシュホールドがある 8 つの標準キューを意味します。
- **1p1q4t** は次を意味します。
  - 1 つの完全優先キュー
  - 4 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キュー

- **1p1q0t** は次を意味します。
  - 1 つの完全優先キュー
  - 設定変更可能なスレッシュホールドがない 1 つの標準キュー（実質的には 100% のテール廃棄スレッシュホールド）
- **1p1q8t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 1 つの標準キュー：
    - それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 8 つのスレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド

出力キューのタイプ

出力 LAN ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **2q2t** は、それぞれ 2 つの設定変更可能なテール廃棄スレッシュホールドがある 2 つの標準キューを意味します。
- **1p2q2t** は次を意味します。
  - 1 つの完全優先キュー
  - それぞれ 2 つの設定変更可能な WRED 廃棄スレッシュホールドがある 2 つの標準キュー
- **1p3q1t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 3 つの標準キュー：
    - WRED 廃棄またはテール廃棄として設定変更可能な 1 つのスレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド
- **1p2q1t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 2 つの標準キュー：
    - 1 つの WRED 廃棄スレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド
- **1p3q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED 廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 8 つある、3 つの標準キュー
- **1p7q4t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED 廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 4 つある、7 つの標準キュー

- **1p7q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED 廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 8 つある、7 つの標準キュー

モジュールとキュー タイプのマッピング

次の表は、モジュールとキュー構造のマッピングを示します。

- スーパーバイザ エンジン モジュールの QoS キュー構造
- イーサネットおよびファスト イーサネット モジュールのキュー構造
- ギガビットおよび 10/100/1000 イーサネット モジュール
- 10 ギガビット イーサネット モジュール

表 41-2　スーパーバイザ エンジン モジュールの QoS キュー構造

スーパーバイザ エンジン	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-SUP720	1p1q4t	—	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-SUP720-3B							
WS-SUP720-3BXL							
WS-SUP32-10GE	2q8t	WRR	1p3q8t	DWRR SRR			
10 ギガビット イーサネット ポート					193 MB	105 MB	88 MB
ギガビット イーサネット ポート					17.7 MB	9.6 MB	8.1 MB
WS-SUP32-GE					17.7 MB	9.6 MB	8.1 MB
WS-X6K-S2U-MSFC2	1p1q4t	—	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6K-S2-MSFC2							
WS-X6K-S2-PFC2							

表 41-3　イーサネットおよびファスト イーサネット モジュールのキュー構造

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6524-100FX-MM	1p1q0t	—	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6548-RJ-21							
WS-X6548-RJ-45							
WS-X6324-100FX-MM	1q4t	—	2q2t	WRR	128 KB	16 KB	112 KB
WS-X6324-100FX-SM							
WS-X6348-RJ-45							
WS-X6348-RJ-45V							
WS-X6348-RJ-21V							
WS-X6224-100FX-MT					64 KB	8 KB	56 KB
WS-X6248-RJ-45							
WS-X6248-TEL							
WS-X6248A-TEL					128 KB	16 KB	112 KB
WS-X6148-RJ-45							
WS-X6148-RJ-45V							
WS-X6148-45AF							
WS-X6148-RJ-21							
WS-X6148-RJ-21V							
WS-X6148-21AF							
WS-X6148A-RJ45	1p1q4t	—	1p3q8t	DWRR	5.3 MB	60KB	5.3 MB
WS-X6148A-45AF							
WS-X6148X2-RJ-45	1p1q0t	—	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6148X2-45AF							
WS-X6196-RJ-21							
WS-X6196-21AF							
WS-X6024-10FL-MT	1q4t	—	2q2t	WRR	64 KB	8 KB	56 KB

表 41-4　ギガビットおよび 10/100/1000 イーサネット モジュール

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6816-GBIC	1p1q4t	—	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6748-GE-TX および DFC3	2q8t	WRR	1p3q8t	DWRR	1.3 MB	166 KB	1.2 MB
WS-X6748-GE-TX および CFC	1q8t	—					
WS-X6748-SFP および DFC3	2q8t	WRR					
WS-X6748-SFP および CFC	1q8t	—					
WS-X6724-SFP および DFC3	2q8t	WRR					
WS-X6724-SFP および CFC	1q8t	—					
WS-X6548-GE-TX	1q2t	—	1p2q2t	WRR	1.4 MB	185 KB	1.2 MB
WS-X6548V-GE-TX							
WS-X6548-GE-45AF							
WS-X6516-GBIC	1p1q4t	—	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6516A-GBIC				WRR	1 MB	135 KB	946 KB
WS-X6516-GE-TX				WRR	512 KB	73 KB	439 KB
WS-X6408-GBIC	1q4t	—	2q2t	WRR		80 KB	432 KB
WS-X6408A-GBIC	1p1q4t	—	1p2q2t	WRR		73 KB	439 KB
WS-X6416-GBIC							
WS-X6416-GE-MT							
WS-X6316-GE-TX							
WS-X6148-GE-TX	1q2t	—			1.4 MB	185 KB	1.2 MB
WS-X6148V-GE-TX							
WS-X6148-GE-45AF							
WS-X6148A-GE-TX			1p3q8t	DWRR	5.5 MB	120 KB	5.4 MB
WS-X6148A-GE-45AF							

表 41-5　10 ギガビット イーサネット モジュール

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6708-10GE	8q4t	DWRR	1p7q4t	DWRR SRR	200 MB	108 MB	90 MB
WS-X6704-10GE および DFC3	8q8t	WRR	1p7q8t	DWRR	16 MB	2 MB	14 MB
WS-X6704-10GE および CFC	1q8t	—					
WS-X6502-10GE	1p1q8t	—	1p2q1t	DWRR	64.2 MB	256 KB	64 MB
WS-X6501-10GEX4							

PFC QoS のデフォルト設定

ここでは、PFC QoS デフォルトの設定手順について説明します。

- 「PFC QoS のグローバルな設定」（P.41-32）
- 「PFC QoS がイネーブルの場合のデフォルト値」（P.41-33）
- 「PFC QoS がディセーブルの場合のデフォルト値」（P.41-54）

PFC QoS のグローバルな設定

次のグローバル PFC QoS 設定が適用されます。

機能	デフォルト値
PFC QoS のグローバル イネーブル ステート	ディセーブル
PFC QoS のポート イネーブル ステート	PFC QoS がグローバルにイネーブルの場合、イネーブル
ポートの CoS 値	0
マイクロフロー ポリシング	イネーブル
VLAN 内マイクロフロー ポリシング	ディセーブル
ポート ベースまたは VLAN ベースの PFC QoS	ポートベース
受信した CoS と初期内部 DSCP とのマッピング（受信した CoS 値に基づき設定された初期内部 DSCP）	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
受信した IP precedence と初期内部 DSCP とのマッピング（受信した IP precedence 値に基づき設定された初期内部 DSCP）	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
最終内部 DSCP と出力 CoS とのマッピング（最終内部 DSCP 値に基づき設定された出力 CoS）	DSCP 0–7 = CoS 0 DSCP 8–15 = CoS 1 DSCP 16–23 = CoS 2 DSCP 24–31 = CoS 3 DSCP 32–39 = CoS 4 DSCP 40–47 = CoS 5 DSCP 48–55 = CoS 6 DSCP 56–63 = CoS 7
DSCP マップからの DSCP のマークダウン	マークダウンされた DSCP 値は元の DSCP 値と等しい（マークダウンなし）
ポリサー	なし
ポリシー マップ	なし
プロトコル独立型 MAC ACL フィルタリング	ディセーブル
VLAN ベースの MAC ACL QoS フィルタリング	ディセーブル

PFC QoS がイネーブルの場合のデフォルト値

ここでは、PFC QoS がイネーブルである場合に適用されるデフォルト値を示します。

（注）　入力 LAN ポート信頼状態は、QoS がイネーブルで untrusted にデフォルト設定されています。

受信キューの制限

機能	デフォルト値
2q8t	ロー プライオリティ：80%
	ハイ プライオリティ：20%
8q4t	ロー プライオリティ：80%
	中間キュー：0%
	ハイ プライオリティ：20%
8q8t	最小プライオリティ：80%
	中間キュー：0%
	最大プライオリティ：20%

送信キューの制限

機能	デフォルト値
2q2t	ロー プライオリティ：80%
	ハイ プライオリティ：20%
1p2q2t	ロー プライオリティ：70%
	ハイ プライオリティ：15%
	完全優先：15%
1p2q1t	ロー プライオリティ：70%
	ハイ プライオリティ：15%
	完全優先：15%
1p3q8t	ロー プライオリティ：50%
	ミディアム プライオリティ：20%
	ハイ プライオリティ：15%
	完全優先：15%

機能	デフォルト値
1p7q4t	標準キュー 1（最小プライオリティ）：50%
	標準キュー 2：20%
	標準キュー 3：15%
	標準キュー 4 ～ 7：0%
	完全優先：15%
1p7q8t	標準キュー 1（最小プライオリティ）：50%
	標準キュー 2：20%
	標準キュー 3：15%
	標準キュー 4 ～ 7：0%
	完全優先：15%

帯域幅割り当て比率

機能	デフォルト値
2q8t	90:10
8q4t	90:0:0:0:0:0:0:10
8q8t	90:0:0:0:0:0:0:10
1p3q8t	100:150:200
1p7q4t	100:150:200:0:0:0:0:0
1p7q8t	100:150:200:0:0:0:0
1p2q1t	100:255
2q2t、**1p2q2t**、および **1p2q1t**	5:255
1p3q1t	100:150:255

デフォルトの廃棄スレッシュホールドの割合および CoS 値マッピング

次のテーブルでは、キュー タイプ別の デフォルトの廃棄スレッシュホールド値および CoS 値マッピングを示します。

（注）　ここに示す受信キューの値は、CoS または DSCP を信頼するようにポートを設定した場合に有効です。信頼できないポートの場合は、受信キューの値は、QoS をグローバルにディセーブルにした場合と同じ値となります。

1q2t 受信キュー

機能			デフォルト値
標準受信キュー	スレッシュホールド 1	CoS	0、1、2、3、4
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	5、6、7
		テール廃棄	100%（設定はできません）
		WRED 廃棄	サポートされません。

1q4t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0 および 1
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	2 および 3
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 3	CoS	4 および 5
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。

1p1q4t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0 および 1
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	2 および 3
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 3	CoS	4
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。
完全優先受信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p1q0t 受信キュー

機能		デフォルト値
標準受信キュー	CoS	0、1、2、3、4、6、7
	テール廃棄	100%（設定はできません）
	WRED 廃棄	サポートされません。
完全優先受信キュー	CoS	5
	テール廃棄	100%（設定はできません）

1p1q8t 受信キュー

機能			デフォルト値
標準受信キュー	スレッシュホールド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	1
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 3	CoS	2
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：80%
	スレッシュホールド 4	CoS	3
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：80%
	スレッシュホールド 5	CoS	4
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：60%、ハイ：90%
	スレッシュホールド 6	CoS	6
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：60%、ハイ：90%
	スレッシュホールド 7	CoS	7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
完全優先受信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1q8t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	なし
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 3	CoS	1, 2, 3, 4
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 4	CoS	なし
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 5	CoS	6 および 7
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 6	CoS	なし
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 7	CoS	5
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッショルド 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。

2q8t 受信キュー

機能			デフォルト値
標準受信キュー 1 （ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	70%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 3	CoS	4
		テール廃棄	90%
		WRED 廃棄	サポートされません。
	スレッシュホールド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッシュホールド 5 ～ 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。
標準受信キュー 2 （ハイ プライオリティ）	スレッシュホールド 1	CoS	5
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。

8q4t 受信キュー

機能			デフォルト値
標準受信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		DSCP	
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：80%
	スレッシュホールド 3	CoS	4
		DSCP	
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：90%
	スレッシュホールド 4	CoS	6 および 7
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：100%

機能 （続き）			デフォルト値
標準受信キュー 2 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	14
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	12
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	10
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準受信キュー 3 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	22
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	20
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	18
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
標準受信キュー 4 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	24 および 30
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	28
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	26
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準受信キュー 5 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	32、34 ～ 38
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
標準受信キュー 6 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	48 ～ 63
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準受信キュー 7 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
標準受信キュー 8 （ハイ プライオリティ）	スレッシュホールド 1	CoS	5
		DSCP	40 および 46
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

8q8t 受信キュー

機能			デフォルト値
標準受信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：80%
	スレッシュホールド 3	CoS	4
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：90%
	スレッシュホールド 4	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：100%
	スレッシュホールド 5 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：100%
標準受信キュー 2 ～ 7 （ミディアム プライオリティ）	スレッシュホールド 1 ～ 8	CoS	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準受信キュー 8 （最大プライオリティ）	スレッシュホールド 1	CoS	5
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

2q2t 送信キュー

機能			デフォルト値
標準送信キュー 1 （ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	100%
		WRED 廃棄	サポートされません。
標準送信キュー 2 （ハイ プライオリティ）	スレッシュホールド 1	CoS	4 および 5
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。

1p2q2t 送信キュー

機能			デフォルト値
標準送信キュー 1 （ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：70%、ハイ：100%
標準送信キュー 2 （ハイ プライオリティ）	スレッシュホールド 1	CoS	4 および 6
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	7
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p3q8t 送信キュー

機能			デフォルト値
標準送信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 5 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：100%
標準送信キュー 2 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	2
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	3 および 4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%

機能 （続き）			デフォルト値
標準送信キュー 3 （ハイ プライオリティ）	スレッシュホールド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p7q4t 送信キュー

機能			デフォルト値
標準送信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、 21、23、25、27、29、31、33、 39、41 ～ 45、47
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3	CoS	4
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 4	CoS	6 および 7
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%

機能 （続き）			デフォルト値
標準送信キュー 2 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	14
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	なし
		DSCP	12
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	10
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 3 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	22
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	20
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	18
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%

機能 （続き）			デフォルト値
標準送信キュー 4 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	24 および 30
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	28
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	26
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準送信キュー 5 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	32、34 ～ 38
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
標準送信キュー 6 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	48 ～ 63
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
標準送信キュー 7 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
完全優先送信キュー		CoS	5
		DSCP	40 および 46
		テール廃棄	100%（設定はできません）

1p7q8t 送信キュー

機能			デフォルト値
標準送信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 2 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	2
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッシュホールド 2	CoS	3 および 4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 3 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：100%、 ハイ：100%

機能 （続き）			デフォルト値
標準送信キュー 4 ～ 7 （ミディアム プライオリティ）	スレッシュホールド 1 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：100%、 ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p3q1t 送信キュー

機能			デフォルト値
標準送信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 2 （ミディアム プライオリティ）	スレッシュホールド 1	CoS	2、3、4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 3 （ハイ プライオリティ）	スレッシュホールド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p2q1t 送信キュー

機能			デフォルト値
標準送信キュー 1 （最小プライオリティ）	スレッシュホールド 1	CoS	0、1、2、3
		テール廃棄	サポートされません。
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
標準送信キュー 3 （ハイ プライオリティ）	スレッシュホールド 1	CoS	4、6、7
		テール廃棄	サポートされません。
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

PFC QoS がディセーブルの場合のデフォルト値

機能	デフォルト値
入力 LAN ポートの信頼状態	trust DSCP
受信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キュー帯域幅割り当て比率	255:1.
送信キュー容量の比率	ロー プライオリティ：100%（他のキューが使用されない場合）
CoS 値および廃棄スレッシュホールドのマッピング	すべての QoS ラベルをロー プライオリティ キューにマッピング

PFC QoS 設定時の注意事項および制約事項

PFC QoS を設定する際に、次の注意事項と制約事項に従ってください。

全般的な注意事項

- **match ip precedence** および **match ip dscp** コマンドは、IPv4 トラフィックだけをフィルタリングします。
- Release 12.2(18)SXE 以降のリリースでは、**match precedence** および **match dscp** コマンドは IPv4 および IPv6 トラフィックをフィルタリングします。
- Release 12.2(18)SXE 以降のリリースでは、**set ip dscp** および **set ip precedence** コマンドは **set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は IPv4 および IPv6 トラフィックに対して **set dscp** および **set precedence** ポリシー マップ クラス コマンドをサポートします。
- QoS、NetFlow、および NetFlow Data Export（NDE; NetFlow データ エクスポート）のフローマスク要件は、特にマイクロフロー ポリシングを設定する場合に競合する可能性があります。
- 再マーキングされた DSCP に対する出力 ACL サポート、および VACL キャプチャの両方を 1 つのインターフェイス上に設定すると、VACL キャプチャによって各パケットが 2 コピーずつキャプチャされることがあります。この場合、2 つめのコピーは壊れている可能性があります。

- 再マーキングされた DSCP に対する出力 ACL サポートは、トンネル インターフェイスには設定できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートは、IP ユニキャスト トラフィックをサポートします。
- 再マーキングされた DSCP に対する出力 ACL のサポートは、マルチキャスト トラフィックとは無関係です。PFC QoS は出力 QoS を適用する前に、入力 QoS の変更をマルチキャスト トラフィックに適用します。
- NetFlow および NetFlow データ エクスポート（NDE）は、再マーキングされた DSCP に対する出力 ACL のサポートが設定されたインターフェイスはサポートしません。
- 再マーキングされた DSCP に対する出力 ACL のサポートをいずれかのインターフェイスに設定している場合に、これを設定していないインターフェイスで NetFlow および NDE のサポートをイネーブルにするには、インターフェイス固有のフローマスクを設定する必要があります。**mls flow ip interface-destination-source**、または **mls flow ip interface-full** のいずれかのグローバル コンフィギュレーション モード コマンドを入力してください。
- 再マーキングされた DSCP に対する出力 ACL のサポートを設定しているインターフェイスでは、インターフェイス カウンタの値が不正確となります。
- マイクロフロー ポリシングを IPv6 マルチキャスト トラフィックに適用できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、マイクロフロー ポリシングを適用できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、MPLS トラフィックとしてタグを付けることはできません（このトラフィックは、他のネットワーク装置上では MPLS トラフィックとしてタグ付けできます）。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません（CSCea23571）。
- トラフィックに集約ポリシングとマイクロフロー ポリシングを実行する場合、集約ポリサーおよびマイクロフロー ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。
- トンネル インターフェイス上では、PFC QoS 機能を設定できません。
- PFC QoS は、トンネル トラフィックのペイロード ToS バイトを書き換えません。
- PFC QoS フィルタリングの基準になるのは、ACL、DSCP 値、または IP precedence 値だけです。
- 次のコマンドに対し、PFC QoS は同一 ASIC によって制御されるすべての LAN ポートに、同じ設定を適用します。
  - **rcv-queue random-detect**
  - **rcv-queue queue-limit**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**（ギガビット イーサネット LAN ポートを除く）
  - **priority-queue cos-map**
  - **rcv-queue cos-map**
  - **wrr-queue cos-map**
  - **wrr-queue threshold**

  - **rcv-queue threshold**
  - **wrr-queue random-detect**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue random-detect max-threshold**
- これらのコマンドは、物理ポートだけで設定してください。論理インターフェイスでは設定できません。
  - **priority-queue cos-map**
  - **wrr-queue cos-map**
  - **wrr-queue random-detect**
  - **wrr-queue random-detect max-threshold**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue threshold**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**
  - **rcv-queue cos-map**
  - **rcv-queue bandwidth**
  - **rcv-queue random-detect**
  - **rcv-queue random-detect max-threshold**
  - **rcv-queue random-detect min-threshold**
  - **rcv-queue queue-limit**
  - **rcv-queue cos-map**
  - **rcv-queue threshold**

（注）　出力パケット レプリケーションを使用する IP マルチキャスト スイッチングは、QoS と互換性がありません。場合によっては、出力レプリケーションを実行するとパケットで不正な COS マーキングまたは DSCP マーキングが行われる可能性があります。QoS を使用していて、スイッチング モジュールが出力レプリケーションできる場合は、**mls ip multicast replication-mode ingress** コマンドを入力して出力レプリケーションを強制してください。

PFC3 に関する注意事項

- Release 12.2(18)SXE 以降のリリースでは、PFC3 の全バージョンで、IPv6 ユニキャストおよびマルチキャスト トラフィックに対する QoS がサポートされます。
- IPv6 PFC QoS についての情報を表示するには、**show mls qos ipv6** コマンドを入力します。
- ポート ASIC（キュー アーキテクチャおよびデキューイング アルゴリズム）に実装された QoS 機能は、IPv4 および IPv6 トラフィックをサポートします。
- PFC3 は、IPv6 の名前付き拡張 ACL、および名前付き標準 ACL をサポートします。
- Release 12.2(18)SXE 以降のリリースでは、PFC3 は **match protocol ipv6** コマンドをサポートします。

- TCAM 検索のフロー キー ビット要件が競合するため、IPv6 DSCP ベースのフィルタリングと Ipv6 レイヤ 4 範囲ベースのフィルタリングは同一インターフェイス上に設定できません。次に、例を示します。
  - 1 つの IPv6 Access Control Entry（ACE; アクセス制御エントリ）内に DSCP 値と、レイヤ 4 の「greater than（gt）」または「less than（lt）」演算子を、両方設定した場合、この ACL は PFC QoS フィルタリングには使用できません。
  - 1 つの IPv6 ACL 内に DSCP 値を設定し、別の IPv6 ACL 内にレイヤ 4 の「greater than（gt）」または「less than（lt）」演算子を設定した場合は、同一インターフェイス上の異なるクラスマップで両方の ACL を使用して、PFC QoS フィルタリングを行うことはできません。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに集約ポリサーおよびマイクロフロー ポリサーを適用できますが、IPv6 マルチキャスト トラフィックにはマイクロフロー ポリシングを適用できません。
- 再マーキングされた DSCP に対する出力 ACL サポートを設定すると、PFC3 は次の機能に対するハードウェア支援を行わなくなります。
  - Cisco IOS 再帰 ACL
  - TCP インターセプト
  - Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）
  - Network Address Translation（NAT; ネットワーク アドレス変換）
- PFC3 では、マイクロフロー ポリシングを ARP トラフィックに適用できません。
- PFC3 は、MSFC3 へブリッジされるトラフィックに出力ポリシングを適用しません。
- PFC3 は、MSFC3 からのマルチキャスト トラフィックに出力ポリシングまたは出力 DSCP 変換を適用しません。
- PFC3 では、PFC QoS はブリッジド マルチキャスト トラフィックの ToS バイトを書き換えません。
- PFC3 は最大 1022 の集約ポリサーをサポートしますが、**police** コマンド以外の一部の PFC QoS コマンドはこの数に含まれます。デフォルトでは、**set** コマンドまたは **trust** コマンドを使用するポリシーは集約ポリサー数に含まれます。**no mls qos marking statistics** コマンドを入力することにより、集約ポリサー数への **set** コマンドまたは **trust** コマンドの 追加をディセーブルにすることができますが、これらのコマンドに関連付けられているクラスマップの統計情報を収集できなくなります。**show platform hardware capacity qos** コマンドの出力の QoS Policer Resources セクションで、集約ポリサー数を確認できます。

PFC2 に関する注意事項

- PFC2 は **match protocol** クラス マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入出力両方のトラフィックをすべて送信し、MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm
- PFC2 は、次の PFC QoS 機能をサポートしていません。
  - 出力ポリシング
  - 出力 DSCP 変換
  - DSCP の透過性
  - DFC が取り付けられている場合の VLAN ベースの QoS
- PFC2 は、IEEE 802.1Q トンネル ポートでの入力 CoS 変換に対応したモジュールをサポートしていません。

クラス マップ コマンドの制約事項

- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は **match any** クラス マップ コマンドをサポートします。
- PFC QoS は、***match*** コマンドが **1 つだけ**指定されているクラス マップをサポートします。
- PFC QoS では、次のクラス マップ コマンドはサポートされません。
  - **match cos**
  - **match classmap**
  - **match destination-address**
  - **match input-interface**
  - **match qos-group**
  - **match source-address**

ポリシー マップ コマンドの制約事項

PFC QoS では、次のポリシー マップ コマンドはサポートされません。

- **class** *class_name* **destination-address**
- **class** *class_name* **input-interface**
- **class** *class_name* **protocol**
- **class** *class_name* **qos-group**
- **class** *class_name* **source-address**

ポリシー マップ クラス コマンドの制約事項

PFC QoS では、次のポリシー マップ クラス コマンドはサポートされません。

- **bandwidth**
- **priority**
- **queue-limit**
- **random-detect**
- **set qos-group**
- **service-policy**

CIR および PIR レート値に対してサポートされる粒度

PFC QoS では、CIR および PIR レート値に対し、ハードウェアで次の粒度が使用されます。

CIR および PIR レート値の範囲	粒度
32768 ～ 2097152（2 Mbs）	32768（32 Kb）
2097153 ～ 4194304（4 Mbs）	65536（64 Kb）
4194305 ～ 8388608（8 Mbs）	131072（128 Kb）
8388609 ～ 16777216（16 Mbs）	262144（256 Kb）
16777217 ～ 33554432（32 Mbs）	524288（512 Kb）
33554433 ～ 67108864（64 Mbs）	1048576（1 Mb）
67108865 ～ 134217728（128 Mbs）	2097152（2 Mb）
134217729 ～ 268435456（256 Mbs）	4194304（4 Mb）
268435457 ～ 536870912（512 Mbs）	8388608（8 Mb）
536870913 ～ 1073741824（1 Gps）	16777216（16 Mb）
1073741825 ～ 2147483648（2 Gps）	33554432（32 Mb）
2147483649 ～ 4294967296（4 Gps）	67108864（64 Mb）
4294967296 ～ 8589934592（8 Gps）	134217728（128 Mb）
8589934592 ～ 10000000000（10 Gps）	268435456（256 Mb）

各範囲で、PFC QoS は粒度の倍数に相当するレート値を使用して、PFC をプログラミングします。

CIR および PIR トークン バケット サイズに対してサポートされる粒度

PFC QoS では、CIR および PIR トークン バケット（バースト）サイズに対し、ハードウェアで次の粒度が使用されます。

CIR および PIR トークン バケット サイズの範囲	粒度
1 ～ 32768（32 KB）	1024（1 KB）
32769 ～ 65536（64 KB）	2048（2 KB）
65537 ～ 131072（128 KB）	4096（4 KB）
131073 ～ 262144（256 KB）	8196（8 KB）
262145 ～ 524288（512 KB）	16392（16 KB）
524289 ～ 1048576（1 MB）	32768（32 Kb）
1048577 ～ 2097152（2 MB）	65536（64 KB）
2097153 ～ 4194304（4 MB）	131072（128 KB）
4194305 ～ 8388608（8 MB）	262144（256 KB）
8388609 ～ 16777216（16 MB）	524288（512 KB）
16777217 ～ 33554432（32 MB）	1048576（1 MB）

各範囲で、PFC QoS は粒度の倍数に相当するトークン バケット サイズを使用して、PFC をプログラミングします。

IP precedence 値と DSCP 値

3 ビット IP precedence	ToS の MSb 上位 6 ビット[1]						6 ビット DSCP
	8	7	6	5	4	3	
0	0	0	0	0	0	0	0
	0	0	0	0	0	1	1
	0	0	0	0	1	0	2
	0	0	0	0	1	1	3
	0	0	0	1	0	0	4
	0	0	0	1	0	1	5
	0	0	0	1	1	0	6
	0	0	0	1	1	1	7
1	0	0	1	0	0	0	8
	0	0	1	0	0	1	9
	0	0	1	0	1	0	10
	0	0	1	0	1	1	11
	0	0	1	1	0	0	12
	0	0	1	1	0	1	13
	0	0	1	1	1	0	14
	0	0	1	1	1	1	15
2	0	1	0	0	0	0	16
	0	1	0	0	0	1	17
	0	1	0	0	1	0	18
	0	1	0	0	1	1	19
	0	1	0	1	0	0	20
	0	1	0	1	0	1	21
	0	1	0	1	1	0	22
	0	1	0	1	1	1	23
3	0	1	1	0	0	0	24
	0	1	1	0	0	1	25
	0	1	1	0	1	0	26
	0	1	1	0	1	1	27
	0	1	1	1	0	0	28
	0	1	1	1	0	1	29
	0	1	1	1	1	0	30
	0	1	1	1	1	1	31

3 ビット IP precedence	ToS の MSb 上位 6 ビット[1]						6 ビット DSCP
	8	7	6	5	4	3	
4	1	0	0	0	0	0	32
	1	0	0	0	0	1	33
	1	0	0	0	1	0	34
	1	0	0	0	1	1	35
	1	0	0	1	0	0	36
	1	0	0	1	0	1	37
	1	0	0	1	1	0	38
	1	0	0	1	1	1	39
5	1	0	1	0	0	0	40
	1	0	1	0	0	1	41
	1	0	1	0	1	0	42
	1	0	1	0	1	1	43
	1	0	1	1	0	0	44
	1	0	1	1	0	1	45
	1	0	1	1	1	0	46
	1	0	1	1	1	1	47
6	1	1	0	0	0	0	48
	1	1	0	0	0	1	49
	1	1	0	0	1	0	50
	1	1	0	0	1	1	51
	1	1	0	1	0	0	52
	1	1	0	1	0	1	53
	1	1	0	1	1	0	54
	1	1	0	1	1	1	55
7	1	1	1	0	0	0	56
	1	1	1	0	0	1	57
	1	1	1	0	1	0	58
	1	1	1	0	1	1	59
	1	1	1	1	0	0	60
	1	1	1	1	0	1	61
	1	1	1	1	1	0	62
	1	1	1	1	1	1	63

1. MSb = Most Significant bit（最上位ビット）

PFC QoS の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で PFC QoS を設定する手順について説明します。

（注）　PFC QoS は、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

PFC QoS のグローバルなイネーブル化

PFC QoS をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	スイッチで PFC QoS をグローバルにイネーブルにします。
	`Router(config)# no mls qos`	スイッチで PFC QoS をグローバルにディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos [ipv6]`	設定を確認します。

次に、PFC QoS をグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# mls qos
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos
  QoS is enabled globally
  Microflow QoS is enabled globally

QoS global counters:
    Total packets: 544393
    IP shortcut packets: 1410
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 467
    IP packets with COS changed by policing: 59998
    Non-IP packets with COS changed by policing: 0

Router#
```

ignore port trust のイネーブル化

Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能を使用できます。これにより、入力ポリシーにおいて、設定済みの IP precedence または DSCP 値を、信頼できないトラフィックだけではなくすべてのトラフィックに適用できます。

ignore port trust をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos marking ignore port-trust`	スイッチで ignore port trust をグローバルにイネーブルにします。
	`Router(config)# no mls qos marking ignore port-trust`	スイッチで ignore port trust をグローバルにディセーブルにします（デフォルト）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos | include ignores`	設定を確認します。

（注）　信頼できないトラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。

- IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
- 認識可能な ToS バイトが含まれないトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。

次に、ignore port trust をイネーブルにし、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos marking ignore port-trust
Router(config)# end
Router# show mls qos | include ignores
  Policy marking ignores port_trust
Router#
```

DSCP の透過性の設定

（注）
- 他の IP トラフィックへのサポートに加え、PFC3B および PFC3BXL は MPLS トラフィック、IP-in-IP トンネルのトラフィック、GRE トンネルのトラフィックに対して、**no mls qos rewrite ip dscp** コマンドをサポートします。
- PFC3A は、MPLS トラフィック、IP-in-IP トンネルのトラフィック、GRE トンネルのトラフィック以外の IP トラフィックすべてに対して、**no mls qos rewrite ip dscp** コマンドをサポートします。

DSCP 透過性をイネーブルにして、受信したレイヤ 3 ToS バイトを保持するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos rewrite ip dscp`	スイッチで出力 ToS バイトの書き換えをグローバルにディセーブルにします。
	`Router(config)# mls qos rewrite ip dscp`	スイッチで出力 ToS バイトの書き換えをグローバルにイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos | include rewrite`	設定を確認します。

受信したレイヤ 3 ToS バイトを保持する場合、QoS では出力キューイング用に、およびタグ付き出力トラフィックで、マーキングした CoS 値またはマークダウンした CoS 値が使用されます。

次に、受信したレイヤ 3 ToS バイトを保持し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# no mls qos rewrite ip dscp
Router(config)# end
Router# show mls qos | include rewrite
  QoS ip packet dscp rewrite disabled globally
Router#
```

queueing-only モードのイネーブル化

スイッチで queueing-only モードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos queueing-only`	スイッチで queueing-only モードをイネーブルにします。
	`Router(config)# no mls qos queueing-only`	スイッチで PFC QoS をグローバルにディセーブルにします。 （注）　queueing-only モードは個別にディセーブルにできません。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos`	設定を確認します。

queueing-only モードをイネーブルにする場合、スイッチは次の処理を行います。

- マーキングおよびポリシングをグローバルにディセーブルにします。
- すべてのポートがレイヤ 2 CoS を信頼するように設定します。

（注）　スイッチでは、タグなし入力トラフィックと、trust CoS に設定できないポートを介して受信されるトラフィックにポート CoS 値が適用されます。

次に、queueing-only モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# mls qos queueing-only
Router(config)# end
Router#
```

ブリッジド トラフィックのマイクロフロー ポリシングのイネーブル化

（注）　PFC2 の場合、マルチキャスト トラフィックにマイクロフロー ポリシングを適用するには、レイヤ 3 マルチキャスト入力インターフェイスで **mls qos bridged** コマンドを入力する必要があります。

デフォルトでは、マイクロフロー ポリサーはルーテッド トラフィックだけに影響します。特定の VLAN 上のブリッジド トラフィックに対してマイクロフロー ポリシングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **mls qos bridged**	VLAN 上で、ブリッジド トラフィック（ブリッジ グループも含む）のマイクロフロー ポリシングをイネーブルにします。
	Router(config-if)# **no mls qos bridged**	ブリッジド トラフィックのマイクロフロー ポリシングをディセーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show mls qos**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、VLAN 3 ～ 5 のブリッジド トラフィックに対してマイクロフロー ポリシングをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface range vlan 3 - 5
Router(config-if)# mls qos bridged
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos | begin Bridged QoS
Bridged QoS is enabled on the following interfaces:
    Vl3 Vl4 Vl5
<...output truncated...>
Router#
```

レイヤ 2 LAN ポートでの VLAN ベース PFC QoS のイネーブル化

（注）
- PFC2 では、DFC が搭載されている場合、VLAN ベースの QoS は PFC QoS によってサポートされません。
- PFC3 では、DFC3 が搭載されている場合、VLAN ベースの QoS がサポートされます。
- PFC3 では、出力トラフィックに対する PFC QoS アプリケーション用に、レイヤ 3 インターフェイスにポリシー マップを付加できます。レイヤ 2 ポート上の VLAN ベースまたはポート ベースの PFC QoS は、レイヤ 3 インターフェイス上の出力トラフィックに対する PFC QoS アプリケーションとは関係ありません。

デフォルトでは、PFC QoS は LAN ポートに付加されたポリシー マップを使用します。**switchport** キーワードを使用してレイヤ 2 LAN ポートとして設定されているポートでは、PFC QoS が VLAN に付加されたポリシー マップを使用するように設定できます。**switchport** キーワードを使用せずに設定されたポートは、VLAN に関連付けられません。

レイヤ 2 LAN ポートで VLAN ベース PFC QoS をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**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 2	Router(config-if)# **mls qos vlan-based**	レイヤ 2 LAN ポートまたはレイヤ 2 EtherChannel で VLAN ベース PFC QoS をイネーブルにします。
	Router(config-if)# **no mls qos vlan-based**	VLAN ベース PFC QoS をディセーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show mls qos**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/42 で VLAN ベースの PFC QoS をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/42
Router(config-if)# mls qos vlan-based
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show mls qos | begin QoS is vlan-based
  QoS is vlan-based on the following interfaces:
    Fa5/42
<...Output Truncated...>
```

（注）　レイヤ 2 LAN ポートを VLAN ベースの PFC QoS に設定しても、ポリシー マップに関するポート設定はそのままの状態です。**no mls qos vlan-based** ポート コマンドを使用すると、すでに設定されていたポート コマンドが再びイネーブルになります。

再マーキングされた DSCP に対する出力 ACL のサポートのイネーブル化

再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイスでイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	設定する入力インターフェイスを選択します。
ステップ 2	Router(config-if)# **platform ip features sequential** [**access-group** *IP_acl_name_or_number*]	再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイス上でイネーブルにします。
	Router(config-if)# **no platform ip features sequential** [**access-group** *IP_acl_name_or_number*]	再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイス上でディセーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show running-config interface** ({*type*[1] *slot/port*} | {**port-channel** *number*}}	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

再マーキングされた DSCP に対する出力 ACL のサポートを入力インターフェイスに設定する場合は、次の点に注意してください。

- 再マーキングされた DSCP に対する出力 ACL のサポートを、特定の標準 ACL、拡張名前付き ACL、または拡張番号付き IP ACL によってフィルタリングしたトラフィックだけに対してイネーブルにするには、IP ACL の名前または番号を入力します。
- IP ACL 名または番号を入力しないと、再マーキングされた DSCP に対する出力 ACL のサポートは、インターフェイス上のすべての IP 入力 IP トラフィックに対してイネーブルになります。

次に、再マーキングされた DSCP に対する出力 ACL のサポートを、ファスト イーサネット ポート 5/36 上でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# platform ip features sequential
Router(config-if)# end
```

名前付き集約ポリサーの作成

名前付き集約ポリサーを作成するには、次の作業を行います。

コマンド	目的
Router(config)# **mls qos aggregate-policer** *policer_name bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit**[1] *dscp_value* | **set-prec-transmit**[1] *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	名前付き集約ポリサーを作成します。
Router(config)# **no mls qos aggregate-policer** *policer_name*	名前付き集約ポリサーを削除します。

1. **set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。

名前付き集約ポリサーを作成する場合、次の点に注意してください。

- 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチ仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに集約ポリサーを適用できます。
- PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。
- PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS 設定時の注意事項および制約事項」（P.41-54）を参照してください。
- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 - 32 Kbps（32000 と入力）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。

- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - 最小トークン バケット サイズは 1 KB（1000 と入力）（*maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります）。
  - 最大トークン バケット サイズは 512 MB（512000000 と入力）。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 4000 で割った値よりも大きくなるように設定します。トークンは 1 秒の 4000 分の 1（0.25 ミリ秒）ごとにバケットから削除されるからです。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、パラメータには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
- 有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 - 32 Kbps（32000 と入力、CIR *bits_per_second* パラメータより小さい値は使用できません）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- （任意）一致する適合トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。このアクションでは、ポリシー マップ クラスに *trust* コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が **trust dscp** に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマークするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマークします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致したトラフィックをすべて廃棄するには、**drop** キーワードを入力します。

（注）　**drop** を conform アクションとして設定すると、PFC QoS は **drop** を exceed アクションおよび violate アクションとして設定します。

- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

（注）　exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致した不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意）PIR を超過するトラフィックについて、violate アクションを次のように指定できます。
  - ポリシングを行わずにトラフィックをマーキングするには、**transmit** キーワードを入力して、一致する不適合トラフィックをすべて送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致した不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致した不適合トラフィックをすべて送信します。

（注）　入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

次に、1 Mbps のレート制限および 10 MB のバースト サイズの名前付き集約ポリサーを作成し、適合するトラフィックを送信し、不適合トラフィックをマークダウンする例を示します。

```
Router(config)# mls qos aggregate-policer aggr-1 1000000 10000000 conform-action transmit
exceed-action policed-dscp-transmit
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos aggregate-policer aggr-1
ag1 1000000 1000000 conform-action transmit exceed-action policed-dscp-transmit AgId=0
[pol4]
Router#
```

出力では次の情報が表示されます。

- ハードウェア ポリサー ID は、**AgId** パラメータで表示されます。
- ポリサーを使用しているポリシー マップは、角カッコ（[]）で囲まれて表示されます。

PFC QoS ポリシーの設定

ここでは、PFC QoS ポリシーの設定手順について説明します。

（注）　PFC QoS ポリシーは、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

PFC QoS ポリシー設定作業の概要

（注）　帯域幅利用を制限しないでトラフィックをマーキングするには、適合するトラフィックと適合しないトラフィックの両方に対して、**transmit** キーワードを使用するポリサーを作成します。

次に示すコマンドを使用すると、トラフィック クラスおよびトラフィック クラスに適用されるポリシーが設定され、ポートにポリシーが付加されます。

- **access-list**（IP トラフィックの場合は任意です。IP トラフィックは **class-map** コマンドでフィルタリングできます。）
  - PFC QoS は、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	あり： 1 ～　99 1300 ～ 1999	あり： 100 ～　199 2000 ～ 2699	あり
IPv6	—	あり（名前付き）	あり
IPX（PFC2 でだけサポート）	あり：800 ～ 899	あり：900 ～ 999	あり
MAC レイヤ	なし	なし	あり
ARP	なし	なし	あり

  - Release 12.2(18)SXE 以降のリリースでは、PFC3 は IPv6 名前付き拡張 ACL、および名前付き標準 ACL をサポートします。

- Release 12.2(18)SXD 以降のリリースでは、PFC3 は ARP ACL をサポートします。

（注）
- PFC2 は IP ACL を ARP トラフィックに適用します。
- PFC3 は IP ACL を ARP トラフィックに適用しません。
- PFC3 の場合は、マイクロフロー ポリシングを ARP トラフィックに適用できません。

- PFC3 は IPX ACL をサポートしません。PFC3 では、IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
- PFC2 の場合、PFC QoS は、*source-network* パラメータ、任意の *destination-network* パラメータ、任意の *destination-node* パラメータを備えた IPX ACL をサポートしています。PFC QoS は、他のパラメータ（*source-node*、*protocol*、*source-socket*、*destination-socket*、または *service-type* など）を備えた IPX ACL をサポートしていません。
- PFC2 または PFC3 の場合、PFC QoS は時間ベースの Cisco IOS ACL をサポートします。
- MAC ACL および ARP ACL 以外の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm
- Catalyst 6500 シリーズ スイッチの ACL の詳細については、第 33 章「ネットワーク セキュリティの設定」を参照してください。

- **class-map**（任意）- **class-map** コマンドを使用してトラフィックの分類基準を指定することにより、1 つまたは複数のトラフィック クラスを定義します。
- **policy-map** - **policy-map** コマンドを使用して、次の定義を行います。
  - ポリシー マップ クラスの信頼モード
  - 集約ポリシングおよびマーキング
  - マイクロフロー ポリシングおよびマーキング
- **service-policy** - **service-policy** コマンドを使用して、ポリシー マップをインターフェイスに付加します。

MAC ACL の設定

ここでは、MAC ACL の設定手順について説明します。

（注）　VLAN ACL（VACL）で MAC ACL を使用できます。詳細については、第 35 章「VLAN アクセス制御リスト（VACL）の設定」を参照してください。

プロトコル独立型 MAC ACL フィルタリングの設定

Release 12.2(18)SXD 以降のリリースでは、PFC3BXL モードおよび PFC3B モードは、プロトコル独立型 MAC ACL フィルタリングをサポートします。プロトコル独立型 MAC ACL フィルタリングでは、MAC ACL をすべての入力トラフィック タイプ（MAC レイヤ トラフィックのほかに IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に適用します。

次のインターフェイス タイプを プロトコル独立型 MAC ACL フィルタリングに設定できます。

- IP アドレスのない VLAN インターフェイス
- EoMPLS をサポートするように設定された物理 LAN ポート
- EoMPLS をサポートするように設定された論理 LAN サブインターフェイス

プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否された入力トラフィックは、出力インターフェイスによって MAC レイヤ トラフィックとして処理されます。プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否されたトラフィックに、出力 IP ACL を適用することはできません。

プロトコル独立型 MAC ACL フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID}	{type[1] slot/port[.subinterface]}	{port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mac packet-classify`	インターフェイス上でプロトコル独立型 MAC ACL フィルタリングをイネーブルにします。
	`Router(config-if)# no mac packet-classify`	インターフェイス上でプロトコル独立型 MAC ACL フィルタリングをディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

プロトコル独立型 MAC ACL フィルタリングを設定する場合、次の点に注意してください。

- IP アドレスが設定されている VLAN インターフェイス上で、プロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックがブリッジされる場合、またはレイヤ 3 がハードウェアで PFC3BXL によってスイッチングされる場合は、マイクロフロー ポリシングにプロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックが MSFC3 によってソフトウェアでルーティングされる場合は、プロトコル独立型 MAC ACL フィルタリングはマイクロフロー ポリシングをサポートします。

次に、VLAN インターフェイス 4018 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface vlan 4018
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface vlan 4018 | begin 4018
interface Vlan4018
mtu 9216
ipv6 enable
mac packet-classify
end
```

次に、ギガビット イーサネット インターフェイス 6/1 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 6/1
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 6/1 | begin 6/1
interface GigabitEthernet6/1
mtu 9216
no ip address
mac packet-classify
mpls l2transport route 4.4.4.4 4094
end
```

次に、ギガビット イーサネット インターフェイス 3/24 およびサブインターフェイス 4000 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 3/24.4000
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 3/24.4000 | begin 3/24.4000
interface GigabitEthernet3/24.4000
encapsulation dot1Q 4000
mac packet-classify
mpls l2transport route 4.4.4.4 4000
end
```

VLAN ベースの MAC QoS フィルタリングのイネーブル化

Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングを、PFC3BXL または PFC3B モードでグローバルにイネーブルまたはディセーブルにできます。MAC ACL の VLAN ベースの QoS 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。

MAC ACL の VLAN ベースの QoS フィルタリングをイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mac packet-classify use vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをイネーブルにします。

MAC ACL の VLAN ベースの QoS フィルタリングをディセーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# no mac packet-classify use vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをディセーブルにします。

MAC ACL の設定

MAC アドレスに基づいて IPX（PFC3 でだけサポートされている MAC ACL による IPX フィルタリング）、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングする名前付き ACL を設定できます。

Release 12.2(17b)SXA 以降のリリースの PFC3BXL または PFC3B モードでは、VLAN ベースのフィルタリング、CoS ベースのフィルタリング、または両方のフィルタリングを行うように MAC ACL を設定できます。

Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングを、グローバルにイネーブルまたはディセーブルにできます（デフォルトではディセーブル）。

MAC ACL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mac access-list extended` *list_name*	MAC ACL を設定します。
	`Router(config)# no mac access-list extended` *list_name*	MAC ACL を削除します。
ステップ 2	`Router(config-ext-macl)#` {**permit** | **deny**} {*src_mac_mask* | **any**} {*dest_mac_mask* | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]	MAC ACL にアクセス制御エントリ（ACE）を設定します。
	`Router(config-ext-macl)#` **no** {**permit** | **deny**} {*src_mac_mask* | **any**} {*dest_mac_mask* | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]	MAC ACL から ACE を削除します。

MAC レイヤ ACL のエントリを設定する場合、次の点に注意してください。

- PFC3 は、**ipx-arpa** および **ipx-non-arpa** キーワードをサポートしています。
- PFC2 は、**ipx-arpa** および **ipx-non-arpa** キーワードをサポートしていません。
- **vlan** および **cos** キーワードは、Release 12.2(17b)SXA 以降のリリースの PFC3BXL または PFC3B モードでサポートされます。
- **vlan** および **cos** キーワードは、VACL フィルタリングに使用する MAC ACL ではサポートされません。
- Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングに対する **vlan** キーワードは、グローバルにイネーブルまたはディセーブルにできます。デフォルトではディセーブルに設定されています。
- MAC アドレスは、ドット付き 16 進表記の 3 つの 2 バイト値で入力できます。たとえば、0030.9629.9f84 を入力できます。
- MAC アドレス マスクは、ドット付き 16 進表記の 3 つの 2 バイト値で入力できます。1 のビットをワイルドカードとして使用します。たとえば、アドレスを完全に一致させるには、0000.0000.0000 を使用します（0.0.0 と入力してもかまいません）。
- EtherType および EtherType マスクを 16 進値で入力できます。
- プロトコル パラメータを指定しないエントリは、どのプロトコルとも一致します。
- ACL エントリは、入力順に従ってスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。

- ACL の末尾に **permit any any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny any any** エントリが存在します。
- 既存のリストに新しいエントリを追加すると、新しいエントリはすべてリストの末尾に置かれます。リストの途中にはエントリを追加できません。
- 次に、EtherType の値と対応するプロトコル キーワードを示します。
  - 0x0600 - xns-idp - Xerox XNS IDP
  - 0x0BAD - vines-ip - Banyan VINES IP
  - 0x0baf - vines-echo - Banyan VINES Echo
  - 0x6000 - etype-6000 - DEC 未割り当て、実験的
  - 0x6001 - mop-dump - DEC Maintenance Operation Protocol（MOP）ダンプ/ロード補助
  - 0x6002 - mop-console - DEC MOP リモート コンソール
  - 0x6003 - decnet-iv - DEC DECnet Phase IV Route
  - 0x6004 - lat - DEC Local Area Transport（LAT）
  - 0x6005 - diagnostic - DEC DECnet Diagnostics
  - 0x6007 - lavc-sca - DEC Local-Area VAX Cluster（LAVC）、SCA
  - 0x6008 - amber - DEC AMBER
  - 0x6009 - mumps - DEC MUMPS
  - 0x0800 - ip - Malformed、invalid、または deliberately corrupt IP フレーム
  - 0x8038 - dec-spanning - DEC LANBridge Management
  - 0x8039 - dsm - DEC DSM/DDP
  - 0x8040 - netbios - DEC PATHWORKS DECnet NETBIOS Emulation
  - 0x8041 - msdos - DEC Local Area System Transport
  - 0x8042 - etype-8042 - DEC 未割り当て
  - 0x809B - appletalk - Kinetics EtherTalk（AppleTalk over Ethernet）
  - 0x80F3 - aarp - Kinetics AppleTalk Address Resolution Protocol（AARP）

次に、mac_layer という名前の MAC レイヤ ACL を作成する例を示します。この ACL は、送信元アドレスが 0000.4700.0001、宛先アドレスが 0000.4700.0009 である dec-phase-iv トラフィックを拒否しますが、それ以外のトラフィックをすべて許可します。

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

QoS フィルタリングに対する ARP ACL の設定

（注）
- PFC2 では、IP ACL を ARP トラフィックに適用します。
- PFC3 では、IP ACL を ARP トラフィックに適用しません。
- PFC3 では、マイクロフロー ポリシングを ARP トラフィックに適用できません。

PFC3 および Release 12.2(18)SXD 以降のリリースを使用する場合、ARP トラフィック（EtherType 0x0806）を QoS にフィルタリングする名前付き ACL を設定できます。

QoS フィルタリング用に ARP ACL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# arp access-list list_name`	QoS フィルタリングに ARP ACL を設定します。
	`Router(config)# no arp access-list list_name`	ARP ACL を削除します。
ステップ 2	`Router(config-arp-nacl)# {permit | deny} {ip {any | host sender_ip | sender_ip sender_ip_wildcardmask} mac any`	QoS フィルタリングに対する ARP ACL のアクセス制御エントリ（ACE）を設定します。
	`Router(config-arp-nacl)# no {permit | deny} {ip {any | host sender_ip | sender_ip sender_ip_wildcardmask} mac any`	ARP ACL から ACE を削除します。

ARP ACL のエントリを QoS フィルタリングに設定する場合、次の点に注意してください。

- このマニュアルでは、PFC3 によってハードウェアでサポートされる ARP ACL 構文について説明します。疑問符（?）を入力した場合に Command-Line Interface（CLI; コマンドライン インターフェイス）ヘルプで表示されるその他の ARP ACL 構文はサポートされず、QoS の ARP トラフィックのフィルタリング処理にも使用できません。
- ACL エントリは、入力順に従ってスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。
- ACL の末尾に **permit ip any mac any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny ip any mac any** エントリが存在します。
- 既存のリストに新しいエントリを追加すると、新しいエントリはすべてリストの末尾に置かれます。リストの途中にはエントリを追加できません。

次に、arp_filtering という名前の ARP ACL を作成する例を示します。この ACL は、IP アドレスが 1.1.1.1 から始まるトラフィックだけを許可します。

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 1.1.1.1 mac any
```

クラス マップの設定

ここでは、クラス マップの設定手順について説明します。

- 「クラス マップの作成」（P.41-77）
- 「クラス マップ フィルタリングの注意事項および制約事項」（P.41-77）
- 「クラス マップでのフィルタリングの設定」（P.41-78）

クラス マップの作成

クラス マップを作成するには、次の作業を行います。

コマンド	目的
Router(config)# **class-map** *class_name*	クラス マップを作成します。
Router(config)# **no class-map** *class_name*	クラス マップを削除します。

クラス マップ フィルタリングの注意事項および制約事項

クラス マップ フィルタリングを設定する場合は、次の注意事項および制約事項に従ってください。

- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は、**match-any** キーワードを使用して設定した複数の一致基準をクラス マップ内でサポートします。
- 1 つの **match-any** クラス マップに複数の **match access-group** ACL が含まれ、1 つの ACL に **deny** エントリが含まれる場合、**deny** エントリの後のすべての一致基準（同じ ACL または異なる ACL 内の）は TCAM にインストールされません。

  次の例では、ACL acl4 および acl5 は、**deny ip any any** エントリが含まれる acl3 の後にあるため、インストールされません。

```
ip access-list ext acl3
  deny ip any any

class-map cmap1
  match access-group acl1
  match access-group acl2
  match access-group acl3
  match access-group acl4
  match access-group acl5
```

  この問題を回避するため、次のいずれかの回避策を利用できます。

  - **deny** エントリを ACL の最後に移動し、その ACL をクラス マップの最後に移動します。
  - **deny** エントリの後のすべての ACL を別のクラス マップに設定します。
- Release 12.2(18)SXE よりも前のリリースでは、PFC QoS は 1 つの **match** コマンドを保持するクラス マップをサポートします。
- Release 12.2(18)SXE 以降のリリースでは、PFC3 は **match protocol ipv6** コマンドをサポートします。
- TCAM 検索のフロー キー ビット要件が競合するため、IPv6 DSCP ベースのフィルタリングと Ipv6 レイヤ 4 範囲ベースのフィルタリングは同一インターフェイス上に設定できません。次に、例を示します。
  - 1 つの IPv6 ACE 内に DSCP 値と、レイヤ 4 の「greater than（gt）」または「less than（lt）」演算子を、両方設定した場合、この ACL は PFC QoS フィルタリングには使用できません。
  - 1 つの IPv6 ACL 内に DSCP 値を設定し、別の IPv6 ACL 内にレイヤ 4 の「greater than（gt）」または「less than（lt）」演算子を設定した場合は、同一インターフェイス上の異なるクラス マップで両方の ACL を使用して、PFC QoS フィルタリングを行うことはできません。
- Release 12.2(18)SXE 以降のリリースでは、IPv4 トラフィックに対して **match protocol ip** コマンドがサポートされます。
- Release 12.2(18)SXE 以降のリリースでは、**match any** クラス マップ コマンドがサポートされます。

- PFC QoS は、**match cos**、**match classmap**、**match destination-address**、**match input-interface**、**match qos-group**、および **match source-address** クラス マップ コマンドをサポートしません。
- Catalyst 6500 シリーズ スイッチは、インターフェイスにポリシー マップが付加されない限り、サポート対象外のコマンドが使用されているかどうかを検出しません。
- PFC2 は **match protocol** クラス マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入力と出力の両方のトラフィックをすべて MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm
- 出力 QoS の IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence または DSCP を使用します。出力 QoS フィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。

（注） ここでは、次の ACL に関する内容を説明します。

- 「MAC ACL の設定」（P.41-71）
- 「QoS フィルタリングに対する ARP ACL の設定」（P.41-76）

このマニュアルでは、その他の ACL については説明しません。「PFC QoS ポリシー設定作業の概要」（P.41-70）に記載されている **access-list** の説明を参照してください。

クラス マップでのフィルタリングの設定

クラス マップにフィルタリングを設定するには、次のいずれかの作業を行います。

コマンド	目的
`Router(config-cmap)# match access-group name acl_index_or_name`	（任意）ACL を使用してフィルタリングするように、クラス マップを設定します。
`Router(config-cmap)# no match access-group name acl_index_or_name`	クラス マップから ACL 設定を消去します。
`Router (config-cmap)# match protocol ipv6`	（任意 — IPv6 トラフィック用）IPv6 トラフィックをフィルタリングするように、クラス マップを設定します。
`Router (config-cmap)# no match protocol ipv6`	IPv6 フィルタリングを消去します。
`Router (config-cmap)# match precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	（任意 — IPv4 または IPv6 トラフィック用）最大 8 つの IP precedence 値に基づいてフィルタリングするように、クラス マップを設定します。 **（注）** 送信元ベース、または宛先ベースのマイクロフロー ポリシングをサポートしません。
`Router (config-cmap)# no match precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	設定された IP precedence 値をクラス マップから消去します。
`Router (config-cmap)# match dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	（任意 — IPv4 または IPv6 トラフィックに限る）最大 8 つの DSCP 値に基づいてフィルタリングするように、クラス マップを設定します。 **（注）** 送信元ベース、または宛先ベースのマイクロフロー ポリシングをサポートしません。
`Router (config-cmap)# no match dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	設定された DSCP 値をクラス マップから消去します。

コマンド	目的
Router (config-cmap)# **match ip precedence** *ipp_value1* [*ipp_value2* [*ipp_valueN*]]	(任意 — IPv4 トラフィック用) 最大 8 つの IP precedence 値に基づいてフィルタリングするように、クラス マップを設定します。 **(注)** 送信元ベース、または宛先ベースのマイクロフロー ポリシングをサポートしません。
Router (config-cmap)# **no match ip precedence** *ipp_value1* [*ipp_value2* [*ipp_valueN*]]	設定された IP precedence 値をクラス マップから消去します。
Router (config-cmap)# **match ip dscp** *dscp_value1* [*dscp_value2* [*dscp_valueN*]]	(任意 — IPv4 トラフィック用) 最大 8 つの DSCP 値に基づいてフィルタリングするように、クラス マップを設定します。 **(注)** 送信元ベース、または宛先ベースのマイクロフロー ポリシングをサポートしません。
Router (config-cmap)# **no match ip dscp** *dscp_value1* [*dscp_value2* [*dscp_valueN*]]	設定された DSCP 値をクラス マップから消去します。

クラス マップの設定の確認

クラス マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router (config-cmap)# **end**	コンフィギュレーション モードを終了します。
ステップ 2	Router# **show class-map** *class_name*	設定を確認します。

次に、**ipp5** という名前のクラス マップを作成し、IP precedence 5 のトラフィックと一致するようにフィルタリングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
```

次に、設定を確認する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

ポリシー マップの設定

1 つのインターフェイスに付加できるポリシー マップは、1 つに限られます。ポリシー マップには、ポリシー マップ コマンドがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

インターフェイスで受信するトラフィック タイプごとに、個別のポリシー マップ クラスをポリシー マップ内に設定します。各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。PFC QoS は、一致したトラフィックに複数のポリシー マップ クラスのコマンドを適用することはありません。

ここでは、ポリシー マップの設定手順について説明します。

- 「ポリシー マップの作成」（P.41-80）
- 「ポリシー マップ クラスの設定に関する注意事項および制約事項」（P.41-80）
- 「ポリシー マップ クラスの作成およびフィルタリングの設定」（P.41-81）
- 「ポリシー マップ クラス アクションの設定」（P.41-81）

ポリシー マップの作成

ポリシー マップを作成するには、次の作業を行います。

コマンド	目的
`Router(config)# policy-map policy_name`	ポリシー マップを作成します。
`Router(config)# no policy-map policy_name`	ポリシー マップを削除します。

ポリシー マップ クラスの設定に関する注意事項および制約事項

ポリシー マップ クラスを設定する場合は、次の注意事項および制約事項に従ってください。

- PFC2 は **class** *class_name* **protocol** ポリシー マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入力と出力の両方のトラフィックをすべて MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

- PFC QoS は、**class** *class_name* **destination-address**、**class** *class_name* **input-interface**、**class** *class_name* **qos-group**、および **class** *class_name* **source-address** ポリシー マップ コマンドをサポートしていません。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は **class default** ポリシー マップ コマンドをサポートします。
- PFC QoS は、インターフェイスにポリシー マップが付加されない限り、サポート対象外のコマンドが使用されているかどうかを検出しません。

ポリシー マップ クラスの作成およびフィルタリングの設定

ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap)# class class_name`	ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定します。 （注）　PFC QoS は、**match** コマンドが 1 つだけ指定されているクラス マップをサポートします。
`Router(config-pmap)# no class class_name`	クラス マップの使用を解除します。

ポリシー マップ クラス アクションの設定

ポリシー マップ クラスのアクションを設定する場合、次の点に注意してください。

- ポリシー マップには、1 つまたは複数のポリシー マップ クラスを含めることができます。
- トラフィック タイプごとに、すべての信頼状態およびポリシング コマンドを、同一のポリシー マップ クラスに入れてください。
- PFC QoS は、1 つのポリシー マップ クラスのコマンドだけをトラフィックに適用します。1 つのポリシー マップ クラスのフィルタリングに一致したトラフィックには、他のポリシー マップ クラスで設定したフィルタリングが適用されます。
- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシー マップ クラス コマンドをサポートしません。これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**set qos-group** ポリシー マップ クラス コマンドはサポートされません。
- PFC QoS では、IPv4 トラフィック用の **set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドがサポートされます。
  - Release 12.2(18)SXD 以降のリリースおよび Release 12.2(17d)SXB 以降のリリースでは、非 IP トラフィック上の **set ip dscp** および **set ip precedence** コマンドを使用して、出力レイヤ 2 CoS 値の基準である内部 DSCP 値をマーキングできます。
  - Release 12.2(18)SXE 以降のリリースでは、**set ip dscp** および **set ip precedence** コマンドは **set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は IPv4 および IPv6 トラフィックに対して **set dscp** および **set precedence** ポリシー マップ クラス コマンドをサポートします。
- ポリシー マップ クラスで、次の 3 つすべてを実行することはできません。
  - **set** コマンドによるトラフィックのマーキング
  - 信頼状態の設定
  - ポリシングの設定

  ポリシー マップ クラスでは、トラフィックを **set** コマンドによってマーキングするか、次のいずれか、あるいは両方を実行できます。
  - 信頼状態の設定
  - ポリシングの設定

（注）　ポリシングを設定する場合は、ポリシング キーワードでトラフィックをマーキングできます。

ここでは、ポリシー マップ クラスのアクションを設定する手順について説明します。

- 「ポリシー マップ クラス マーキングの設定」（P.41-82）
- 「ポリシー マップ クラスの信頼状態の設定」（P.41-82）
- 「ポリシー マップ クラスのポリシングの設定」（P.41-83）

ポリシー マップ クラス マーキングの設定

Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能をイネーブルにしている場合、PFC QoS はすべてのトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。

すべてのリリースにおいて PFC QoS は、信頼できないトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。

ポリシー マップ クラス マーキングを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# set {dscp dscp_value | precedence ip_precedence_value}`	ポリシー マップ クラスを設定して、設定されている DSCP 値または IP precedence 値と一致する信頼できないトラフィックをマーキングするようにします。
`Router(config-pmap-c)# no set {dscp dscp_value | precedence ip_precedence_value}`	マーキングの設定を消去します。

（注）　Release 12.2(18)SXE よりも前のリリースでは、**set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドがサポートされます。

ポリシー マップ クラスの信頼状態の設定

（注）　**service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを付加することはできません。

ポリシー マップ クラスの信頼状態を設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# trust {cos | dscp | ip-precedence}`	ポリシー マップ クラスの信頼状態を設定します。この設定によって、PFC QoS が初期内部 DSCP 値の作成元として使用する値が選択されます。
`Router(config-pmap-c)# no trust`	デフォルトのポリシー マップ クラスの信頼状態（untrusted）に戻します。

ポリシー マップ クラスの信頼状態を設定する場合、次の点に注意してください。

- 入力ポート上に設定されている信頼状態を使用するには、**no trust** コマンド（これがデフォルトです）を使用します。
- **cos** キーワードを使用すると、PFC QoS は受信した CoS または入力ポートの CoS に基づいて、内部 DSCP 値を設定します。
- **dscp** キーワードを使用すると、PFC QoS は受信した DSCP を使用します。
- **ip-precedence** キーワードを使用すると、PFC QoS は受信した IP precedence に基づいて DSCP を設定します。

ポリシー マップ クラスのポリシングの設定

ポリシー マップ クラスのポリシングを設定する場合、次の点に注意してください。

- PFC QoS は **set-qos-transmit** ポリサー キーワードをサポートしません。
- PFC QoS は、**exceed-action** キーワードの引数として **set-dscp-transmit** キーワードまたは **set-prec-transmit** キーワードをサポートしません。
- PFC QoS は、インターフェイスにポリシー マップが付加されない限り、サポート対象外のキーワードが使用されているかどうかを検出しません。

ここではポリシー マップ クラスによるポリシングを設定する手順について説明します。

- 「名前付き集約ポリサーの使用」（P.41-83）
- 「インターフェイス別ポリサーの設定」（P.41-84）

（注）　**conform-action transmit** キーワードによるポリシングでは、一致するトラフィックのポート信頼状態が、trust dscp またはポリシー マップ クラスの **trust** コマンドで設定される信頼状態に設定されます。

名前付き集約ポリサーの使用

名前付き集約ポリサーを使用するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police aggregate` *aggregate_name*	定義済みの名前付き集約ポリサーを使用するように、ポリシー マップ クラスを設定します。
`Router(config-pmap-c)# no police aggregate` *aggregate_name*	名前付き集約ポリサーの使用を解除します。

インターフェイス別ポリサーの設定

インターフェイス別のポリサーを設定するには、次の作業を行います。

コマンド	目的
Router(config-pmap-c)# **police** [**flow** [**mask** {**src-only** | **dest-only** | **full-flow**}]] *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	インターフェイス別のポリサーを作成して、それを使用するようにポリシー マップ クラスを設定します。
Router(config-pmap-c)# **no police** [**flow** [**mask** {**src-only** | **dest-only** | **full-flow**}]] *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	ポリシー マップ クラスからインターフェイス別のポリサーを削除します。

インターフェイス別ポリサーを設定する場合、次の点に注意してください。

- 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチ仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。
- PFC3 の場合、入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに集約ポリサーおよびマイクロフロー ポリサーを適用できます。
- PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。
- PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS 設定時の注意事項および制約事項」（P.41-54）を参照してください。

- マイクロフロー ポリサーを定義するには、**flow** キーワードを入力します（マイクロフロー ポリシングは ARP トラフィックには適用できません）。マイクロフロー ポリサーを設定する場合、次の点に注意してください。
  - PFC3 の場合、送信元アドレスだけに基づいてフローの識別を行うには、**mask src-only** キーワードを入力します。これによりマイクロフロー ポリサーが、各送信元アドレスからのすべてのトラフィックに適用されます。Release 12.2(17d)SXB 以降のリリースでは、IP トラフィックと MAC トラフィックの両方で **mask src-only** キーワードをサポートしています。Release 12.2(17d)SXB より以前のリリースでは、IP トラフィックだけで **mask src-only** キーワードをサポートしています。
  - PFC3 の場合、宛先アドレスだけに基づいてフローの識別を行うには、**mask dest-only** キーワードを入力します。これによりマイクロフロー ポリサーが、各送信元アドレスのすべてのトラフィックに適用されます。Release 12.2(17d)SXB 以降のリリースでは、IP トラフィックと MAC トラフィックの両方で **mask dest-only** キーワードをサポートしています。Release 12.2(17d)SXB より以前のリリースでは、IP トラフィックだけで **mask dest-only** キーワードをサポートしています。
  - デフォルトおよび **mask full-flow** キーワードを使用する場合は、PFC QoS は送信元 IP アドレス、宛先 IP アドレス、レイヤ 3 プロトコル、レイヤ 4 ポート番号に基づいて IP フローの識別を行います。
  - PFC2 の場合、PFC QoS は、送信元ノードまたは送信元ソケットが異なるトラフィックを含め、同じ送信元ネットワーク、宛先ネットワーク、および宛先ノードを持つ IPX トラフィックを同じフローの一部であると見なします。
  - PFC QoS は、プロトコルおよび送信元と宛先 MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が違っていても、同じフローの一部であると見なします。
  - マイクロフロー ポリサーでは、*maximum_burst_bytes* パラメータ、**pir** *bits_per_second* キーワードおよびパラメータ、または **violate-action** キーワードはサポートされません。

（注） マイクロフロー ポリシング、NetFlow、および NetFlow データ エクスポート（NDE）のフローマスク要件は、競合する可能性があります。

- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 - 32 Kbps（32000 と入力）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します（**flow** キーワードではサポートされません）。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - 最小トークン バケット サイズは 1 KB（1000 と入力）（*maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります）。
  - 最大トークン バケット サイズは 512 MB（512000000 と入力）。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 4000 で割った値よりも大きくなるように設定します。トークンは 1 秒の 4000 分の 1（0.25 ミリ秒）ごとにバケットから削除されるからです。

  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、パラメータには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
- （**flow** キーワードではサポートされません）有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 - 32 Kbps（32000 と入力、CIR *bits_per_second* パラメータより小さい値は使用できません）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- （任意）一致する適合トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマークするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマークします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致するトラフィックをすべて廃棄するには、**drop** キーワードを入力します。
  - 同じトラフィックに適用する集約ポリサーおよびマイクロフロー ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。
- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致したすべての不適合トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

（注） exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致したすべての不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

（注） **pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意 - **flow** キーワードではサポートされません）PIR を超過するトラフィックに対して、violate アクションを次のように指定できます。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致したすべての不適合トラフィックを送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致したすべての不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

次に、**max-pol-ipp5** という名前のポリシー マップを作成する例を示します。このポリシー マップは、クラス マップ **ipp5** を使用し、受信した IP precedence 値に基づいて信頼状態を設定し、最大容量に関する集約ポリサーおよびマイクロフロー ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

ポリシー マップの設定の確認

ポリシー マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了します。 （注）　ポリシー マップにクラスを追加するには、追加の **class** コマンドを入力します。
ステップ 2	`Router# show policy-map` *policy_name*	設定を確認します。

次に、設定を確認する例を示します。

```
Router# show policy-map max-pol-ipp5
 Policy Map max-pol-ipp5
  class  ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
    trust precedence
    police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit

Router#
```

インターフェイスへのポリシー マップの付加

ポリシー マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*[*.subinterface*]} | {**port-channel** *number*[*.subinterface*]}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **service-policy** [**input** | **output**] *policy_map_name*	ポリシー マップをインターフェイスに付加します。
	Router(config-if)# **no service-policy** [**input** | **output**] *policy_map_name*	インターフェイスからポリシー マップを削除します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show policy-map interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ポリシー マップをインターフェイスに付加するには、次の点に注意してください。

- EtherChannel のメンバであるポートに、サービス ポリシーを付加しないでください。
- DFC が搭載されている場合は、PFC2 は VLAN ベースの QoS をサポートしません。**mls qos vlan-based** コマンドを入力することも、VLAN インターフェイスにサービス ポリシーを付加することもできなくなります。
- PFC QoS は、PFC3 を搭載している場合にだけ、レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）で **output** キーワードをサポートします。PFC3 の場合、入力ポリシー マップと出力ポリシー マップの両方をレイヤ 3 インターフェイスに付加できます。
- レイヤ 2 ポート上の VLAN ベースまたはポートベースの PFC QoS は、**output** キーワードを使用してレイヤ 3 インターフェイスに付加されたポリシーとは関係ありません。
- **output** キーワードが付いたポリシーでは、マイクロフロー ポリシングはサポートされません。
- **service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを付加することはできません。
- **output** キーワードを使用して付加されたポリシーの IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence 値または DSCP 値が使用されます。**output** キーワードを使用して付加されたポリシーの IP precedence または DSCP に基づいたフィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。
- 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチ仮想インターフェイスに適用されたポリサー

  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

- PFC3 の場合、入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

次に、ポリシー マップ **pmap1** をファスト イーサネット ポート 5/36 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show policy-map interface fastethernet 5/36
 FastEthernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class cmap1
    police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
  class cmap2
    police 8000 10000 conform-action transmit exceed-action drop
Router#
```

PFC3 による出力 DSCP 変換の設定

（注） PFC2 は出力 DSCP 変換をサポートしません。

ここでは、PFC3 で出力 DSCP 変換を設定する手順について説明します。

- 「名前付き DSCP 変換マップの設定」（P.41-90）
- 「インターフェイスへの出力 DSCP 変換マップの付加」（P.41-91）

名前付き DSCP 変換マップの設定

名前付き DSCP 変換マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map dscp-mutation** *map_name dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *mutated_dscp*	名前付き DSCP 変換マップを設定します。
	Router(config)# **no mls qos map dscp-mutation** *map_name*	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

名前付き DSCP 変換マップを設定する場合、次の点に注意してください。

- 変換された DSCP 値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を変換された DSCP 値にマッピングできます。
- 変換された DSCP 値ごとに個別のコマンドを入力できます。

次に、DSCP 30 を変換された DSCP 値 8 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map dscp-mutation mutmap1 30 to 8
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map | begin DSCP mutation
DSCP mutation map mutmap1:                    (dscp= d1d2)
     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 :    08 31 32 33 34 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
<...Output Truncated...>
Router#
```

（注） DSCP 変換マップの出力で、マトリクスの本体に表示されるのがマークダウンされた DSCP 値です。元の DSCP 値の最初の桁の数字は d1 のカラムに、2 番目の桁の数字は一番上の行に表示されます。上記の例では、DSCP 30 は DSCP 08 にマッピングされています。

インターフェイスへの出力 DSCP 変換マップの付加

出力 DSCP 変換マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*[*.subinterface*]} | {**port-channel** *number*[*.subinterface*]}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **mls qos dscp-mutation** *mutation_map_name* Router(config-if)# **no mls qos dscp-mutation** *mutation_map_name*	出力 DSCP 変換マップをインターフェイスに付加します。 インターフェイスから出力 DSCP 変換マップを削除します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show running-config interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、mutmap1 という名前の出力 DSCP 変換マップをファスト イーサネット ポート 5/36 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# mls qos dscp-mutation mutmap1
Router(config-if)# end
```

IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定

（注）　Supervisor Engine 2 は、入力 CoS 変換に対応したスイッチング モジュールをサポートしていません。

Release 12.2(17b)SXA 以降のリリースでは、受信した CoS を信頼するように設定された、IEEE 802.1Q トンネル ポートの入力 CoS 変換をサポートします（サポート対象モジュールについては、「入力 CoS 変換の設定に関する注意事項および制約事項」（P.41-92）を参照してください）。

受信した CoS を信頼するように設定された IEEE 802.1Q トンネル ポート上で入力 CoS 変換を設定する場合、PFC QoS は、入力廃棄スレッシュホールド内および任意の trust-CoS マーキングおよびポリシング用の受信した CoS 値ではなく、変換された CoS 値を使用します。

ここでは、入力 CoS 変換の設定手順について説明します。

- 「入力 CoS 変換の設定に関する注意事項および制約事項」（P.41-92）
- 「入力 CoS 変換マップの設定」（P.41-93）
- 「IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用」（P.41-94）

入力 CoS 変換の設定に関する注意事項および制約事項

入力 CoS 変換を設定する場合は、次の注意事項および制約事項に従ってください。

- Release 12.2(17b)SXA 以降のリリースでは、WS-X6704-10GE、WS-X6748-SFP、WS-X6724-SFP、および WS-X6748-GE-TX スイッチング モジュールで入力 CoS 変換がサポートされます。
- IEEE 802.1Q トンネル ポートとして設定されていないポートは、入力 CoS 変換をサポートしません。
- 受信した CoS を信頼するよう設定されていないポートは、入力 CoS 変換をサポートしません。
- 入力 CoS 変換では、カスタマー フレームにより伝送された CoS 値を変更しません。カスタマー トラフィックが 802.1Q トンネルから送出される場合、元の CoS がそのまま残ります。
- 入力 CoS 変換の設定は、ポート グループ内のすべてのポートに適用されます。ポート グループは次のとおりです。
  - WS-X6704-10GE - 4 ポート、4 ポート グループ、各グループに 1 ポート
  - WS-X6748-SFP - 48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
  - WS-X6724-SFP - 24 ポート、2 ポート グループ：ポート 1 ～ 12、13 ～ 24
  - WS-X6748-GE-TX - 48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
- 入力 CoS 変換の設定エラーを回避するために、メンバ ポートのすべてが入力 CoS 変換をサポートしている、またはメンバ ポートのすべてが入力 CoS 変換をサポートしていない EtherChannel だけを作成してください。入力 CoS 変換に対するサポートが混在する EtherChannel を作成しないでください。
- EtherChannel のメンバであるポート上で 入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャネル インターフェイスに適用されます。
- ポートチャネル インターフェイス上で、入力 CoS 変換を設定できます。
- ポートチャネル インターフェイス上で入力 CoS 変換が設定されている場合、次の動作が発生します。
  - 入力 CoS 変換の設定は、EtherChannel のすべてのメンバ ポートのポート グループに適用されます。任意のメンバ ポートが、入力 CoS 変換をサポートできない場合、設定はエラーになります。
  - ポート グループ内のあるポートが、2 番目の EtherChannel のメンバである場合、入力 CoS 変換の設定は、2 番目のポートチャネル インターフェイスおよび 2 番目の EtherChannel のすべてのメンバ ポートのポート グループに適用されます。2 番目の EtherChannel の任意のメンバ ポートが入力 CoS 変換をサポートできない場合、1 番目の EtherChannel 上の設定がエラーになります。1 番目の EtherChannel のメンバ ポートがあるポート グループ内の非メンバ ポートで、設定が行われた場合、この設定は非メンバ ポート上でエラーになります。
  - ポートが CoS を信用するように設定されているかどうか、または IEEE 802.1Q トンネル ポートとして設定されているかどうかにかかわらず、入力 CoS 変換の設定はポート グループ、メンバ ポート、ポートチャネル インターフェイスを通して、制限なく伝播します。
- 入力 CoS 変換を設定する予定の EtherChannel では、入力 CoS 変換をサポートしていないメンバ ポートがある他の EtherChannel のメンバ ポートを含むポート グループ内のポートをメンバとすることができません （この制約は、ポートグループにリンクされるすべてのメンバ ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます）。

- 入力 CoS 変換を設定する予定のポートは、入力 CoS 変換をサポートしていないメンバがある EtherChannel のメンバ ポートを含むポート グループ内に組み込むことはできません （この制約は、ポートグループにリンクされるすべてのメンバ ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます)。
- ポートグループにリンクされるメンバ ポートおよびポートチャネルインターフェイスにリンクされるポートすべてに適用される入力 CoS 変換の設定は、1 つだけです。

入力 CoS 変換マップの設定

入力 CoS 変換マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos map cos-mutation` *mutation_map_name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4 mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8*	入力 CoS 変換マップを設定します。PFC QoS が入力 CoS 値 0 ～ 7 をマッピングする、8 つの変換 CoS 値を入力する必要があります。
	`Router(config)# no mls qos map cos-mutation` *map_name*	名前付きマップを削除します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos maps cos-mutation`	設定を確認します。

次に、testmap という名前の CoS 変換マップを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map cos-mutation testmap 4 5 6 7 0 1 2 3
Router(config)# end
Router#
```

次に、マップの設定を確認する例を示します。

```
Router(config)# show mls qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
------------------------------------
cos-out :   4  5  6  7  0  1  2  3
Router#
```

IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用

IEEE 802.1Q トンネル ポートに入力 CoS 変換マップを付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**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 2	Router(config-if)# **mls qos cos-mutation** *mutation_map_name* Router(config-if)# **no mls qos cos-mutation** *mutation_map_name*	入力 CoS 変換マップをインターフェイスに付加します。 インターフェイスから入力 CoS 変換マップを削除します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show running-config interface** {{*type*[1] *slot/port*} | {**port-channel** *number*}} Router# **show mls qos maps cos-mutation**	設定を確認します。

1. *type* = **gigabitethernet** または **tengigabitethernet**

次に、testmap という名前の入力 CoS 変換マップを、ギガビット イーサネット ポート 1/1 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos cos-mutation testmap
Router(config-if)# end
Router# show mls qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
------------------------------------
cos-out :   4  5  6  7  0  1  2  3

testmap is attached on the following interfaces
Gi1/1
Router#
```

DSCP 値マッピングの設定

ここでは、DSCP 値を他の値にマッピングする方法について説明します。

- 「受信 CoS 値から内部 DSCP 値へのマッピング」（P.41-95）
- 「受信 IP precedence 値から内部 DSCP 値へのマッピング」（P.41-95）
- 「DSCP マークダウン値の設定」（P.41-96）
- 「内部 DSCP 値から出力 CoS 値へのマッピング」（P.41-97）

受信 CoS 値から内部 DSCP 値へのマッピング

受信した CoS 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map cos-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した CoS 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が CoS 値 0 ～ 7 をマッピングする、8 つの DSCP 値を入力する必要があります。
	Router(config)# **no mls qos map cos-dscp**	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

次に、受信した CoS 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map cos-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos maps | begin Cos-dscp map
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     ---------------------------------
         dscp:   0  1  2  3  4  5  6  7
<...Output Truncated...>
Router#
```

受信 IP precedence 値から内部 DSCP 値へのマッピング

受信した IP precedence 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map ip-prec-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した IP precedence 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が受信した IP precedence 値 0 ～ 7 をマッピングする、8 つの内部 DSCP 値を入力する必要があります。
	Router(config)# **no mls qos map ip-prec-dscp**	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

次に、受信した IP precedence 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map ip-prec-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos maps | begin IpPrecedence-dscp map
   IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     ---------------------------------
       dscp:   0  1  2  3  4  5  6  7
<...Output Truncated...>
Router#
```

DSCP マークダウン値の設定

ポリサーが使用する DSCP マークダウン値のマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map policed-dscp** {**normal-burst** | **max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *markdown_dscp*	DSCP マークダウン値のマッピングを設定します。
	Router(config)# **no mls qos map policed-dscp** {**normal-burst** | **max-burst**}	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

DSCP マークダウン値のマッピングを設定する場合、次の点に注意してください。

- **exceed-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**normal-burst** キーワードを使用します。
- **violate-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**max-burst** キーワードを使用します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- パケットの順序誤りを防ぐため、適合するトラフィックおよび適合しないトラフィックが同じキューを使用するように、マークダウン値のマッピングを設定してください。
- マークダウンされた DSCP 値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をマークダウンされた DSCP 値にマッピングできます。
- マークダウンされた DSCP 値ごとに個別のコマンドを入力できます。

（注）　マークダウンされた DSCP 値は、マークダウン ペナルティと矛盾しない CoS 値にマッピングするように設定してください。

次に、DSCP 1 をマークダウンされた DSCP 値 0 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map policed-dscp normal-burst 1 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map
   Normal Burst Policed-dscp map:                                    (dscp= d1d2)
     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 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

   Maximum Burst Policed-dscp map:                                   (dscp= d1d2)
     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 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
<...Output Truncated...>
Router#
```

（注） Policed-dscp の出力で、マトリクスの本体に表示されるのがマークダウンされた DSCP 値です。元の DSCP 値の最初の桁の数字は d1 のカラムに、2 番目の桁の数字は一番上の行に表示されます。上記の例では、DSCP 41 は DSCP 41 にマッピングされています。

内部 DSCP 値から出力 CoS 値へのマッピング

PFC QoS が PFC 上で内部的に使用する DSCP 値から、出力 LAN ポートのスケジューリングおよび輻輳回避に使用される CoS 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map dscp-cos** *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *cos_value*	内部 DSCP 値から出力 CoS 値へのマッピングを設定します。
	Router(config)# **no mls qos map dscp-cos**	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

内部 DSCP 値から出力 CoS 値へのマッピングを設定する場合、次の点に注意してください。

- PFC QoS が CoS 値にマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を CoS 値にマッピングできます。
- CoS 値ごとに個別のコマンドを入力できます。

次に、内部 DSCP 値 0、8、16、24、32、40、48、および 54 を、出力 CoS 値 0 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 54 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map | begin Dscp-cos map
   Dscp-cos map:                                     (dscp= d1d2)
     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 :    06 06 06 06 00 06 07 07 07 07
      6 :    07 07 07 07
<...Output Truncated...>
Router#
```

（注）　Dscp-cos map の出力で、マトリクスの本体に表示されるのが CoS 値です。DSCP 値の最初の桁の数字は d1 のカラムに、2 番目の桁の数字は一番上の行に表示されます。上記の例では、DSCP 値 41 ～ 47 は、いずれも CoS 05 にマッピングしています。

イーサネット LAN ポートおよび OSM ポートの信頼状態の設定

デフォルトでは、すべてのポートは信頼できない（untrusted）状態です。すべてのイーサネット LAN ポートおよび OSM ポートに対し、ポートの信頼状態を設定できます。

（注）　非ギガビット イーサネット **1q4t/2q2t** ポートの場合は、信頼状態をクラス マップ内でも繰り返し設定する必要があります。

ポートの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {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 2	`Router(config-if)# mls qos trust [dscp | ip-precedence | cos[2] ]`	ポートの信頼状態を設定します。
	`Router(config-if)# no mls qos trust`	デフォルトの信頼状態（untrusted）に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface type[1] slot/port | include Trust state`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**ge-wan**、**pos**、または **atm**
2. **serial**、**pos**、または **atm** インターフェイス タイプではサポートされません。

ポートの信頼状態を設定する場合、次の点に注意してください。

- 他のキーワードを指定しない場合、**mls qos trust** コマンドは **mls qos trust dscp** コマンドと同じです。
- Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで **mls qos trust dscp** コマンドを使用して、DSCP ベースの受信キュー廃棄スレッシュホールドをイネーブルにできます（「DSCP ベースのキュー マッピングの設定」（P.41-108）を参照）。DSCP ベースのキュー マッピングがイネーブルにされている場合に、DSCP 値の矛盾によるトラフィック廃棄を防ぐには、受信するトラフィックが明らかにネットワーク ポリシーと矛盾しない DSCP 値である場合に限り、**mls qos trust cos** コマンドを使用してポートを設定します。
- **mls qos trust cos** コマンドを使用すると、CoS ベースの受信キュー廃棄スレッシュホールドがイネーブルになります。CoS 値の矛盾によるトラフィック廃棄を防ぐには、受信するトラフィックが明らかにネットワーク ポリシーと矛盾しない CoS 値を伝送する ISL または 802.1Q フレームである場合に限り、**mls qos trust cos** コマンドを使用してポートを設定します。
- Release 12.2(17b)SXA 以降のリリースでは、**mls qos trust cos** コマンドで設定される IEEE 802.1Q トンネル ポートに、受信された CoS 値ではなく変換された CoS 値を使用するよう設定できます（「IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定」（P.41-91）を参照）。
- ポート状態を untrusted に戻すには、**no mls qos trust** コマンドを使用します。

次に、**trust cos** キーワードを使用してギガビット イーサネット ポート 1/1 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos trust cos
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | include trust
  Trust state: trust COS
Router#
```

入力 LAN ポート CoS 値の設定

（注）　PFC QoS が **mls qos cos** コマンドによって適用された CoS 値を使用するかどうかは、ポートの信頼状態とそのポート経由で受信したトラフィックの信頼状態によって決まります。**mls qos cos** コマンドを入力しても、ポートの信頼状態またはポート経由で受信したトラフィックの信頼状態は設定されません。

mls qos cos コマンドを使用して適用された CoS 値を内部 DSCP の基準として使用するには、次の設定を行います。

- タグなし入力トラフィックだけを受信するポートでは、入力ポートを信頼できるポートとして設定するか、または入力トラフィックと一致する trust CoS ポリシー マップを設定します。
- タグ付き入力トラフィックを受信するポートでは、入力トラフィックと一致する trust CoS ポリシー マップを設定します。

trusted として設定されている入力 LAN ポートからのタグなしフレーム、および untrusted として設定されている入力 LAN ポートからの全フレームに PFC QoS が割り当てる CoS 値を設定できます。

入力 LAN ポートの CoS 値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**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 2	Router(config-if)# **mls qos cos** *port_cos* Router(config-if)# **no mls qos cos** *port_cos*	入力 LAN ポートの CoS 値を設定します。 デフォルトのポート CoS 値に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queuing interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/24 に CoS 値 5 を設定し、設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos cos 5
Router(config-if)# end
Router# show queueing interface fastethernet 5/24 | include Default COS
  Default COS is 5
Router#
```

標準キューの廃棄スレッシュホールドの割合設定

ここでは、標準キューの廃棄スレッシュホールドの割合を設定する手順を説明します。

（注）

- ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。
- **1p1q0t** ポートに、設定変更可能なスレッシュホールドはありません。
- **1p3q1t**（送信）、**1p2q1t**（送信）、および **1p1q8t**（受信）ポートにも、設定変更できないテール廃棄スレッシュホールドがあります。

スレッシュホールドを設定する場合、次の点に注意してください。

- キュー番号 1 は、プライオリティが一番低い標準キューです。
- キュー番号が大きくなると、標準キューのプライオリティが高くなります。

複数のスレッシュホールド標準キューを設定する場合、次の点に注意してください。

- 最初に入力したパーセント値は、プライオリティが一番低いスレッシュホールドを設定します。
- 2 番目に入力したパーセント値は、2 番目にプライオリティが高いスレッシュホールドを設定します。
- 最後に入力したパーセント値は、プライオリティが一番高いスレッシュホールドを設定します。
- 1 ～ 100 の範囲のパーセント値を使用します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。
- プライオリティが一番高いスレッシュホールドは、常に 100% に設定してください。

WRED 廃棄スレッシュホールドを設定する場合、次の点に注意してください。

- WRED 廃棄 スレッシュホールドには、それぞれロー WRED 値およびハイ WRED 値があります。
- ローおよびハイ WRED 値は、キュー容量のパーセント値で表されます（範囲は 1 ～ 100）。
- ロー WRED 値は、トラフィック レベルがその値より下がるとトラフィックがまったく廃棄されなくなる限界を表します。ロー WRED 値には、ハイ WRED 値より小さい値を指定する必要があります。
- ハイ WRED 値は、トラフィック レベルがその値を超過するとすべてのトラフィックが廃棄される限界を表します。
- ロー WRED 値とハイ WRED 値の中間にあるキュー内のトラフィックは、キューが満たされるにつれて、廃棄される可能性が高くなります。

テール廃棄受信キューの設定

次のポート タイプには、受信キューにテール廃棄スレッシュホールドだけがあります。

- **1q2t**
- **1p1q4t**
- **2q8t**
- **1q8t**

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**fastethernet** | **gigabitethernet**} *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue threshold** *queue_id thr1% thr2% thr3% thr4% {thr5% thr6% thr7% thr8%}*	受信キューのテール廃棄スレッシュホールドの割合を設定します。
	Router(config-if)# **no rcv-queue threshold** [*queue_id*]	受信キューのテール廃棄スレッシュホールドをデフォルトの割合に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

次に、ギガビット イーサネット ポート 1/1 について、受信キュー廃棄スレッシュホールドを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | begin Receive queues
Receive queues [type = 1p1q4t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard            4
       2         Priority            1

  Trust state: trust COS

    queue tail-drop-thresholds
    --------------------------
    1     60[1] 75[2] 85[3] 100[4]
<...Output Truncated...>
Router#
```

WRED 廃棄送信キューの設定

次のポート タイプには、送信キューに WRED 廃棄スレッシュホールドだけがあります。

- **1p2q2t**（送信）
- **1p2q1t**（送信）

	コマンド	目的
ステップ 1	Router(config)# **interface** type[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue random-detect min-threshold** *queue_id thr1%* [*thr2%*]	ロー WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **wrr-queue random-detect max-threshold** *queue_id thr1%* [*thr2%*]	ハイ WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。
ステップ 4	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 5	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

WRED 廃棄およびテール廃棄受信キューの設定

次のポート タイプは、受信キューに WRED 廃棄およびテール廃棄スレッシュホールドの両方があります。

- **8q4t**（受信）
- **8q8t**（受信）
- **1p1q8t**（受信）

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	テール廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue threshold** [*queue_id*]	デフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **rcv-queue random-detect min-threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	ロー WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。
ステップ 4	Router(config-if)# **rcv-queue random-detect max-threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	ハイ WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。

	コマンド	目的
ステップ 5	Router(config-if)# **rcv-queue random-detect** *queue_id*	WRED 廃棄スレッシュホールドをイネーブルにします。
	Router(config-if)# **no rcv-queue random-detect** [*queue_id*]	テール廃棄スレッシュホールドをイネーブルにします。
ステップ 6	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 7	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

WRED 廃棄およびテール廃棄送信キューの設定

次のポート タイプは、送信キューに WRED 廃棄およびテール廃棄スレッシュホールドの両方があります。

- **1p3q1t**（送信）
- **1p3q8t**（送信）
- **1p7q8t**（送信）

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue threshold** *queue_id thr1%* [*thr2% thr3% thr4% thr5% thr6% thr7% thr8%*]	テール廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue threshold** [*queue_id*]	デフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **wrr-queue random-detect min-threshold** *queue_id thr1%* [*thr2% thr3% thr4% thr5% thr6% thr7% thr8%*]	ロー WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。
ステップ 4	Router(config-if)# **wrr-queue random-detect max-threshold** *queue_id thr1%* [*thr2% thr3% thr4% thr5% thr6% thr7% thr8%*]	ハイ WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。
ステップ 5	Router(config-if)# **wrr-queue random-detect** *queue_id*	WRED 廃棄スレッシュホールドをイネーブルにします。
	Router(config-if)# **no wrr-queue random-detect** [*queue_id*]	テール廃棄スレッシュホールドをイネーブルにします。
ステップ 6	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 7	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ギガビット イーサネット ポート 1/1 について、ロー プライオリティ送信キューのハイ WRED 廃棄スレッシュホールドを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# wrr-queue random-detect max-threshold 1 70 70
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | begin Transmit queues
  Transmit queues [type = 1p2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         WRR low             2
       2         WRR high            2
       3         Priority            1

    queue random-detect-max-thresholds
    ----------------------------------
      1    40[1] 70[2]
      2    40[1] 70[2]
<...Output Truncated...>
Router#
```

1q4t/2q2t テール廃棄スレッシュホールドの割合設定

次に、**1q4t/2q2t** ポートでの受信キューおよび送信キューの廃棄スレッシュホールドの関係を示します。

- 受信キュー 1（標準）スレッシュホールド 1 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 2 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 2
- 受信キュー 1（標準）スレッシュホールド 3 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 4 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 2

1q4t/2q2t LAN ポートに標準受信キューおよび送信キューのテール廃棄スレッシュホールドの割合を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue threshold** *queue_id thr1% thr2%*	受信キューおよび送信キューのテール廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue threshold** [*queue_id*]	受信キューおよび送信キューのデフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# show queueing interface {**ethernet** | **fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

受信キューおよび送信キューのテール廃棄スレッシュホールドを設定する場合、次の点に注意してください。

- 送信キュー番号およびスレッシュホールド番号を使用する必要があります。
- *queue_id* は、標準ロー プライオリティ キューについては 1、標準ハイ プライオリティ キューについては 2 です。
- 1 ～ 100 の範囲のパーセント値を使用します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。
- スレッシュホールドは常に 2 ～ 100% の範囲で設定してください。
- イーサネットおよびファスト イーサネット **1q4t** ポートは、受信キュー テール廃棄スレッシュホールドをサポートしません。

次に、ギガビット イーサネット ポート 2/1 について、受信キュー 1/スレッシュホールド 1、および送信キュー 1/スレッシュホールド 1 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 2/1
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 2/1
  Transmit queues [type = 2q2t]:

<...Output Truncated...>

queue tail-drop-thresholds
    --------------------------
    1     60[1] 100[2]
    2     40[1] 100[2]

<...Output Truncated...>

Receive queues [type = 1q4t]:

<...Output Truncated...>

queue tail-drop-thresholds
    --------------------------
    1     60[1] 100[2] 40[3] 100[4]
<...Output Truncated...>
Router#
```

QoS ラベルのキューおよび廃棄スレッシュホールドへのマッピング

ここでは、QoS ラベルをキューおよび廃棄スレッシュホールドにマッピングする方法について説明します。

（注）　ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

ここでは、QoS ラベルをキューおよび廃棄スレッシュホールドにマッピングする方法について説明します。

- 「キューおよび廃棄スレッシュホールドへのマッピングに関する注意事項および制約事項」（P.41-107）
- 「DSCP ベースのキュー マッピングの設定」（P.41-108）
- 「CoS ベースのキュー マッピングの設定」（P.41-113）

キューおよび廃棄スレッシュホールドへのマッピングに関する注意事項および制約事項

QoS ラベルをキューおよびスレッシュホールドにマッピングする場合、次の点に注意してください。

- SRR がイネーブルにされている場合は、CoS 値 または DSCP 値を完全優先キューにマッピングできません。
- キュー番号 1 は、プライオリティが一番低い標準キューです。
- キュー番号が大きくなると、標準キューのプライオリティが高くなります。
- 最大 8 つの CoS 値をスレッシュホールドにマッピングできます。
- 最大 64 個の DSCP 値をスレッシュホールドにマッピングできます。
- スレッシュホールド 0 は、次のポート タイプの場合、設定変更できない 100% テール廃棄スレッシュホールドを意味します。
  - **1p1q0t**（受信）
  - **1p1q8t**（受信）
  - **1p3q1t**（送信）
  - **1p2q1t**（送信）
- 標準キュー スレッシュホールドは、次のポート タイプでテール廃棄または WRED 廃棄スレッシュホールドとして設定できます。
  - **1p1q8t**（受信）
  - **1p3q1t**（送信）
  - **1p3q8t**（送信）
  - **1p7q1t**（送信）

DSCP ベースのキュー マッピングの設定

ここでは、DSCP ベースのキュー マッピングを設定する手順について説明します。

- 「入力 DSCP ベースのキュー マッピングの設定」（P.41-108）
- 「標準送信キュー スレッショルドへの DSCP 値のマッピング」（P.41-111）
- 「送信完全優先キューへの DSCP 値のマッピング」（P.41-112）

（注）　DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートでサポートされます。

DSCP ベースのキュー マッピングのイネーブル化

DSCP ベースのキュー マッピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tengigabitethernet slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos queue-mode mode-dscp`	DSCP ベースのキュー マッピングをイネーブルにします。
	`Router(config-if)# no mls qos queue-mode mode-dscp`	CoS ベースのキュー マッピングに戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface tengigabitethernet slot/port | include Queueing Mode`	設定を確認します。

次に、10 ギガビット イーサネット ポート 6/1 上で DSCP ベースのキュー マッピングをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | include Queueing Mode
    Queueing Mode In Tx direction: mode-dscp
    Queueing Mode In Rx direction: mode-dscp
```

入力 DSCP ベースのキュー マッピングの設定

入力 DSCP とキューとのマッピングは、DSCP を信頼するように設定されたポートだけでサポートされます。

ここでは、入力 DSCP ベースのキュー マッピングを設定する手順について説明します。

- 「DSCP ベースのキュー マッピングのイネーブル化」（P.41-108）
- 「標準受信キュー スレッショルドへの DSCP 値のマッピング」（P.41-109）

信頼 DSCP ポートの設定

DSCP を信頼するようにポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **mls qos trust dscp**	受信した DSCP 値を信頼するようにポートを設定します。
	Router(config-if)# **no mls qos trust**	デフォルトの信頼状態（untrusted）に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port* **| include Trust state**	設定を確認します。

次に、10 ギガビット イーサネット ポート 6/1 を、受信した DSCP 値を信頼するように設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface gigabitethernet 6/1
Router(config-if)# mls qos trust dscp
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 6/1 | include Trust state
  Trust state: trust DSCP
```

標準受信キュー スレッシュホールドへの DSCP 値のマッピング

DSCP 値を標準受信キュー スレッシュホールドにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue dscp-map** *queue_# threshold_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	標準受信キューのスレッシュホールドに DSCP 値をマッピングします。
	Router(config-if)# **no rcv-queue dscp-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port*	設定を確認します。

DSCP 値をマッピングする場合、次の点に注意してください。

- キューおよびスレッシュホールドにマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびスレッシュホールドにマッピングできます。
- キューおよびスレッシュホールドごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 6/1 に対して、標準受信キューのスレッシュホールド 1 に DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# rcv-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　受信キュー マッピングは、**show queueing interface** コマンドによって表示される、2 回目の「queue thresh dscp-map」に表示されます。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 1/1 | begin queue thresh dscp-map
<...Output Truncated...>
queue thresh dscp-map
----------------------------------------
1     1      0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45 47
1     2
1     3
1     4
2     1      14
2     2      12
2     3      10
2     4
3     1      22
3     2      20
3     3      18
3     4
4     1      24 30
4     2      28
4     3      26
4     4
5     1      32 34 35 36 37 38
5     2
5     3
5     4
6     1      48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1      40 46
8     2
8     3
8     4
<...Output Truncated...>
Router#
```

標準送信キュー スレッシュホールドへの DSCP 値のマッピング

標準送信キュー スレッシュホールドに DSCP 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue dscp-map** *transmit_queue_# threshold_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	標準送信キューのスレッシュホールドに DSCP 値をマッピングします。
	Router(config-if)# **no wrr-queue dscp-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port*	設定を確認します。

DSCP 値をマッピングする場合、次の点に注意してください。

- キューおよびスレッシュホールドにマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびスレッシュホールドにマッピングできます。
- キューおよびスレッシュホールドごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 6/1 に対して、標準送信キュー 1、およびスレッシュホールド 1 に、DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# wrr-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、8 番目のキューは完全優先キューです。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
queue thresh dscp-map
----------------------------------------
1     1      0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45 47
1     2
1     3
1     4
2     1       14
2     2       12
2     3       10
2     4
3     1       22
3     2       20
3     3       18
3     4
4     1       24 30
4     2       28
4     3       26
4     4
```

```
5     1      32 34 35 36 37 38
5     2
5     3
5     4
6     1      48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1      40 46
<...Output Truncated...>
Router#
```

送信完全優先キューへの DSCP 値のマッピング

DSCP 値を送信完全優先キューにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **priority-queue dscp-map** *queue_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	送信完全優先キューに DSCP 値をマッピングします。複数の **priority-queue dscp-map** コマンドを入力することで、8 つ以上の DSCP 値を完全優先キューにマッピングできます。
	Router(config-if)# **no priority-queue dscp-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port*	設定を確認します。

完全優先キューに DSCP 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に 1 です。
- キューにマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューにマッピングできます。

次に、10 ギガビット イーサネット ポート 6/1 の完全優先キューに、DSCP 値 7 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# priority-queue dscp-map 1 7
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、完全優先キューは 8 番目のキューです。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
    queue thresh dscp-map
    ----------------------------------------
<...Output Truncated...>
    8     1       7 40 46
<...Output Truncated...>
Router#
```

CoS ベースのキュー マッピングの設定

ここでは、CoS ベースのキュー マッピングを設定する手順について説明します。

- 「標準受信キュー スレッシュホールドへの CoS 値のマッピング」（P.41-113）
- 「標準送信キュー スレッシュホールドへの CoS 値のマッピング」（P.41-114）
- 「完全優先キューへの CoS 値のマッピング」（P.41-114）
- 「1q4t/2q2t LAN ポートのテール廃棄スレッシュホールドへの CoS 値のマッピング」（P.41-115）

標準受信キュー スレッシュホールドへの CoS 値のマッピング

CoS 値を標準受信キュー スレッシュホールドにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue cos-map** *queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	標準受信キューのスレッシュホールドに CoS 値をマッピングします。
	Router(config-if)# **no rcv-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ギガビット イーサネット ポート 1/1 に対して、標準受信キューのスレッシュホールド 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1
<...Output Truncated...>
    queue thresh cos-map
    ----------------------------------------
    1     1       0 1
    1     2       2 3
    1     3       4 5
    1     4       6 7
<...Output Truncated...>
Router#
```

標準送信キュー スレッシュホールドへの CoS 値のマッピング

標準送信キュー スレッシュホールドに CoS 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue cos-map** *transmit_queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	標準送信キューのスレッシュホールドに CoS 値をマッピングします。
	Router(config-if)# **no wrr-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/36 に対して、標準送信キュー 1/スレッシュホールド 1 に、CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4 5
    2     2      6 7
<...Output Truncated...>
Router#
```

完全優先キューへの CoS 値のマッピング

CoS 値を送受信完全優先キューにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **priority-queue cos-map** *queue_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	受信および送信完全優先キューに CoS 値をマッピングします。
	Router(config-if)# **no priority-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に 1 です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

次に、ギガビット イーサネット ポート 1/1 の完全優先キューに、CoS 値 7 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1
<...Output Truncated...>
Transmit queues [type = 1p2q2t]:
<...Output Truncated...>
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4
    2     2      6
    3     1      5 7

  Receive queues [type = 1p1q4t]:
<...Output Truncated...>
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4
    1     4      6
    2     1      5 7
<...Output Truncated...>
Router#
```

1q4t/2q2t LAN ポートのテール廃棄スレッシュホールドへの CoS 値のマッピング

（注）　ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

次に、**1q4t/2q2t**LAN ポートでの受信キューおよび送信キューのテール廃棄スレッシュホールドの関係を示します。

- 受信キュー 1（標準）スレッシュホールド 1 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 2 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 2
- 受信キュー 1（標準）スレッシュホールド 3 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 4 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 2

テール廃棄スレッシュホールドに CoS 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# wrr-queue cos-map transmit_queue_# threshold_# cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]`	テール廃棄スレッシュホールドに CoS 値をマッピングします。
ステップ 3	`Router(config-if)# no wrr-queue cos-map`	デフォルトのマッピングに戻します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show queueing interface type[1] slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

テール廃棄スレッシュホールドに CoS 値をマッピングする場合、次の点に注意してください。

- 送信キュー番号およびスレッシュホールド番号を使用する必要があります。
- キュー 1 は、ロー プライオリティ標準送信キューです。
- キュー 2 は、ハイ プライオリティ標準送信キューです。
- キューごとに 2 つのスレッシュホールドがあります。
- スレッシュホールドにマッピングする、最大 8 つの CoS 値を入力します。

次に、ファスト イーサネット ポート 5/36 に対して、標準送信キュー 1/スレッシュホールド 1 に、CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4 5
    2     2      6 7
<...Output Truncated...>
Router#
```

標準送信キュー間での帯域幅の割り当て

スイッチはいずれかのデキューイング アルゴリズムを使用して、一度に 1 つの標準キューからフレームを送信します。デキューイング アルゴリズムはパーセント値または重み値を使用して、ラウンドロビン方式で処理された各キューに、相対的な帯域幅を割り当てます。

- シェイプド ラウンド ロビン（SRR）—SRR を使用すると、1 つのキューは、割り当てられた帯域幅だけの使用が許可されます。Supervisor Engine 32 SFP の **1p3q8t** ポートおよび **1p7q4t** ポートのオプションとしてサポートされます。
- Deficit Weighted Round Robin（DWRR）— より高いプライオリティのキュー内のトラフィックによってプライオリティを低く設定されている、転送中のすべてのキューを追跡し、次回のラウンドでこの差分を補います。DWRR は、**1p3q1t**、**1p2q1t**、**1p3q8t**、**1p7q4t**、および **1p7q8t** ポートでのデキューイング アルゴリズムです。

（注）　DWRR ポートの設定には、WRR ポートで使用するものと同じコマンドを使用します。

- 重み付きラウンドロビン（WRR）- WRR では、他のキューが帯域幅を使用していない場合、キューは割り当てられた帯域幅を超えて、ポートの最大帯域幅まで使用できます。WRR は、他のすべてのポートで有効なデキューイング アルゴリズムです。

Release 12.2(18)SXF 以降のリリースでは、帯域幅の割り当てにパーセント値または重み値を入力できます。Release 12.2(18)SXF よりも前のリリースでは、重み値を入力して帯域幅を割り当てます。

割り当てられたパーセント値または重み値の比率が大きいキューほど、多くの送信帯域幅が割り当てられます。重み値を入力した場合は、重み値間の比率によってキューの合計帯域幅の分割比率が決定します。たとえば、ギガビット イーサネット ポート上の 3 つのキューの場合、重み値は 25:25:50 になり、次のように割り当てられます。

- キュー 1—250 Mbps
- キュー 2—250 Mbps
- キュー 3—500 Mbps

（注）　実際の帯域幅の割り当ては、設定済みのパーセント値または重み値に対してポート ハードウェアが適用する粒度によって異なります。

標準送信キュー間で帯域幅を割り当てるには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue** [**bandwidth** | **shape**] **percent** *low_priority_queue_percentage* [*intermediate_priority_queue_percentages*] *high_priority_queue_percentage* または Router(config-if)# **wrr-queue** [**bandwidth** | **shape**] *low_priority_queue_weight* [*intermediate_priority_queue_weights*] *high_priority_queue_weight*	標準送信キュー間で帯域幅を割り当てます。 • **bandwidth** キーワードを入力して、DWRR または WRR を設定します。 • **shape** キーワードを入力して、SRR を設定します。SRR を使用する場合は、完全優先キューを使用できません。SRR を設定する場合は、完全優先キューにマッピングされたすべての CoS 値または DSCP 値を、標準キューに再マッピングする必要があります（「QoS ラベルのキューおよび廃棄スレッシュホールドへのマッピング」（P.41-107）を参照）。 • 各パーセント値は、必ず合計で 100 となるようにします。また、ポートのすべての標準送信キューに対してパーセント値を入力する必要があります（Release 12.2(18)SXF 以降のリリースでサポートされます）。 • 重み値の有効範囲は 1 ～ 255 です。ポートのすべての標準送信キューに対して重み値を入力する必要があります。
	Router(config-if)# **no wrr-queue** [**bandwidth** | **shape**]	デフォルトの帯域幅の割り当てに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ギガビット イーサネット ポート 1/2 に対して、帯域幅の比率を 3 対 1 に割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/2 | include bandwidth
WRR bandwidth ratios:    3[queue 1]   1[queue 2]
Router#
```

受信キューのサイズ比の設定

2q8t、**8q4t**、および **8q8t** ポートの標準受信キュー間で、さらに **1p1q0t** または **1p1q8t** ポートの完全優先受信キューと標準受信キューとの間で、サイズ比を設定できます。

受信キュー間のサイズ比を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**fastethernet** | **tengigabitethernet**} *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue queue-limit** *low_priority_queue_weight* [*intermediate_priority_queue_weights*] *high_priority_queue_weight* または Router(config-if)# **rcv-queue queue-limit** *standard_queue_weight* *strict_priority_queue_weight*	受信キュー間のサイズ比を設定します。
	Router(config-if)# **no rcv-queue queue-limit**	デフォルトのサイズ比に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** {**fastethernet** | **tengigabitethernet**} *slot/port*	設定を確認します。

受信キュー サイズ比を設定する場合、次の点に注意してください。

- **rcv-queue queue-limit** コマンドは、ASIC 単位でポートを設定します。
- ネットワークにおける、プライオリティの異なるトラフィックの比率を概算してください（例：標準トラフィック 80%、完全優先トラフィック 20% など）。
- 概算したパーセント値を、各キューの重みとして使用します。
- 有効値は 1 ～ 100% です。ただし、**1p1q8t** ポートの場合、完全優先キューの有効値は 3 ～ 100% です。

次に、ファスト イーサネット ポート 2/2 について、受信キュー サイズ比を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 2/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 2/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  15[queue 2]
Router#
```

送信キューのサイズ比の設定

送信キューのサイズ比を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# wrr-queue queue-limit low_priority_queue_weight [intermediate_priority_queue_weights] high_priority_queue_weight`	送信キュー間のキュー サイズ比を設定します。
ステップ 3	`Router(config-if)# priority-queue queue-limit strict_priority_queue_weight`	完全優先キューのサイズを設定します。 （注）　この機能は、すべてのスイッチング モジュールでサポートされているわけではありません。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show queueing interface type[1] slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

送信キュー間の送信キュー サイズ比を設定する場合、次の点に注意してください。

- **wrr-queue queue-limit** コマンドは、**1p3q1t** ポートではサポートされません。
- 出力完全優先キューを持つポートの場合：
  - Release 12.2(18)SXF2 以降のリリースでは、**priority-queue queue-limit** インターフェイス コマンドを入力することで、次のスイッチング モジュールに対して出力完全優先キューのサイズを設定できます。

    —WS-X6502-10GE（**1p2q1t**）
    —WS-X6148A-GE-TX（**1p3q8t**）
    —WS-X6148-RJ-45（**1p3q8t**）
    —WS-X6148-FE-SFP（**1p3q8t**）
    —WS-X6748-SFP（**1p3q8t**）
    —WS-X6724-SFP（**1p3q8t**）
    —WS-X6748-GE-TX（**1p3q8t**）
    —WS-X6704-10GE（**1p7q4t**）
    —WS-SUP32-10GE-3B（**1p3q8t**）
    —WS-SUP32-GE-3B（**1p3q8t**）
    —WS-X6708-10GE（**1p7q4t**）
  - Release 12.2(18)SXF2 よりも前のリリース、および他のモジュールでは、PFC QoS は出力完全優先キューのサイズを、ハイ プライオリティ キューと同じサイズに設定します。
- ネットワークにおけるロー プライオリティ トラフィックとハイ プライオリティ トラフィックの比率を概算してください（例：ロー プライオリティ トラフィック 80%、ハイ プライオリティ トラフィック 20% など）。
- 概算したパーセント値を、各キューの重みとして使用します。
- インターフェイス上の標準送信キューすべてに重み（2、3、または 7 の重み）を入力する必要があります。
- 有効値は 1 ～ 100% です。ただし、**1p2q1t** 出力 LAN ポートの場合、ハイ プライオリティ キューの有効値は 5 ～ 100% です。

次に、ギガビット イーサネット ポート 1/2 に対して、送信キュー サイズ比を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue queue-limit 75 15
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  25[queue 2]
Router#
```

一般的な QoS のシナリオ

ここでは、いくつかの一般的な QoS シナリオでの設定例を示します。使用するネットワークでの PFC QoS の設定方法をすでに理解している場合、または特定の設定情報を確認する場合は、この章内の他のセクションを参照してください。

このセクションで示す各シナリオは、「サンプル ネットワークの設計の概要」（P.41-121）で説明したサンプル ネットワークに基づいています。ここでは、このサンプル ネットワークを使用して、一般的に使用されるいくつかの QoS 設定について説明します。

ここで説明する一般的な QoS シナリオは、次のとおりです。

サンプル ネットワークの設計の概要

このサンプル ネットワークは、アクセス レイヤ、ディストリビューション レイヤ、およびコア レイヤに Catalyst 6500 シリーズ スイッチを使用した、従来的なキャンパス ネットワーク アーキテクチャに基づきます。アクセス レイヤは、デスクトップ ユーザに 10/100 イーサネット サービスを提供します。このネットワークでは、アクセス レイヤとディストリビューション レイヤはギガビット イーサネット リンクで接続され、ディストリビューション レイヤとコア レイヤはギガビットまたは 10 ギガビット イーサネット リンクで接続されます。

基本的なポート設定は次のとおりです。

アクセス レイヤ

```
switchport mode access
switchport access vlan 10
switchport voice vlan 110
```

ディストリビューションおよびコア レイヤのスイッチ間リンク

```
switchport mode trunk
```

このサンプル ネットワークには、次の 3 つのトラフィック クラスがあります。

- 音声
- ハイ プライオリティ アプリケーション トラフィック
- ベストエフォート トラフィック

ここで説明する QoS 設定では、上記の各トラフィック クラスが識別され、優先付けられます。

（注）　これより多くのサービス レベルを必要とするネットワークの場合も、PFC QoS は最大 64 のトラフィック クラスをサポートできます。

各 QoS シナリオでは、次の 3 つの基本的な QoS 設定について説明します。これらは、多くの場合に QoS 構成の基本部分となります。

- アクセス レイヤにおいて、PC および IP Phone からのトラフィックを分類
- レイヤ間のスイッチ間リンクで、トラフィック プライオリティ値を受け入れ
- レイヤ間のスイッチ間リンクで、各トラフィックを優先付け

各 QoS シナリオでは、ネットワーク上では IP トラフィックだけが伝送され、トラフィック プライオリティの割り当てには IP DSCP 値が使用されることを前提とします。IP サービス タイプ（ToS）またはイーサネット 802.1p サービス クラス（CoS）は直接使用しません。

IP パケットはプライオリティ値を伝送できますが、この値は、ネットワーク トポロジ内のさまざまな地点で設定できます。設計に関して推奨されるベスト プラクティスは、トラフィックの送信元にできるだけ近い位置でトラフィックを分類およびマーキングすることです。ネットワーク エッジでトラフィックのプライオリティが正しく設定されていれば、中間ホップではトラフィックを詳しく識別する必要がなくなります。代わりに、すでに設定済みのプライオリティ値に基づき、QoS ポリシーを管理できます。この方法だと、ポリシー管理が容易です。

（注）

- 特定のネットワーク トラフィック タイプとアプリケーションにパケット プライオリティを割り当てるための、適切な QoS 構成戦略を作成する必要があります。QoS に関する注意事項については、RFC 2597、RFC 2598、および米国シスコシステムズ社の発行するさまざまな QoS 設計ガイドを参照してください。
- PFC QoS をグローバルにイネーブルにし、他のすべての PFC QoS 設定をデフォルト値のままにすることはしないでください。PFC QoS をグローバルにイネーブル化すると、デフォルト値が使用されます。PFC QoS のデフォルト設定の使用には、次のような 2 つの問題があります。
  - PFC QoS をグローバルにイネーブル化すると、システム内のイーサネット ポートのデフォルトの信頼状態が untrusted となります。ポートの信頼状態が untrusted の場合は、スイッチ経由で送信されるすべてのトラフィックの QoS プライオリティが、ポートの CoS 値（デフォルトでは 0）に設定されます。つまり、すべてのトラフィックがプライオリティ 0 となります。
  - PFC QoS をグローバルにイネーブル化すると、ポートのバッファが CoS ベースのキューに割り当てられるので、プライオリティ 0 のトラフィックはバッファの一部しか使用できなくなります。つまり、プライオリティ 0 のトラフィックが使用できるバッファの量が、PFC QoS がディセーブルにされている場合よりも少なくなります。

  PFC QoS のデフォルト設定を使用することで生じるこのような問題は、ネットワーク パフォーマンスに悪影響を及ぼす可能性があります。

アクセス レイヤにおける PC および IP Phone からのトラフィックの分類

アクセス レイヤのスイッチには、100 Mbps リンクによって、IP Phone と PC がデイジーチェーン接続されています。ここでは、IP Phone からの音声トラフィックと PC からのデータ トラフィックを分類し、それぞれ異なるプライオリティを設定する方法について説明します。

アクセス レイヤ ポートで受信したトラフィックに対する QoS 分類スキームは、次のとおりです。

- 音声トラフィック：DSCP 46（最大プライオリティ）
- 音声シグナリング トラフィック：DSCP 24（ミディアム プライオリティ）
- PC SAP トラフィック：DSCP 25（ミディアム プライオリティ）
- 他のすべての PC トラフィック：DSCP 0（ベスト エフォート）

この分類戦略によって、ネットワーク上の次の 3 種類のサービス クラスをサポートできるようになります。

- ハイ プライオリティの音声トラフィック
- ミディアム プライオリティの音声シグナリング トラフィックおよび重要なアプリケーション トラフィック
- ロー プライオリティの残りのトラフィック

このモデルは、他のネットワーク環境に合わせて適宜変更できます。

PFC QoS は受信したプライオリティを信頼することも、QoS ポリシーをトラフィックに適用して、新たなプライオリティを割り当てることもできます。QoS ポリシーを設定するには、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。アクセス スイッチでは、トラフィックは ACL によって識別されます。ACL は、ポートに送られるさまざまなトラフィック タイプを区別します。識別されたトラフィックは、QoS ポリシーによって、適切な DSCP 値がマーキングされます。このように割り当てられた DSCP 値は、トラフィックがディストリビューション スイッチおよびコア スイッチに送られたときに信頼されます。

IP Phone と PC が接続されているアクセス スイッチのポートは、音声 VLAN（VLAN 110）用に設定されています。これは、IP Phone のトラフィック（サブネット 10.1.110.0/24）を PC トラフィック（サブネット 10.1.10.0/24）から区別する働きをします。音声 VLAN サブネットは、音声トラフィックを一意に識別します。UDP および TCP ポート番号は、異なるアプリケーションの識別に使用されます。

次に、アクセス ポートのアクセス制御リスト（ACL）設定を示します。

IP Phone からの音声トラフィック（VVLAN）を識別

```
ip access-list extended CLASSIFY-VOICE
    permit udp 10.1.110.0 0.0.0.255 any range 16384 32767
```

IP Phone からの音声シグナリング トラフィック（VVLAN）を識別

```
ip access-list extended CLASSIFY-VOICE-SIGNAL
    permit udp 10.1.110.0 0.0.0.255 any range 2000 2002
```

PC からの SAP トラフィック（DVLAN）を識別

```
ip access-list extended CLASSIFY-PC-SAP
    permit tcp 10.1.10.0 0.0.0.255 any range 3200 3203
    permit tcp 10.1.10.0 0.0.0.255 any eq 3600 any

ip access-list extended CLASSIFY-OTHER
    permit ip any any
```

QoS ポリシー設定の次の手順は、クラス マップを定義することです。クラス マップは、識別に使用する ACL を、実行させたい QoS アクション（この場合はマーキング）に関連付けます。クラス マップの構文は次のとおりです。

```
class-map match-all CLASSIFY-VOICE
    match access-group name CLASSIFY-VOICE
class-map match-all CLASSIFY-VOICE-SIGNAL
    match access-group name CLASSIFY-VOICE-SIGNAL
class-map match-all CLASSIFY-PC-SAP
    match access-group name CLASSIFY-PC-SAP
class-map match-all CLASSIFY-OTHER
    match access-group name CLASSIFY-OTHER
```

クラス マップを作成したら、次はポリシー マップを作成します。ポリシー マップは、各トラフィック タイプまたは各トラフィック クラスに特定の DSCP 値を設定できるように、QoS ポリシーのアクションを定義します。この例では 1 つのポリシー マップ（IPPHONE-PC）を作成します。すべてのクラス マップはこの単一ポリシー マップに含まれ、クラス マップごとに 1 つのアクションが定義されます。ポリシー マップとクラス マップの構文は次のとおりです。

```
policy-map IPPHONE-PC
   class CLASSIFY-VOICE
    set dscp ef
   class CLASSIFY-VOICE-SIGNAL
    set dscp cs3
   class CLASSIFY-PC-SAP
    set dscp 25
   class CLASSIFY-OTHER
    set dscp 0
```

この時点では、ポリシー マップ内で定義された QoS ポリシーは、まだ有効ではありません。設定の済んだポリシー マップは、トラフィックが影響を受けるように、インターフェイスに適用する必要があります。ポリシー マップを適用するには、**service-policy** コマンドを使用します。入力サービス ポリシーはポートにも VLAN インターフェイスにも適用できますが、出力サービス ポリシーは VLAN インターフェイスにしか適用できないことに注意してください（PFC3 だけが出力ポリシーをサポート）。この例では、PC と IP Phone がそれぞれ接続された各インターフェイスに、ポリシーを入力サービス ポリシーとして適用します。ここではポートベースの QoS を使用しますが、これはイーサネット ポートのデフォルトです。

```
interface FastEthernet5/1
 service-policy input IPPHONE-PC
```

これで、QoS ポリシーは正しく設定され、IP Phone と PC 両方から送信されるトラフィックを分類できるようになりました。

ポリシー マップが正しく設定されたことを確認するには、次のコマンドを入力します。

```
Router# show policy-map interface fastethernet 5/1
 FastEthernet5/1

  Service-policy input:IPPHONE-PC

    class-map:CLASSIFY-VOICE (match-all)
      Match:access-group name CLASSIFY-VOICE
      set dscp 46:

    class-map:CLASSIFY-PC-SAP (match-all)
      Match:access-group name CLASSIFY-PC-SAP
      set dscp 25:

    class-map:CLASSIFY-OTHER (match-all)
      Match:access-group name CLASSIFY-OTHER
      set dscp 0:

    class-map:CLASSIFY-VOICE-SIGNAL (match-all)
      Match:access-group name CLASSIFY-VOICE-SIGNAL
      set dscp 24:
```

ポートに正しい QoS モードが使用されているかどうかを確認するには、次のコマンドを入力します。

```
Router# show queueing interface gigabitethernet 5/1 | include Port QoS
Port QoS is enabled
```

クラス マップの設定が正しいかどうかを確認するには、次のコマンドを入力します。

```
Router# show class-map
 Class Map match-all CLASSIFY-OTHER (id 1)
   Match access-group name CLASSIFY-OTHER

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all CLASSIFY-PC-SAP (id 2)
   Match access-group name CLASSIFY-PC-SAP

 Class Map match-all CLASSIFY-VOICE-SIGNAL (id 4)
   Match access-group name CLASSIFY-VOICE-SIGNAL

 Class Map match-all CLASSIFY-VOICE (id 5)
   Match access-group name CLASSIFY-VOICE
```

各トラフィック クラスのバイト統計をモニタするには、次のコマンドを入力します。

```
Router# show mls qos ip gig 5/1
   [In] Policy map is IPPHONE-PC   [Out] Default.
 QoS Summary [IP]:     (* - shared aggregates, Mod - switch module)

           Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                       Id         Id

-------------------------------------------------------------------------------
          Gi5/1  5  In CLASSIFY-V   46    1     No  0              0  0
          Gi5/1  5  In CLASSIFY-V   24    2     No  0              0  0
          Gi5/1  5  In CLASSIFY-O    0    3     No  0              0  0
          Gi5/1  5  In CLASSIFY-P   25    4     No  0              0  0
Router#
```

スイッチ間リンクでのトラフィック プライオリティ値の受け入れ

前のセクションでは、マーキング処理の設定方法について説明しました。ここでは、アップストリーム装置がこのパケット マーキングを使用する仕組みについて説明します。

着信トラフィックのプライオリティが受け入れられるかどうかを決定する必要があります。この決定を反映させるには、ポートの信頼状態を設定します。着信トラフィックのプライオリティ設定を信頼しないように設定されたポートにトラフィックが着信すると、この着信トラフィックのプライオリティ設定は、最小プライオリティ（0）に書き換えられます。着信トラフィックのプライオリティ設定を信頼するように設定されたインターフェイスにトラフィックが着信した場合は、このトラフィックのプライオリティ設定は維持されます。

着信するプライオリティ設定を信頼するポートの例は、IP Phone や他の IP 音声装置、ビデオ装置、または、定義済みの有効なプライオリティが設定されたフレームの送信が信頼されるさまざまな装置に接続されているポートです。トラフィックが最初にネットワークに送信された時点で、適切なマーキングが完了していることがわかっている場合は、着信したプライオリティ設定を信頼するようにアップリンク インターフェイスを設定することもできます。

定義済みの有効なプライオリティを持つどのトラフィックも伝送しないワークステーションまたは他の装置に接続されたポートは、untrusted（デフォルト）として設定します。

前の例では、アクセス レイヤにおいて、音声、SAP、および他のベスト エフォート トラフィックを適切にマーキングするように QoS を設定しました。次の例では、トラフィックが他のネットワーク装置を通過するときに、これらのプライオリティ値が受け入れられるように QoS を設定します。これには、パケットの DSCP 値を信頼するようにスイッチ間リンクを設定します。

前の例では、いくつかの種類のトラフィック クラスがポートに入力されると仮定して、個々のトラフィック タイプにそれぞれ異なる QoS ポリシーを選択して適用しました。この設定は、MQC QoS ポリシー構文によって行いました。これにより、1 つのポートに着信するさまざまな種類のトラフィック クラスに対し、異なるマーキングまたは信頼アクションを個別に適用できます。

すべてのトラフィックが、信頼可能な 1 つの特定ポートに着信することがわかっている場合は（アクセス レイヤとディストリビューション レイヤ間、またはディストリビューション レイヤとコア レイヤ間のアップリンク ポートがこれに該当）、ポートを trust 状態に設定できます。ポートの trust 設定を使用すると、このポートで受信するさまざまなトラフィック タイプは区別されませんが、設定作業は大幅に単純化されます。ポートの trust 設定のコマンド構文は次のとおりです。

```
interface gigabitethernet 5/1
 mls qos trust dscp
```

受信した DSCP を信頼するようにポートを設定した場合は、スイッチから送信されるトラフィックの DSCP 値は、信頼されたポートに送られるトラフィックの DSCP 値と同じです。信頼状態を設定したあとは、次のコマンドを使用して、設定が有効になっているかどうかを確認できます。

```
Router# show queueing interface gigabitethernet 5/1 | include Trust
Trust state:trust DSCP
```

スイッチ間リンクでのトラフィックの優先付け

ここでは、スイッチが信頼値を使用してどのように動作するかを説明します。

QoS の基本原則の 1 つは、オーバーサブスクリプションが発生した場合に、プライオリティの高いトラフィックを保護することです。「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」（P.41-123）および「スイッチ間リンクでのトラフィック プライオリティ値の受け入れ」（P.41-126）で説明したマーキングおよび信頼アクションでは、オーバーサブスクリプションに対処できるようにトラフィックを準備しますが、さまざまなレベルのサービスを提供することはできません。さまざまなレベルのサービスを実現するには、ネットワーク装置が、特定のインターフェイスからトラフィックを送信するときに各トラフィックを優先付ける、高度なスケジューリング アルゴリズムを備えている必要があります。このようなスケジューリング機能は、プライオリティの高いトラフィックが、プライオリティの低いトラフィックよりも高頻度に送信されることを保証します。最終的に得られる効果は、さまざまなトラフィック クラスに対して差別化したサービスを提供できることです。

さまざまなトラフィック クラスに対して差別化したサービスを提供するうえで、次の 2 つの基本概念があります。

- トラフィックを特定のキューに割り当て
- キューのスケジューリング アルゴリズムを設定

QoS をイネーブルにすると、これらの各機能にデフォルト値が適用されます。多くのネットワークでは、ネットワーク トラフィックを区別するのに、デフォルト値で十分対応できます。それ以外のネットワークでは、必要とする結果が得られるように、デフォルト値を調整しなければならない場合もあります。これらの機能に対するデフォルト設定を大幅に変更しなければならないのは、ごくまれなケースだけです。

Catalyst 6500 シリーズ スイッチのイーサネット モジュールは、単一キュー アーキテクチャから、最大 8 つのキューからなるアーキテクチャまで、さまざまなキュー アーキテクチャをサポートします。キュー アーキテクチャは、トラフィック タイプごとに異なるサービスを提供する複数の車線をグループ化したようなもの、と考えることができます。たとえば警官は高速道路において、事故現場や犯罪現場に迅速に到着できるように、優先的に走行できる権限を持ちます。同様に、IP ネットワーク上の音声トラフィックも、このように優先的に扱われる必要があります。スイッチはキュー アーキテクチャを使用して、差別化した各サービスに対して個別のレーンを用意しています。

具体的なキュー タイプは、使用するイーサネット モジュールによって異なります。この例では、4 つの送信キューを持つモジュールを使用します。このキューは 1p3q8t と表され、次の内容を意味します。

- 1 つの完全優先キュー（1p）
- WRR スケジューリングをサポートする、3 つの標準キュー（3q）。各キューはそれぞれ 8 つの WRED スレッシュホールドを保持します（8t、ここでは説明しません）。

Catalyst 6500 シリーズ スイッチのイーサネット モジュールは入力キュー アーキテクチャも備えていますが、これはあまり使用されません。また、スイッチ ファブリック内ではあまり輻輳が発生しないと考えられるため、この例では入力キュー アーキテクチャを扱いません。

これらのキューにトラフィックを割り当てるには、プライオリティ値をキューにマッピングする必要があります。QoS では DSCP と CoS のマッピングを使用して、発信される 64 の DSCP 値を 8 つの 802.1p 値にマッピングしてから、CoS とキューのマッピングを使用して、CoS 値をキューにマッピングします。

パケットがスイッチに入力されると、QoS は設定に応じて、設定済み DSCP 値に基づきパケットを分類およびマーキングするか（「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」（P.41-123）を参照）、またはパケットの着信 DSCP 値を信頼します（「スイッチ間リンクでのトラフィック プライオリティ値の受け入れ」（P.41-126）を参照）。これらのオプションに応じて、スイッチから出力される際のパケットのプライオリティが決まります。

次に、DSCP と CoS のマッピングを表示する例を示します。

```
Router# show mls qos maps dscp-cos
   Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
Router#
```

この例では、音声トラフィックに DSCP 値 46 をマーキングします。コマンドの出力結果を使用して、DSCP 46 を CoS 5 に変換できます。また、コマンドの出力結果を使用して、マーキングされた他の DSCP 値を CoS 値に変換することもできます。

特定のネットワーク要件に応じて、このマッピング テーブルを変更してください。通常は、少量の変更が必要になるだけです。この例では変更を加えません。

キューイングを行う目的のため、この設定では発信される DSCP 値に基づいて CoS 値を導出しています。この CoS 値は、発信ポートがトランク ポートではなくアクセス ポートであっても、キューの割り当てに使用されます。ただし、発信ポートがアクセス ポートである場合は、ネットワーク上に 802.1Q VLAN タグは送信されません。

導出された各 CoS 値を、キュー構造にマッピングします。次に、CoS とキューとのデフォルト マッピングを表示する例を示します。これにより、8 つの CoS 値それぞれがマッピングされているキューを確認できます。

```
Router# show queueing interface gigabitethernet 5/1 | begin cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0
    1     2      1
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1      2
    2     2      3 4
    2     3
    2     4
    2     5
    2     6
    2     7
    2     8
    3     1      6 7
    3     2
    3     3
    3     4
    3     5
    3     6
    3     7
    3     8
    4     1      5

<output truncated>
```

音声トラフィックは完全優先キューにマッピングします。これは、1p3q8t ポートにおけるキュー 4 です。この例では、DSCP 46 音声トラフィックを CoS 5 にマッピングします。つまり、CoS 5 トラフィックを完全優先キューにマッピングする必要があります。**show queueing interface** コマンドの出力結果を使用すると、CoS 5 トラフィックが完全優先キューにマッピングされていることを確認できます。

次に、この例のすべてのトラフィック タイプに対するキュー マッピングの一覧を示します。

トラフィック タイプ	DSCP	CoS（DSCP から CoS へのマッピング）	出力キュー
音声	46	5	完全優先
音声シグナリング	24	3	キュー 2、スレッショルド 2
PC SAP	25	3	キュー 2、スレッショルド 2
その他のトラフィック	0	0	キュー 1、スレッショルド 1

スイッチ経由で送信されるトラフィックは、プライオリティに基づき、各種のキュー（つまり「車線」）に転送されます。出力キュー（この例ではインターフェイスごとに 3 つ）より CoS 値（0 ～ 7）の数が多いため、各標準キュー（完全優先ではないキュー）にはそれぞれ廃棄スレッショルドが設定されています。1 つのキューに複数の CoS 値が割り当てられている場合は、各 CoS 値に数種類の廃棄スレッショルドを割り当て、異なるプライオリティを区別することができます。スレッショルドは、特定の CoS 値を持つトラフィックが、この CoS 値を持つトラフィックの廃棄が開始される前に使用可能なキューの最大割合を指定します。この例で使用している QoS 値は 3 つだけなので（ハイ、ミディアム、ロー）、各 CoS 値を個別のキューに割り当て、デフォルトの 100% の廃棄スレッショルドを使用できます。

特定のネットワーク要件に応じて、DCSP と CoS とのマッピング、および CoS とキューとのマッピングを変更してください。通常は、少量の変更が必要になるだけです。この例では変更を加えていません。異なるマッピングが必要なネットワークの場合は、「標準送信キュー スレッショルドへの CoS 値のマッピング」（P.41-114）を参照してください。

スイッチの出力ポートでの有効なキューに、トラフィックが割り当てられる仕組みについての説明は以上です。次に学習する概念は、キューの重み値が機能する仕組みであり、これをキューのスケジューリング アルゴリズムと呼びます。

Catalyst 6500 シリーズ スイッチでは、LAN スイッチング モジュールに使用されるスケジューリング アルゴリズムは、完全優先（SP）キューイング、および重み付きラウンドロビン（WRR）キューイングです。これらのアルゴリズムは、ポート上のさまざまなキューが処理される順序（優先度）を定義します。

完全優先キューイング アルゴリズムは単純です。1 つのキューが、他のすべてのキューより優先される絶対的なプライオリティを付与されます。完全優先キューにパケットが格納されている場合は常に、スケジューラはこのキューを処理します。このため、輻輳が生じた場合であっても、このキュー内のパケットが転送される可能性は最大となり、遅延の可能性が最低限に抑えられます。完全優先キューは、音声トラフィックに対して理想的です。音声トラフィックは、ネットワーク上で最高のプライオリティを必要とし、遅延を最低限に抑える必要があるためです。また、使用する帯域幅が比較的少ないトラフィック タイプでもあるので、通常は、音声トラフィックによってポート上の有効帯域幅がすべて消費されることもありません。FTP などの広帯域幅のアプリケーションは、完全優先キューに割り当てないようにしてください。FTP トラフィックはポートで有効な帯域幅をすべて消費してしまう可能性があり、その場合、他のトラフィック クラスがリソース不足となります。

WRR アルゴリズムでは、各 WRR キューに相対的な重み値を割り当てます。3 つのキューがあり、それぞれの重み値が 100:150:200（デフォルト設定）である場合は、キュー 1 は有効帯域幅の 22% だけを使用でき、キュー 2 は 33%、キュー 3 は 45% の帯域幅を使用できます。WRR では、どのキューもこれらの配分には限定されません。キュー 2 とキュー 3 にトラフィックがまったく存在しない場合は、キュー 1 は有効帯域幅をすべて使用できます。

この例では、キュー 1 よりキュー 2 のプライオリティのほうが高く、キュー 2 よりキュー 3 のプライオリティのほうが高く設定されています。したがって、ロー プライオリティ トラフィック（IP Phone その他、PC その他）はキュー 1 に、ミディアム プライオリティ トラフィック（音声シグナリング、PC SAP）はキュー 2 にマッピングされます。

完全優先キューは、トラフィックをマッピングしたあとは設定は不要です。WRR キューにはデフォルトの帯域幅が割り当てられており、通常のネットワークではこれで十分対応できます。デフォルト値で不十分な場合は、トラフィック タイプに合わせて相対的な重み値を変更できます（「標準送信キュー間での帯域幅の割り当て」（P.41-117）を参照）。

スイッチがオーバーサブスクリプションを適切に処理しているかどうかを確認する最も良い方法は、パケット廃棄が最小限で行われているのを確認することです。パケット損失の発生を確認するには、**show queueing interface** コマンドを使用します。このコマンドでは、各キューで廃棄されたパケット数が表示されます。

ポリサーによる PC からのトラフィック量の制限

特定の装置やトラフィック クラスが予想外の量の帯域幅を消費しないようにするには、レート制限を使用すると便利です。Catalyst 6500 シリーズ スイッチのイーサネット ポートでサポートされるレート制限方法を、ポリシングと呼びます。ポリシングは PFC ハードウェアに実装され、これによるパフォーマンスへの影響はありません。ポリサーは、トラフィック レートが所定のレートを超えない限り、トラフィック フローに何の制限も加えません。設定したバースト サイズ内であれば、トラフィック バーストも許可されます。設定したレートまたはバースト サイズを超えたすべてのトラフィックは、廃棄するか、またはより低いプライオリティにマークダウンできます。ポリシングの利点は、特定のアプリケーションが消費する帯域幅の量を制御できることです。これにより、特にウイルスやワーム攻撃などの異常事態がネットワーク上で発生した場合に、ネットワーク上でのサービス品質を保証しやすくなります。

この例では、基本的なインターフェイス別の集約ポリサーを、入力方向の単一のインターフェイスに適用します。これ以外のポリシング オプションを使用しても、同じ結果を得ることができます。

ポリサーの設定は、「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」（P.41-123）で説明したマーキングの例と似ています。これは、ポリシングでも同一の ACL および MQC 構文を使用するためです。この例で使用した構文では、トラフィックを識別するクラス マップを作成してから、トラフィックのマーキング方法を指定するポリシー マップを作成しました。

ポリシングの構文もこれとよく似ているので、マーキングの例に使用した ACL をそのまま使用します。また、マーキングの例に使用したクラス マップは、**set dscp** コマンドを **police** コマンドに置き換えて修正します。この例では、CLASSIFY-OTHER クラス マップを再利用して、修正した IPPHONE-PC ポリシー マップに基づきトラフィックを識別し、一致トラフィックを最大 50 Mbps にポリシングします。同時に、このレートに従うトラフィックを引き続きマーキングします。

参考までに、「その他」のトラフィックを識別するためのクラス マップ、ACL、および **class-map** コマンドを次に示します。変更は加えません。

- ACL コマンド：

```
ip access-list extended CLASSIFY-OTHER
permit ip any any
```

- class-map コマンド：

```
class-map match-all CLASSIFY-OTHER
match access-group name CLASSIFY-OTHER
```

このポリサー設定とマーキング設定との違いは、ポリシー マップ アクションの定義です。マーキングの例では、**set dscp** コマンドを使用して、特定の DSCP 値によってトラフィックをマーキングしました。このポリシング例では、CLASSIFY-OTHER トラフィックの DSCP 値を 0 にマーキングし、このトラフィックを 50 Mbps にポリシングします。これには、**set dscp** コマンドを **police** コマンドに置き換えます。**police** コマンドでは、マーキング アクションの実行を設定できます。50 Mbps の制限を下回るすべてのトラフィックは DSCP が 0 にマーキングされ、50 Mbps スレッシュホールドを超えるすべてのトラフィックは廃棄されます。

次に、**police** コマンドを加えて修正した IPPHONE-PC ポリシー マップを示します。

```
policy-map IPPHONE-PC
class CLASSIFY-OTHER
police 50000000 1562500 conform-action set-dscp-transmit default exceed-action drop
```

police コマンドの各パラメータの機能は次のとおりです。

- 50000000 パラメータは、このトラフィック クラスで許可されたトラフィックに対し、認定情報速度（CIR）値を定義します。この例では、CIR を 50 Mbps に設定しています。
- 1562500 パラメータは、このトラフィック クラスのトラフィックの CIR バースト サイズを定義します。この例では、デフォルトの最大バースト サイズを使用します。CIR バースト サイズは、ネットワークで使用される最大の TCP ウィンドウ サイズに設定します。
- **conform action** キーワードは、トラフィック レベルが 50 Mbps レートを下回った場合に、送信された CLASSIFY-OTHER パケットに対してポリサーが実行する動作を定義します。この例では、**set-dscp-transmit default** により、このようなパケットの DSCP が 0 に設定されます。
- **exceed action** は、トラフィック レベルが 50 Mbps CIR を超過した場合に、送信された CLASSIFY-OTHER パケットに対してポリサーが実行する動作を定義します。この例では、**exceed action drop** により、このようなパケットが廃棄されます。

これは、基本的な、単一レートのインターフェイス別集約ポリサーです。Supervisor Engine 2 および Supervisor Engine 720 転送エンジンでは、デュアル レート ポリサーもサポートされるため、CIR および最大情報レート（PIR）粒度の両方を使用できます。

service-policy input コマンドを使用して、ポリシー マップを適切なインターフェイスに付加します。

```
interface FastEthernet5/1
service-policy input IPPHONE-PC
```

ポリシングの動作をモニタするには、次のコマンドを使用します。

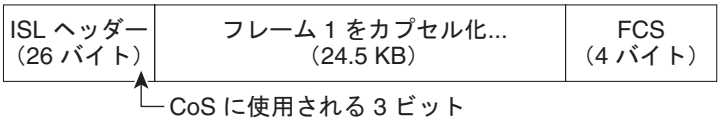
```
show policy-map interface fastethernet 5/1
show class-map
show mls qos ip fastethernet 5/1
```

PFC QoS の用語

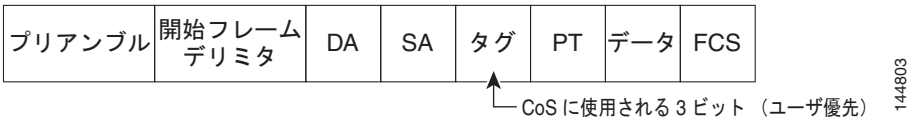
ここでは、この章で使用したいくつかの QoS 用語を定義します。

- *バッファ* - 送信中のデータを処理するための保管領域です。バッファはインターネットワーキングにおいて、ネットワーク装置間の処理速度の違いを補うために使用されます。バースト データは、より低速な処理装置によって処理されるまで、バッファに保管されることがあります。バッファは、パケット バッファと呼ばれることもあります。
- *サービス クラス（CoS）*は、ISL、802.1Q、または 802.1p ヘッダーの 3 ビットによって伝送される、レイヤ 2 QoS ラベルです。CoS 値は 0 ～ 7 の範囲の値です。

レイヤ 2 ISL フレーム

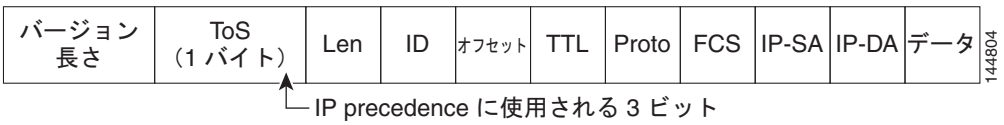


レイヤ 2 802.1Q および 802.1p フレーム



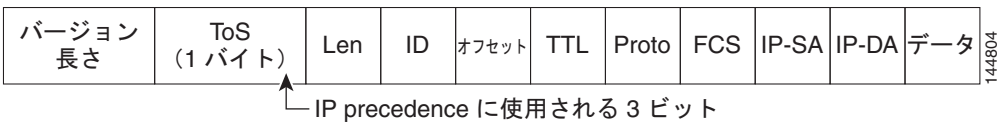
- *分類*は、QoS のマーキングを行うトラフィックを選択する処理です。
- *輻輳回避*は、プライオリティの高いレイヤ 2 CoS 値を持つレイヤ 2 フレームのために、入力 LAN ポートおよび出力 LAN ポートの容量を PFC QoS で確保しておく処理です。PFC QoS では、レイヤ 2 CoS 値ベースの廃棄スレッシュホールドによって輻輳回避を実行します。廃棄スレッシュホールドは、キュー バッファ使用率であり、この割合に達すると、特定のレイヤ 2 CoS 値を持つフレームが廃棄され、よりプライオリティの高いレイヤ 2 CoS 値を持つフレーム用に利用可能なバッファが残されます。
- *Differentiated Services Code Point*（DSCP）は、IP ヘッダー内の ToS バイトの最上位 6 ビットによって伝送される、レイヤ 3 の QoS ラベルです。DSCP 値は 0 ～ 63 の範囲の値です。

レイヤ 3 IPv4 パケット



- *フレーム* - レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームはレイヤ 3 パケットを伝送します。
- *IP Precedence* は、IP ヘッダー内の ToS バイトの最上位 3 ビットによって伝送される、レイヤ 3 の QoS ラベルです。IP precedence 値は 0 ～ 7 の範囲の値です。

レイヤ 3 IPv4 パケット



- *ラベル* - QoS ラベルを参照してください。
- *マーキング*は、レイヤ 3 の DSCP 値をパケットに設定する処理です。このマニュアルでは、マーキングの定義を拡大して、レイヤ 2 CoS 値の設定までを含めています。マーキングは、ラベルの値を変更します。
- *パケット* - レイヤ 3 でトラフィックを伝送します。
- *ポリシング* - トラフィック フローが使用する帯域幅を制限する処理です。ポリシングは、PFC および Distributed Forwarding Card（DFC）上で実行されます。ポリシングによって、トラフィックのマーキングまたは廃棄が可能になります。
- *キュー* - データを一時的にポート上に保管しておくための、バッファ領域の割り当てです。
- *QoS ラベル*—PFC QoS では、CoS、DSCP、および IP Precedence が QoS ラベルとして使用されます。QoS ラベルは、レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。
- *スケジューリング* - レイヤ 2 フレームをキューに割り当てることです。PFC QoS は、レイヤ 2 CoS 値に基づいて、フレームをキューに割り当てます。
- *シェイプド ラウンド ロビン*（SRR）は、デキューイング アルゴリズムです。
- *スレッシュホールド* - トラフィックを廃棄する上限となる、キュー容量の割合です。
- *サービス タイプ*（ToS）は、IPv4 ヘッダーに含まれる 1 バイトのフィールドであり、パケットに適用されるプライオリティ値の指定に使用されます。[ToS] フィールドは 8 ビットで構成されます。最初の 3 ビットは IP precedence 値を指定します。これは 0 ～ 7 の値であり、0 は最小のプライオリティ、7 は最大のプライオリティを示します。[ToS] フィールドは、DSCP 値の指定にも使用されます。DSCP は、ToS の最上位 6 ビットによって定義されます。DSCP 値は 0 ～ 63 の範囲で指定できます。
- *重み値* - キューに割り当てられる帯域幅の割合です。

CHAPTER 42

PFC3BXL または PFC3B モード MPLS QoS の設定

この章では、Catalyst 6500 シリーズ スイッチに PFC 3BXL または PFC3B モードの Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Quality of Service（QoS; サービス品質）を設定する方法について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- PFC3BXL または PFC3B モード MPLS QoS は、第 41 章「PFC QoS の設定」で説明する PFC QoS 機能を、MPLS トラフィックにも対応するように拡張します。
- ここでは、PFC3BXL または PFC3B モード MPLS QoS の各機能についての補足情報を説明します。この章を読むには、PFC QoS 機能を理解していることが前提となります。
- PFC3BXL または PFC3B モード MPLS QoS で使用可能なポリシングおよびマーキングはすべて、モジュラ QoS Command-Line Interface（CLI; コマンドライン インターフェイス）から管理します。Modular QoS CLI（MQC; モジュラ QoS CLI）は、トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定し、トラフィック ポリシーをインターフェイスに付加できるコマンドライン インターフェイスです。モジュラ QoS CLI の詳細については、次の URL にある『*Cisco IOS Quality of Service Solutions Configuration Guide*』*Release 12.2* を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html

この章で説明する内容は、次のとおりです。

用語

ここでは、MPLS QoS 用語の一部を定義します。

- *Class of Service*（CoS; サービス クラス）は、Inter-Switch Link（ISL; スイッチ間リンク）ヘッダーまたは 802.1Q ヘッダー内の 3 ビットを指します。CoS は、スイッチド ネットワークを通過するイーサネット フレームのプライオリティを示すために使用されます。802.1Q ヘッダーの CoS ビットは、一般的に 802.1p ビットと呼びます。レイヤ 2 およびレイヤ 3 ドメインの両方を通過するパケットの QoS を維持するには、Type of Service（ToS; サービス タイプ）値と CoS 値を相互にマッピングします。
- *分類*は、QoS のマーキングを行うトラフィックを選択する処理です。
- *Differentiated Services Code Point*（DSCP）は、IP ヘッダーの ToS バイトの最初の 6 ビットです。DSCP は IP パケット内にのみ存在します。
- *E-LSP* は、ノードが MPLS ヘッダーの experimental（EXP）ビットのみに基づき、MPLS パケットに対する QoS 処理を予測する Label Switched Path（LSP; ラベル スイッチド パス）です。QoS 処理は EXP（クラス優先度および廃棄優先度の両方）から予測されるので、複数のトラフィック クラスを 1 つの LSP に多重化できます（同じラベルを使用）。EXP フィールドは 3 ビット フィールドなので、単一 LSP では最大 8 つのトラフィック クラスをサポートできます。最大クラス数は、コントロール プレーン トラフィックのいくつかの値を予約したあと、または一部のクラス値に関連付けられた廃棄優先度がある場合は、これより少なくなります。
- *EXP ビット*は、ノードがパケットに行う必要がある QoS 処理（Per-Hop Behavior（PHB））を定義します。これは、IP ネットワークの Differentiated Service（DiffServ; 差別化したサービス）Code Point（DSCP）に相当します。DSCP はクラスおよび廃棄優先度を定義します。EXP ビットは通常、IP DSCP で符号化されたすべての情報の伝送に使用されます。ただし、廃棄優先度を符号化するためだけに EXP ビットを使用する場合もあります。
- *フレーム*は、レイヤ 2 のトラフィックを伝送します。レイヤ 2 フレームはレイヤ 3 パケットを伝送します。
- *IP precedence* は、IP ヘッダーの ToS バイト内の最上位 3 ビットです。
- *QoS タグ*は、レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。レイヤ 2 CoS ラベルの値の範囲は 0 ～ 7 であり、数値が高いほどプライオリティは高くなります。レイヤ 3 IP precedence ラベルの値の範囲も 0 ～ 7 であり、数値が高いほどプライオリティは高くなります。IP precedence 値は、1 バイトの ToS バイト内の最上位 3 ビットによって定義されます。レイヤ 3 の DSCP ラベルの値は 0 ～ 63 です。DSCP 値は、1 バイトの IP ToS フィールド内の最上位 6 ビットによって定義されます。
- *Label Edge Router*（LER; ラベル エッジ ルータ）は、パケットにラベルをインポーズまたはディスポーズする装置です。Provider Edge（PE; プロバイダー エッジ）ルータともいいます。
- *Label Switching Router*（LSR; ラベル スイッチング ルータ）は、パケットのラベルに基づきトラフィックを転送する装置です。Provider（P）ルータともいいます。
- *マーキング*は、パケットのレイヤ 3 DSCP 値を設定する処理です。また、輻輳の発生中に必要なプライオリティを各パケットに設定するため、各パケットに対して MPLS EXP フィールドのさまざまな値を選択する処理でもあります。
- *パケット*は、レイヤ 3 でトラフィックを伝送します。

- *ポリシング*- トラフィック フローが使用する帯域幅を制限する処理です。ポリシングによって、トラフィックのマーキングまたは廃棄が可能になります。

PFC3BXL または PFC3B モード MPLS QoS の機能

ネットワークに QoS を導入することで、選択したネットワーク トラフィックに提供するサービスを向上させることができます。ここでは、次の PFC3BXL または PFC3B モード MPLS QoS 機能について説明します。これらは MPLS ネットワークでサポートされます。

MPLS EXP フィールド

MPLS EXP フィールド値の設定により、自身のネットワーク上で送信される IP パケット内の IP precedence フィールド値を変更させたくないという、サービス プロバイダーの要件を満たすことができます。

MPLS EXP フィールドに対して異なる値を選択することで、輻輳期間に必要とするプライオリティを各パケットに設定できるように、パケットをマーキングできます。

デフォルトでは、インポジション中に、IP precedence 値が MPLS EXP フィールドにコピーされます。MPLS EXP ビットは、PFC3BXL または PFC3B モード MPLS QoS ポリシーによってマーキングできます。

信頼性

受信したレイヤ 3 MPLS パケットに対し、PFC3BXL または PFC3B は通常、受信した最上位ラベルの EXP 値を信頼します。MPLS パケットは、次のいずれの影響も受けません。

- インターフェイスの信頼状態
- ポートの CoS 値
- policy-map **trust** コマンド

PFC3BXL または PFC3B は受信したレイヤ 2 MPLS パケットに対し、受信した最上位ラベルの EXP 値を信頼するか、または CoS および出力キューイングの目的で、MPLS パケットにポートの信頼状態またはポリシーの信頼状態を適用します。

分類

分類とは、マーキングするトラフィックを選択する処理です。分類では、トラフィックは複数のプライオリティ レベルまたは CoS に分割されます。トラフィック分類は、クラスベースの QoS プロビジョニングの主要コンポーネントです。PFC3BXL または PFC3B は、受信した MPLS パケット（ポリシーのインストール後）の最上位ラベルの EXP ビットに基づき、分類を行います。詳細については、「MPLS パケット分類のためのクラス マップの設定」（P.42-22）を参照してください。

ポリシングおよびマーキング

ポリシングでは、設定されたレートを超えたトラフィックは廃棄されるか、またはより高い廃棄優先度にマークダウンされます。マーキングは、差別化すべきパケット フローを識別する手段です。パケット マーキングにより、使用するネットワークを複数のプライオリティ レベル、またはサービス クラスに分割できます。

実装可能な PFC3BXL または PFC3B モード MPLS QoS ポリシングおよびマーキング機能は、受信したトラフィック タイプ、およびトラフィックに適用される転送処理によって決まります。詳細については、「ポリシー マップの設定」（P.42-25）を参照してください。

IP ToS の保持

PFC3BXL または PFC3B では、インポジション、スワップ、ディスポジションを含むすべての MPLS 操作中に、IP ToS が自動的に保持されます。IP ToS を保存するためのコマンドを入力する必要はありません。

EXP 変換

最大 8 個の 出力 EXP 変換マップを設定して、内部 EXP 値が出力 EXP 値として書き込まれる前に、内部 EXP 値を変換できます。出力 EXP 変換マップは、次のインターフェイス タイプに付加できます。

- OSM（オプティカル サービス モジュール）ポート
- LAN または OSM ポート サブインターフェイス
- レイヤ 3 VLAN インターフェイス
- レイヤ 3 LAN ポート

EXP 変換 マップは、次のインターフェイス タイプには付加できません。

- レイヤ 2 LAN ポート（スイッチポート）
- FlexWAN ポートまたはサブインターフェイス

設定の詳細については、「PFC3BXL または PFC3B モード MPLS QoS の出力 EXP 変換の設定」（P.42-31）を参照してください。

MPLS DiffServ トンネリング モード

PFC3BXL または PFC3B では、MPLS DiffServ トンネリング モードが使用されます。トンネリングにより、ネットワークの端から端まで、QoS の透過性を提供できます。詳細については、「MPLS DiffServ トンネリング モード」（P.42-34）を参照してください。

PFC3BXL または PFC3B モード MPLS QoS の概要

ネットワーク管理者は PFC3BXL または PFC3B モード MPLS QoS を使用することで、差別化したサービス タイプを MPLS ネットワーク上で提供できます。差別化したサービスでは、送信するパケットごとに、QoS によって各パケットに指定されたサービスを提供することで、幅広い要件を満たします。サービスはさまざまな方法で指定できます。たとえば、IP パケットでは IP precedence ビットの設定を使用します。

IP precedence フィールドでの QoS の指定

あるサイトから別のサイトへ IP パケットを送信する際、IP precedence フィールド（IP パケット ヘッダーに含まれる DSCP フィールドの先頭 3 ビット）は QoS を指定します。IP precedence マーキングに基づき、この QoS に対して設定された処理がパケットに適用されます。サービス プロバイダー ネットワークが MPLS ネットワークである場合、IP precedence ビットはネットワーク エッジで MPLS EXP フィールドにコピーされます。ただし、サービス プロバイダーが MPLS パケットの QoS を、提供するサービスに基づき別の値に設定したい場合もあります。

この場合、サービス プロバイダーは MPLS EXP フィールドを設定できます。IP ヘッダーは、常にカスタマーが利用できます。IP パケットが MPLS ネットワークを通じて送信されても、IP パケットの QoS は変更されません。

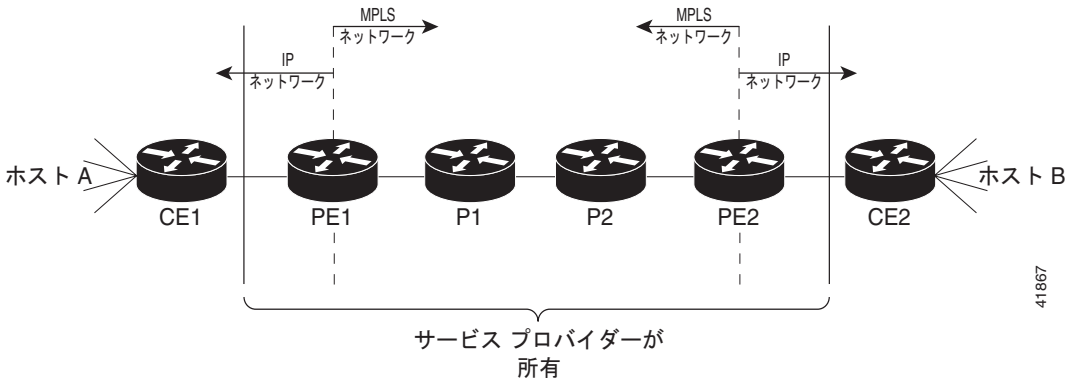
詳細については、「MPLS DiffServ トンネリング モード」（P.42-34）を参照してください。

PFC3BXL または PFC3B モード MPLS QoS

ここでは、PFC3BXL または PFC3B モード MPLS QoS の動作方法について説明します。

図 42-1 に、カスタマー ネットワークの 2 つのサイトを接続する、サービス プロバイダーの MPLS ネットワークを示します。

図 42-1　カスタマー IP ネットワークの 2 つのサイトを接続する MPLS ネットワーク



ネットワークは双方向ですが、このマニュアルではパケットは左から右へ移動することにします。

図 42-1 の記号には、次の意味があります。

- CE1 - カスタマー装置 1
- PE1 - サービス プロバイダーの入力 LER
- P1 - サービス プロバイダーのネットワーク コア内の Label Switch Router（LSR; ラベル スイッチ ルータ）
- P2 - サービス プロバイダーのネットワーク コア内の LSR
- PE2 - サービス プロバイダーの出力 LER
- CE2 - カスタマー装置 2

（注） PE1 および PE2 は、MPLS ネットワークと IP ネットワークの境界に存在します。

次に、MPLS ネットワークでの LER および LSR の動作について説明します。

- 「MPLS ネットワークの入力エッジでの LER」（P.42-6）
- 「MPLS ネットワーク コアの LSR」（P.42-7）
- 「MPLS ネットワークの出力エッジでの LER」（P.42-8）

（注） 入力インターフェイスでの QoS 機能は、入力インターフェイスが LAN ポート、OSM の WAN ポート、FlexWAN または拡張 FlexWAN モジュールのポート アダプタのどれであるかによって異なります。ここでは LAN ポートについて説明します。OSM の詳細については、『*OSM Configuration Note*』12.2SX を参照してください。FlexWAN または拡張 FlexWAN モジュールの詳細については『*FlexWAN and Enhanced FlexWAN Installation and Configuration Note*』を参照してください。

MPLS ネットワークの入力エッジでの LER

（注） 着信ラベルには集約または非集約の 2 つのタイプがあります。集約ラベルの場合は、到着した MPLS または MPLS VPN（仮想施設網）パケットは、IP 検索によって次のホップおよび発信インターフェイスを見つけ出すことでスイッチングされる必要があることを示します。非集約ラベルの場合、パケットに IP ネクストホップ情報が格納されます。

ここでは、MPLS ネットワークの入力側または出力側で、エッジ LER がどのように動作するかを説明します。

MPLS ネットワークの入力側では、LER は次のようにパケットを処理します。

1. レイヤ 2 またはレイヤ 3 トラフィックは、MPLS ネットワークのエッジであるエッジ LER（PE1）に入ります。
2. PFC3BXL または PFC3B は入力インターフェイスからトラフィックを受信し、802.1p ビットまたは IP ToS ビットを使用して EXP ビットを決定して、分類、マーキング、ポリシングを実行します。着信 IP パケットを分類するため、入力サービス ポリシーでは Access Control List（ACL; アクセス制御リスト）も使用されます。
3. PFC3BXL または PFC3B は着信 IP パケットごとに IP アドレスの検索を行い、ネクストホップ ルータを決定します。
4. 適切なラベルがパケットにプッシュ（インポジション）され、QoS の決定に基づく EXP 値がラベル ヘッダーの MPLS EXP フィールドにコピーされます。

5. PFC3BXL または PFC3B は、ラベルの付けられたパケットを、適切な出力インターフェイスに転送して処理します。
6. PFC3BXL または PFC3B は、802.1p ビットまたは IP ToS ビットも出力インターフェイスに転送します。
7. 出力インターフェイスでは、ラベル付きパケットはマーキングまたはポリシングのため、クラスによって区別されます。LAN インターフェイスの場合、出力分類は MPLS ではなく、IP に基づいて行われます。
8. ラベル付きパケット（EXP によってマーキング）は、コア MPLS ネットワークに送信されます。

MPLS ネットワーク コアの LSR

ここでは、MPLS ネットワーク コアで使用される LSR がパケットを処理する仕組みについて説明します。

1. エッジ LER（または他のコア装置）から送られた MPLS ラベル付きパケット（および 802.1p ビットまたは IP ToS ビット）は、コア LSR に着信します。
2. PFC3BXL または PFC3B は、入力インターフェイスからトラフィックを受信し、EXP ビットを使用して分類、マーキング、ポリシングを実行します。
3. PFC3BXL または PFC3B は、テーブルを検索してネクストホップ LSR を決定します。
4. 適切なラベルがパケットに添付（スワップ）され、MPLS EXP ビットがラベル ヘッダーにコピーされます。
5. PFC3BXL または PFC3B は、ラベルの付けられたパケットを、適切な出力インターフェイスに転送して処理します。
6. PFC3BXL または PFC3B は、802.1p ビットまたは IP ToS ビットも出力インターフェイスに転送します。
7. 発信パケットはマーキングまたはポリシングのため、MPLS EXP フィールドによって区別されます。
8. ラベルが添付された（EXP マークの付いた）パケットは、コア MPLS ネットワーク内の別の LSR、または出力エッジの LER に送信されます。

（注） これらは MPLS パケットなので、サービス プロバイダーのネットワーク内には、使用するキューイング アルゴリズム用の IP precedence フィールドが存在しません。パケットは、プロバイダー エッジ ルータである PE2 に着信するまでは MPLS パケットのままです。

MPLS ネットワークの出力エッジでの LER

MPLS ネットワークの出力側では、LER は次のようにパケットを処理します。

1. コア LSR からの MPLS ラベル付きパケット（および 802.1p ビットまたは IP ToS ビット）は、MPLS ネットワーク バックボーンからの出力 LER（PE2）に着信します。
2. PFC3BXL または PFC3B は、MPLS ラベルをパケットからポップ（ディスポジション）します。集約ラベルは、元の 802.1p ビットまたは IP ToS ビットを使用して分類されます。非集約ラベルは、デフォルトでは EXP 値で分類されます。
3. 集約ラベルの場合、PFC3BXL または PFC3B は IP アドレスの検索を行い、パケットの宛先を決定します。次に、PFC3BXL または PFC3B はパケット処理のため、パケットを適切な出力インターフェイスに転送します。非集約ラベルの場合、転送はラベルに基づいて行われます。デフォルトでは、非集約ラベルは出力 PE ルータではなく、直前のホップ LSR ルータ（最後の前）でポップされます。
4. PFC3BXL または PFC3B は、802.1p ビットまたは IP ToS ビットも出力インターフェイスに転送します。
5. パケットは 802.1p ビットまたは IP ToS ビットに従って区別され、適宜処理されます。

（注）　MPLS EXP ビットを使用すると、MPLS パケットに QoS を指定できます。IP precedence ビットおよび DSCP ビットを使用すると、IP パケットに QoS を指定できます。

PFC3BXL または PFC3B モード MPLS QoS の概要

PFC3BXL または PFC3B モード MPLS QoS は、IP QoS をサポートします。MPLS パケットでは、PFC3BXL または PFC3B が非 MPLS の QoS マーキングおよび ポリシングを適用できるように、EXP 値が内部 DSCP にマッピングされます。

入力および出力ポリシーでは、PFC3BXL または PFC3B モード MPLS QoS マーキングおよびポリシングの決定が、入力 PFC3BXL または PFC3B でインターフェイス単位で行われます。入力インターフェイスは物理ポート、サブインターフェイス、または VLAN です。

QoS ポリシー ACL は、入力および出力検索ごとに個別に QoS Ternary Content Addressable Memory（TCAM）でプログラムされます。TCAM 出力検索は、IP 転送テーブル（Forwarding Information Base（FIB; 転送情報ベース））の検索と NetFlow 検索が完了したあとに実行されます。

各 QoS TCAM 検索の結果、ポリサー設定およびポリシング カウンタを保持する RAM にインデックスが作成されます。その他の RAM 領域には、マイクロフロー ポリサー設定が含まれます。マイクロフロー ポリシング カウンタは、QoS ACL と一致する各 NetFlow エントリで維持されます。

入力および出力集約の結果とマイクロフロー ポリシングの組み合わせにより、最終的なポリシングが決定されます。不適合パケットは、廃棄するか、または DSCP でマークダウンできます。

次に、PFC3BXL または PFC3B モード MPLS QoS の以下の機能について説明します。

- 「EoMPLS エッジの LER」（P.42-9）
- 「IP エッジでの LER（MPLS、MPLS VPN）」（P.42-10）
- 「MPLS コアでの LSR」（P.42-14）

（注）　各セクションでは、LAN ポート、OSM ポート、および FlexWAN ポートの QoS 機能を扱います。各機能の動作の詳細については、適切なマニュアルを参照してください。

EoMPLS エッジの LER

ここでは、LER 上で機能する Ethernet over MPLS（EoMPLS）QoS 機能の概要について説明します。EoMPLS QoS のサポートは、IP/MPLS-QoS に類似しています。

- EoMPLS では、ポートが信頼できない場合、CoS の信頼状態は VC タイプ 5（ポート モード）ではなく、VC タイプ 4（VLAN モード）に自動的に設定されます。これは、トンネル上での 802.1Q CoS 保存機能に似ています。
- トンネルの入口で受信されたパケットは、VC タイプ 4 以外の EoMPLS インターフェイスでは信頼不可として処理されます。VC タイプ 4 インターフェイスでは、入力ポートには trust CoS が自動設定され、ポリシー マーキングは適用されません。
- 入力ポートが信頼可能として設定されている場合は、EoMPLS インターフェイス上で受信されるパケットは、元の IP パケット ヘッダーの QoS ポリシーによってマーキングされません。IP ポリシーによるマーキングは、信頼できないポートに対して行われます。
- 802.1Q ヘッダーを介して 802.1p CoS を利用できる場合、これは入力時から出力時まで保存されます。
- 1p タグが EoMPLS ヘッダー（VC タイプ 4）によってトンネリングされた場合、トンネルの出口から出力されたあと、キューイングは保存された 802.1p CoS に基づいて行われます。それ以外の場合、キューイングは QoS の決定から得られた CoS に基づいて行われます。

Ethernet/MPLS

Ethernet/MPLS では、入力インターフェイス、PFC3BXL または PFC3B モード MPLS QoS、出力インターフェイスの各機能は、IP/MPLS における該当機能と類似しています。詳細については、次のセクションを参照してください。

- 「IP/MPLS の分類」（P.42-10）
- 「IP/MPLS PFC3BXL または PFC3B モード MPLS QoS の分類」（P.42-11）
- 「IP/MPLS 入力ポートでの分類」（P.42-11）
- 「IP/MPLS 出力ポートでの分類」（P.42-11）

MPLS/Ethernet

MPLS/Ethernet の場合、入力インターフェイス、PFC3BXL または PFC3B モード MPLS QoS、出力インターフェイスの各機能は、MPLS/IP における該当機能と類似しています。ただし、EoMPLS カプセル開放では、出力 IP ポリシーを適用できません（パケットは MPLS としてのみ分類できます）。詳細については、次のセクションを参照してください。

- 「MPLS/IP の分類」（P.42-11）
- 「MPLS/IP PFC3BXL または PFC3B モード MPLS QoS の分類」（P.42-12）
- 「MPLS/IP 入力ポートでの分類」（P.42-12）
- 「MPLS/IP 出力ポートでの分類」（P.42-13）。

IP エッジでの LER（MPLS、MPLS VPN）

ここでは、MPLS および MPLS VPN ネットワークの入力（CE/PE）エッジおよび出力（PE/CE）エッジでの、LER の QoS 機能について説明します。MPLS および MPLS VPN は、いずれも一般的な MPLS QoS 機能をサポートします。追加された MPLS VPN 固有の QoS 情報については、「MPLS VPN」（P.42-13）を参照してください。

IP/MPLS

PFC3BXL または PFC3B は、IP/MPLS エッジで次の MPLS QoS 機能を提供します。

- **mls qos trust** コマンドまたは **policy-map** コマンドに基づいた EXP 値の割り当て
- ポリシーを使用した EXP 値のマーキング
- ポリシーを使用したトラフィックのポリシング

ここでは、IP/MPLS エッジで PFC3BXL または PFC3B がサポートする MPLS QoS 分類に関する情報を提供します。さらに、入力および出力インターフェイス モジュールによる機能についても説明します。

IP/MPLS の分類

IP トラフィックに対し、PFC3BXL または PFC3B の入力ポリシーと出力ポリシーは、IP precedence、IP DSCP、IP ACL の **match** コマンドを使用して、受信した元の IP 上のトラフィックを分類します。出力ポリシーでは、インポーズした EXP 値、または入力ポリシーによるマーキングに基づくトラフィックの分類は行われません。

PFC3BXL または PFC3B は、ポート信頼ポリシーと QoS ポリシーを適用したあと、内部 DSCP を割り当てます。次に、PFC3BXL または PFC3B はインポーズしたラベルの内部 DSCP/EXP グローバル マップに基づき、EXP 値を割り当てます。複数のラベルがインポーズされている場合でも、各ラベルの EXP 値は同じ値です。MPLS ラベルがインポーズされている場合、PFC3BXL または PFC3B は元の IP ToS を保持します。

PFC3BXL または PFC3B は、内部 DSCP/CoS グローバル マップに基づき、出力 CoS を割り当てます。デフォルトの内部 DSCP/EXP と内部 DSCP/CoS マップに整合性がある場合は、出力 CoS はインポーズされた EXP と同じ値になります。

入力ポートが IP/IP トラフィックと IP/MPLS トラフィックの両方を受信する場合、分類を使用して 2 つのトラフィック タイプを分ける必要があります。たとえば、IP/IP トラフィックと IP/MPLS トラフィックの宛先アドレス範囲が異なる場合は、宛先アドレスに基づきトラフィックを分類します。次に、IP ToS ポリシーを IP/IP トラフィックに適用し、（インポーズされた MPLS ヘッダーに EXP 値をマーキングまたは設定する）適切なポリシーを IP/MPLS トラフィックに適用します。次の 2 つの例を参照してください。

- IP ToS をマーキングする PFC3BXL または PFC3B ポリシーによって内部 DSCP を設定 - このポリシーがトラフィックすべてに適用された場合は、IP/IP トラフィックでは出力ポートによって、出力パケット内の CoS（内部 DSCP から作成）が IP ToS バイトに書き換えられます。IP/MPLS トラフィックでは、PFC3BXL または PFC3B は、内部 DSCP をインポーズされた EXP 値にマッピングします。
- MPLS EXP をマーキングする PFC3BXL または PFC3B ポリシーによって内部 DSCP を設定 - このポリシーがトラフィックすべてに適用された場合は、IP/IP トラフィックでは出力ポートによって、入力 IP ポリシー（または trust）に従って IP ToS が書き換えられます。CoS は ToS からマッピングされます。IP/MPLS トラフィックでは、PFC3BXL または PFC3B は、内部 DSCP をインポーズされた EXP 値にマッピングします。

IP/MPLS PFC3BXL または PFC3B モード MPLS QoS の分類

PFC3BXL または PFC3B モード MPLS QoS は、PE1 への入力時に以下をサポートします。

- IP precedence 値または DSCP 値に基づく照合、またはアクセス グループによるフィルタリング
- **set mpls experimental imposition** および **police** コマンド

PFC3BXL または PFC3B モード MPLS QoS は、PE1 からの出力時に **mpls experimental topmost** コマンドをサポートします。

IP/MPLS 入力ポートでの分類

IP/MPLS の分類は、IP/IP と同じです。LAN ポート分類は、受信したレイヤ 2 802.1Q CoS 値に基づいて行われます。OSM および FlexWAN インターフェイスは、受信したレイヤ 3 IP ヘッダーの情報に基づきトラフィックを分類します。

IP/MPLS 出力ポートでの分類

LAN ポートでの分類は、受信した EXP 値に基づいて行われ、この値から出力 CoS 値がマッピングされます。

OSM および FlexWAN インターフェイスによるトラフィックの分類は、**match mpls experimental** コマンドを使用して、出力 CoS を EXP 値のプロキシとして一致させた場合に行われます。**match mpls experimental** コマンドは、最上位ラベルの EXP 値では一致しません。

出力ポートがトランクの場合は、LAN ポートと OSM GE-WAN ポートは、出力 CoS を出力 802.1Q フィールドにコピーします。

MPLS/IP

PFC3BXL または PFC3B モード MPLS QoS は、MPLS/IP エッジで次の機能をサポートします。

- MPLS ドメインからの出力時に、出力インターフェイスごとに EXP 値を IP DSCP に伝播するオプション
- MPLS/IP 出力インターフェイスで IP サービス ポリシーを使用するオプション

ここでは、MPLS/IP MPLS QoS 分類に関する情報を提供します。さらに、入力および出力モジュールによる機能についても説明します。

MPLS/IP の分類

PFC3BXL または PFC3B は QoS の結果に基づき、内部 DSCP（PFC3BXL または PFC3B が各フレームに割り当てる内部プライオリティ）を割り当てます。QoS の結果は次の影響を受けます。

- trust EXP のデフォルト値
- ラベル タイプ（プレフィクス単位または集約）
- VPN 数
- 明示的な NULL の使用
- QoS ポリシー

分類モードには次の 3 つがあります。

- 通常の MPLS 分類 - 非集約ラベルでは、MPLS の再循環が存在しない場合、PFC3BXL または PFC3B は MPLS EXP 入力または出力ポリシーに基づいてパケットを分類します。PFC3BXL は EXP/DSCP/CoS マッピングから作成した CoS に基づき、パケットをキューイングします。基本 IP DSCP は、出力時のカプセル開放後に保存されるか、または（EXP/DSCP マップに基づき）EXP によって上書きされます。
- VPN CAM 内の集約レベルの一致による IP 分類 - PFC3BXL または PFC3B は、次のいずれかを行います。
  - 基本の IP ToS を保存
  - EXP/DSCP グローバル マップから得られた値によって IP ToS を書き換え
  - IP ToS を、出力 IP ポリシーから得られた任意の値に変更

  すべての場合、出力キューイングは DSCP/CoS マップからの最終 IP ToS に基づいています。
- VPN CAM に集約ラベルが存在しない場合の IP 分類 - 再循環後、PFC3BXL または PFC3B は、MPLS カプセル開放隣接で指定された入力予約済み VLAN に基づき、MPLS/IP パケットを通常の IP/IP パケットから区別します。予約済み VLAN は、VPN および非 VPN において VPN Routing/Forwarding instance（VRF; VPN ルーティング/転送インスタンス）単位で割り当てられます。再循環後の入力 ToS は元の IP ToS 値となるか、または元の EXP 値から作成できます。出力 IP ポリシーは、入力 ToS を任意の値に上書きできます。

（注）　再循環の詳細については、「再循環」（P.24-5）を参照してください。

PE/CE 入力時の着信 MPLS パケットの場合は、PFC3BXL または PFC3B は MPLS 分類のみをサポートします。入力 IP ポリシーはサポートされません。MPLS コアからの PE/CE トラフィックは、出力時に IP として分類またはポリシングされます。

MPLS/IP PFC3BXL または PFC3B モード MPLS QoS の分類

PFC3BXL または PFC3B モード MPLS QoS は、PE2 への入力時に、EXP 値の照合および **police** コマンドをサポートします。

PFC3BXL または PFC3B モード MPLS QoS は、PE2 からの出力時に、IP precedence または DSCP 値の照合、またはアクセス グループと **police** コマンドによるフィルタリングをサポートします。

MPLS/IP 入力ポートでの分類

LAN ポートでの分類は、EXP 値に基づいて行われます。OSM および FlexWAN インターフェイスは、**match mpls experimental** コマンドを使用してトラフィックを分類します。**match mpls experimental** コマンドは、受信した最上位ラベルの EXP 値で一致します。

MPLS/IP 出力ポートでの分類

（注）　出力分類キューイングは、LAN ポートと WAN ポートでは異なります。

MPLS/IP の分類は、IP/IP の分類と同じです。

LAN インターフェイスの分類は、出力 CoS に基づいて行われます。OSM および WAN インターフェイスは、送信した IP ヘッダーの情報に基づいてトラフィックを分類します。

（注）　出力ポリシーでは PFC3BXL または PFC3B QoS 機能、あるいは OSM QoS 機能を使用できますが、同一の出力ポリシー内で両方の機能を使用することはできません。

出力ポートがトランク ポートの場合、LAN ポートおよび OSM GE-WAN ポートは、出力 CoS を出力 802.1Q フィールドにコピーします。

（注）　MPLS/IP では、出力インターフェイスで MPLS IP（またはタグ IP）がイネーブルにされている場合、出力 IP ACL または QoS は出力インターフェイスで無効となります。例外は、VPN CAM 内で一致した場合です。この場合、パケットは出口で IP として分類されます。

MPLS VPN

ここで説明する情報は、MPLS VPN ネットワークにも該当します。

MPLS VPN では、次の PE MPLS QoS 機能がサポートされます。

- VPN サブインターフェイスを通る CE/PE IP トラフィックの分類、ポリシング、またはマーキング
- VPN 単位の QoS（ポート単位、VLAN 単位、またはサブインターフェイス単位）

Customer Edge（CE; カスタマー エッジ）/PE トラフィックの場合、または CE/PE/CE トラフィックの場合は、サブインターフェイスのサポートにより、IP QoS 入力ポリシーまたは出力ポリシーをサブインターフェイスおよび物理インターフェイスに適用できます。VPN 単位ポリシングは、CE 側で指定された VPN に関連付けられた特定のインターフェイスまたはサブインターフェイスにも提供されます。

複数のインターフェイスが同じ VPN に属する状況では、同じ PFC3BXL または PFC3B に関連付けられた類似インターフェイスすべてに対し、入力または出力サービス ポリシー内で同一の共有ポリサーを使用することで、VPN 単位のポリシング集約を実行できます。

集約 VPN ラベルでは、再循環の場合の EXP 伝播機能はサポートされないことがあります。最終パケットが使用する出力インターフェイスが、MPLS 隣接に通知されないためです。

（注）　再循環の詳細については、「再循環」（P.24-5）を参照してください。

VPN のインターフェイスすべてで EXP 伝播機能がイネーブルの場合、PFC3BXL または PFC3B は EXP 値を伝播します。

次の PE MPLS QoS 機能がサポートされます。

- IP パケットに対する一般的な MPLS QoS 機能
- VPN サブインターフェイスを通る CE/PE IP トラフィックの分類、ポリシング、またはマーキング
- VPN 単位の QoS（ポート単位、VLAN 単位、またはサブインターフェイス単位）

MPLS コアでの LSR

ここでは、MPLS および MPLS VPN ネットワーク コアにおける LSR（MPLS/MPLS）の MPLS QoS 機能について説明します。Carrier Supporting Carrier（CSC）QoS 機能における入力機能、出力インターフェイス、PFC3BXL または PFC3B 機能は、次に説明する MPLS/MPLS で使用される各機能と類似しています。CSC と MPLS/MPLS との違いは、CSC ではラベルを MPLS ドメイン内にインポーズできることです。

MPLS/MPLS

MPLS コアにおいて、PFC3BXL または PFC3B モード MPLS QoS は次の機能をサポートします。

- サービス ポリシーに基づく EXP 単位のポリシング
- 最上位 EXP 入力値を、新たにインポーズされた EXP 値にコピー
- MPLS ドメイン間の出力境界上での、任意の EXP 変換（2 つの近接 MPLS ドメイン間で、インターフェイス エッジ上での EXP 値の変更）
- 特定の EXP 値に対する個別のラベル フローに基づくマイクロフロー ポリシング
- マルチラベル スタックから最上位ラベルをポップする際の、最上位 EXP 値の基本 EXP 値への任意伝播

ここでは、MPLS/MPLS における PFC3BXL または PFC3B モード MPLS QoS 分類に関する情報を提供します。さらに、入力および出力モジュールの機能についての情報も提供します。

MPLS/MPLS の分類

受信 MPLS パケットの場合、PFC3BXL または PFC3B はポートの信頼状態、入力 CoS、およびすべての policy-map **trust** コマンドを無視します。代わりに、PFC3BXL または PFC3B は最上位ラベルの EXP 値を信頼します。

（注）　**match mpls experimental** コマンドを入力すると、MPLS トラフィックに対する PFC3BXL または PFC3B モード MPLS QoS 入力ポリシーおよび出力ポリシーは、受信した最上位ラベルの EXP 値に基づきトラフィックを分類します。

PFC3BXL または PFC3B モード MPLS QoS は、EXP/DSCP グローバル マップを使用して、EXP 値を内部 DSCP にマッピングします。PFC3BXL または PFC3B の次の動作は、ラベルのスワップ、新規ラベルのインポーズ、またはラベルのポップのどれを行うかによって異なります。

- ラベルのスワップ - ラベルをスワップする場合、PFC3BXL または PFC3B は受信した最上位ラベルの EXP 値を保持し、発信する最上位ラベルの EXP 値にこの値をコピーします。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。DSCP グローバル マップに整合性がある場合、出力 CoS は発信する最上位ラベルの EXP に基づきます。

  PFC3BXL または PFC3B は、**police** コマンドの **exceed** および **violate** アクションを使用して、不適合トラフィックをマークダウンできます。適合するトラフィックはマーキングされないので、**conform** アクションを送信する必要があります。**set** コマンドは使用できません。PFC3BXL または PFC3B はマークダウンを行う際、内部 DSCP マークダウン マップのインデックスとして内部 DSCP を使用します。PFC3BXL または PFC3B は、内部 DSCP/EXP グローバル マップを使用して、内部 DSCP マークダウンの結果を EXP 値にマッピングします。PFC3BXL または PFC3B は新しい EXP 値を発信最上位ラベルに書き換え、新しい EXP 値をスタック内の他のラベルにコピーしません。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。DSCP マップに整合性がある場合、出力 CoS は発信最上位ラベルの EXP 値に基づきます。

- 追加ラベルのインポーズ - 新規ラベルを既存のラベル スタックにインポーズする場合、PFC3BXL または PFC3B は内部 DSCP/EXP マップを使用して、インポーズされたラベルの EXP 値に内部 DSCP をマッピングします。次に、インポーズしたラベルの EXP 値を基本スワップ ラベルにコピーします。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。DSCP マップに整合性がある場合、出力 CoS はインポーズしたラベルの EXP 値に基づきます。

  PFC3BXL または PFC3B は適合するトラフィックをマーキングし、不適合トラフィックをマークダウンします。内部 DSCP をマーキングしたあと、PFC3BXL または PFC3B は内部 DSCP/EXP グローバル マップを使用して、新規にインポーズされたラベルの EXP 値に内部 DSCP をマッピングします。次に、PFC3BXL または PFC3B は、インポーズしたラベルの EXP 値を基本スワップ ラベルにコピーします。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。したがって、出力 CoS はインポーズしたラベルの EXP に基づきます。
- ラベルのポップ - ラベルをマルチラベル スタックからポップする場合、PFC3BXL または PFC3B はエクスポーズしたラベルの EXP 値を保持します。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。DSCP マップに整合性がある場合、出力 CoS はポップしたラベルの EXP 値に基づきます。
- 出力インターフェイスに EXP 伝播が設定されている場合は、PFC3BXL または PFC3B は DSCP/EXP グローバル マップを使用して、内部 DSCP をエクスポーズしたラベルの EXP 値にマッピングします。PFC3BXL または PFC3B は内部 DSCP/CoS グローバル マップを使用して、出力 CoS を割り当てます。DSCP マップに整合性がある場合、出力 CoS はエクスポーズしたラベルの EXP 値に基づきます。

MPLS/MPLS での PFC3BXL または PFC3B モード MPLS QoS の分類

P1 または P2 への入力時に、PFC3BXL または PFC3B モード MPLS QoS は次の機能をサポートします。

- **mpls experimental topmost** コマンドによる照合
- **set mpls experimental imposition**、**police**、**set imposition** を併用する **police** コマンド

PFC3BXL または PFC3B モード MPLS QoS は、P1 または P2 からの出力時に **mpls experimental topmost** コマンドによる照合をサポートします。

MPLS/MPLS 入力ポートでの分類

LAN ポートでの分類は、PFC3BXL または PFC3B からの出力 CoS に基づいて行われます。OSM および FlexWAN インターフェイスは、**match mpls experimental** コマンドを使用してトラフィックを分類します。**match mpls experimental** コマンドは、受信した最上位ラベルの EXP 値で一致します。

MPLS/MPLS 出力ポートでの分類

LAN ポートでの分類は、PFC3BXL または PFC3B からの出力 CoS 値に基づいて行われます。OSM および FlexWAN インターフェイスは、**match mpls experimental** コマンドを使用してトラフィックを分類します。**match mpls experimental** コマンドは、出力 CoS で一致しますが、最上位ラベルの EXP 値では一致しません。

出力ポートがトランク ポートの場合、LAN ポートおよび OSM GE-WAN ポートは、出力 CoS を出力 802.1Q フィールドにコピーします。

PFC3BXL または PFC3B MPLS QoS のデフォルト設定

ここでは、PFC3BXL または PFC3B MPLS QoS のデフォルト設定について説明します。次のグローバル PFC3BXL または PFC3B MPLS QoS 設定が適用されます。

機能	デフォルト値
PFC QoS のグローバル イネーブル ステート	（注）　PFC QoS がディセーブルで、他のすべての PFC QoS パラメータがデフォルト値の場合、デフォルトの EXP は IP precedence からマッピングされます。 （注）　PFC QoS がイネーブルで、他のすべての PFC QoS パラメータがデフォルト値の場合、PFC QoS は LAN ポート（デフォルトは untrusted）から送信されたすべてのトラフィックで、レイヤ 3 DSCP を 0（**untrusted** ポートのみ）に、レイヤ 2 CoS を 0 に、インポーズされた EXP を 0 に設定します。trust CoS の場合、EXP のデフォルト値は CoS からマッピングされます。trust DSCP の場合、EXP のデフォルト値は IP precedence からマッピングされます。OSM WAN ポートの場合、DSCP（デフォルトは trust DSCP）はインポーズされた EXP にマッピングされます。
PFC QoS のポート イネーブル ステート	PFC QoS がグローバルにイネーブルの場合、イネーブル
ポートの CoS 値	0
マイクロフロー ポリシング	イネーブル
VLAN 内マイクロフロー ポリシング	ディセーブル
ポート ベースまたは VLAN ベースの PFC QoS	ポートベース
EXP/DSCP マップ （EXP 値に基づき設定された DSCP）	EXP 0 = DSCP　0 EXP 1 = DSCP　8 EXP 2 = DSCP 16 EXP 3 = DSCP 24 EXP 4 = DSCP 32 EXP 5 = DSCP 40 EXP 6 = DSCP 48 EXP 7 = DSCP 56
IP precedence/DSCP マップ （IP precedence 値に基づき設定された DSCP）	IP precedence 0 = DSCP　0 IP precedence 1 = DSCP　8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56

機能	デフォルト値
DSCP/EXP マップ （DSCP 値に基づき設定された EXP）	DSCP　0–7　= EXP 0 DSCP　8–15 = EXP 1 DSCP 16–23 = EXP 2 DSCP 24–31 = EXP 3 DSCP 32–39 = EXP 4 DSCP 40–47 = EXP 5 DSCP 48–55 = EXP 6 DSCP 56–63 = EXP 7
DSCP マップからの DSCP のマークダウン	マークダウンされた DSCP 値は元の DSCP 値と等しい（マークダウンなし）
EXP 変換マップ	デフォルトでは変換マップなし
ポリサー	なし
ポリシー マップ	なし
NetFlow テーブルの MPLS フロー マスク	Label + EXP 値
MPLS コア QoS	MPLS コア QoS は、次の 4 つのいずれかとなります。 • スワップ - 着信 EXP フィールドは発信 EXP フィールドにコピーされます。 • スワップ＋インポジション - 着信 EXP フィールドは、スワップされた EXP フィールドとインポーズされた EXP フィールドの両方にコピーされます。 **（注）** EXP フィールド用にサービスポリシーが設定されている場合は、この EXP フィールドはインポーズされたラベル、およびスワップされたラベルに挿入されます。 • 最上位ラベルのディスポジション - エクスポーズした EXP フィールドを保持します。 • ラベルのみのディスポジション - エクスポーズした IP DSCP を保持します。
MPLS/IP エッジ QoS	エクスポーズした IP DSCP を保持します。

MPLS QoS コマンド

Catalyst 6500 シリーズ スイッチの PFC3BXL または PFC3B MPLS QoS は、次の MPLS QoS コマンドをサポートします。

- **match mpls experimental topmost**
- **set mpls experimental imposition**
- **police**
- **mls qos map exp-dscp**
- **mls qos map dscp-exp**
- **mls qos map exp-mutation**
- **mls qos exp-mutation**
- **show mls qos mpls**
- **no mls qos mpls trust exp**

（注）　サポートされる非 MPLS QoS コマンドの詳細については、「PFC QoS の設定」（P.41-61）を参照してください。

次のコマンドはサポートされません。

- **set qos-group**
- **set discard-class**

PFC3BXL または PFC3B モード MPLS QoS の注意事項および制約事項

PFC3BXL または PFC3B モード MPLS QoS を設定する場合は、次の注意事項および制約事項に従ってください。

- 受信パケットが IP パケットの場合の IP/MPLS または EoMPLS インポジション
  - QoS がディセーブルの場合は、EXP 値は受信した IP ToS に基づきます。
  - QoS が queuing-only モードの場合、EXP 値は受信した IP ToS に基づきます。
- 受信パケットが IP パケット以外の場合の EoMPLS インポジション
  - QoS がディセーブルの場合、EXP 値は入力 CoS に基づきます。
  - QoS が queuing-only モードの場合、EXP 値は受信した IP ToS に基づきます。
- MPLS/MPLS 操作
  - QoS がディセーブルの場合にスワップすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がキューイングする場合にのみスワップすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がディセーブルの場合に追加ラベルをインポーズすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。

  - QoS がキューイングする場合にのみ追加ラベルをインポーズすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がディセーブルの場合にラベルを 1 つポップすると、EXP 値は基本 EXP 値に基づきます。
  - QoS が キューイングする場合にのみラベルを 1 つポップすると、EXP 値は基本 EXP 値に基づきます。
- EXP 値は MPLS/IP ディスポジションとは関係ありません。
- **no mls qos rewrite ip dscp** コマンドと MPLS には互換性がありません。PFC3BXL または PFC3B がインポーズするラベルに正しい EXP 値を割り当てられるように、デフォルトの **mls qos rewrite ip dscp** コマンドはイネーブルである必要があります。
- Release 12.2(18)SXF2 以降のリリースでは、**no mls qos mpls trust exp** コマンドを使用すると、CoS および出力キューイングの目的で、MPLS パケットをレイヤ 2 パケットと同様に扱うことができます。この場合、デフォルトの EXP 値ではなく、ポートの信頼状態またはポリシーの信頼状態が適用されます。

PFC3BXL または PFC3B モード MPLS QoS の設定

ここでは、PFC3BXL または PFC3B モード MPLS QoS を設定する手順について説明します。

QoS をグローバルにイネーブルにする方法

PFC3BXL または PFC3B に QoS を設定する前に、**mls qos** コマンドを使用して、QoS 機能をグローバルにイネーブルにする必要があります。このコマンドを使用すると、トラフィックのデフォルトの QoS 処理がイネーブルになります。

mls qos コマンドがイネーブルになると、PFC3BXL または PFC3B はプライオリティ値を各フレームに割り当てます。この値は内部 DSCP です。内部 DSCP は、受信したフレームと QoS 設定の内容に基づいて割り当てられます。この値は、出力フレームの CoS および ToS フィールドに書き換えられます。

QoS をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	スイッチで PFC QoS をグローバルにイネーブルにします。
	`Router(config)# no mls qos`	スイッチで PFC QoS をグローバルにディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos`	設定を確認します。

次に、QoS をグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos
QoS is enabled globally
  Microflow policing is enabled globally
  QoS ip packet dscp rewrite enabled globally

  Qos trust state is DSCP on the following interfaces:
    Gi4/1 Gi4/1.12

  Qos trust state is IP Precedence on the following interfaces:
    Gi4/2 Gi4/2.42
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes


 ----- Module [5] -----
  QoS global counters:
    Total packets: 5957870
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 6
    IP packets with COS changed by policing: 0
    Non-IP packets with COS changed by policing: 3
    MPLS packets with EXP changed by policing: 0
```

queueing-only モードのイネーブル化

queueing-only モードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos queueing-only` `Router(config)# no mls qos queueing-only`	queueing-only モードをイネーブルにします。 PFC QoS をグローバルにディセーブルにします。 （注）　queueing-only モードは個別にディセーブルにできません。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos`	設定を確認します。

queueing-only モードをイネーブルにすると、ルータは次の処理を行います。

- マーキングおよびポリシングをグローバルにディセーブルにします。
- すべてのポートがレイヤ 2 CoS を信頼するように設定します。

（注）　スイッチでは、タグなし入力トラフィックと、trust CoS に設定できないポートを介して受信されるトラフィックにポート CoS 値が適用されます。

次に、queueing-only モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# mls qos queueing-only
Router(config)# end
Router#
```

制約事項および使用上の注意事項

QoS が PFC3BXL または PFC3B でディセーブル（**no mls qos**）の場合、EXP 値は次のように決定されます。

- 受信パケットが IP パケットの場合の IP/MPLS または EoMPLS インポジション
  - QoS がディセーブル（**no mls qos**）の場合、EXP 値は受信した IP ToS に基づきます。
  - QoS が queuing-only モードの場合（**mls qos queueing-only**）、EXP 値は受信した IP ToS に基づきます。
- 受信パケットが IP パケット以外の場合の EoMPLS インポジション
  - QoS がディセーブルの場合、EXP 値は入力 CoS に基づきます。
  - QoS が queuing-only モードの場合、EXP 値は受信した IP ToS に基づきます。
- MPLS/MPLS 操作
  - QoS がディセーブルの場合にスワップすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がキューイングする場合にのみスワップすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がディセーブルの場合に追加ラベルをインポーズすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。

  - QoS が queuing-only モードの場合に追加ラベルをインポーズすると、EXP 値は元の EXP 値に基づきます（EXP 変換が存在しない場合）。
  - QoS がディセーブルの場合にラベルを 1 つポップすると、EXP 値は基本 EXP 値に基づきます。
  - QoS が キューイングする場合にのみラベルを 1 つポップすると、EXP 値は基本 EXP 値に基づきます。
- EXP 値は MPLS/IP ディスポジションとは関係ありません。

MPLS パケット分類のためのクラス マップの設定

パケットの EXP 値によって MPLS ドメイン内のトラフィック クラスを定義するには、**match mpls experimental topmost** コマンドを使用できます。これにより、**police** コマンドを使用して、インターフェイス単位で EXP トラフィックをポリシングするようサービス ポリシーを定義できます。

クラス マップを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# class-map class_name`	パケットと一致するクラス マップを指定します。
ステップ 2	`Router(config-cmap)# match mpls experimental topmost value`	クラスと一致するパケット特性を指定します。
ステップ 3	`Router(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。

次に、MPLS EXP 値 3 を含むパケットすべてがトラフィック クラス exp3 と一致する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map exp3
Router(config-cmap)# match mpls experimental topmost 3
Router(config-cmap)# exit
Router(config)# policy-map exp3
Router(config-pmap)# class exp3
Router(config-pmap-c)# police 1000000 8000000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# end
Router# show class exp3
 Class Map match-all exp3 (id 61)
   Match mpls experimental topmost 3
Router# show policy-map exp3
  Policy Map exp3
    Class exp3
     police cir 1000000 bc 8000000 be 8000000 conform-action transmit exceed-action drop
Router# show running-config interface fastethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface FastEthernet3/27
  ip address 47.0.0.1 255.0.0.0
  tag-switching ip
 end

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/27
```

```
Router(config-if)# service-policy input exp3
Router(config-if)#
Router#
Enter configuration commands, one per line.  End with CNTL/Z.
Router# show running-config interface fastethernet 3/27
Building configuration...

Current configuration : 173 bytes
!
interface FastEthernet3/27
  ip address 47.0.0.1 255.0.0.0
  tag-switching ip
  service-policy input exp3
 end

Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show mls qos mpls
 QoS Summary [MPLS]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
------------------------------------------------------------------------------
    Fa3/27  5  In       exp3    0    2   dscp  0              0              0

       All  5   -    Default    0    0*    No  0     3466140423              0
Router# show policy-map interface fastethernet 3/27
 FastEthernet3/27

  Service-policy input: exp3

    class-map: exp3 (match-all)
      Match: mpls experimental topmost 3
      police :
        1000000 bps 8000000 limit 8000000 extended limit
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/27
Router(config-if)# service-policy output ip2tag
Router(config-if)# end
Router# show mls qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
------------------------------------------------------------------------------
     Vl300  5  In          x   44    1     No  0              0              0
    Fa3/27  5 Out      iptcp   24    2     --  0              0              0

       All  5   -    Default    0    0*    No  0     3466610741              0
```

制約事項および使用上の注意事項

MPLS パケットを分類する場合は、次の制約事項および注意事項が適用されます。

- **match mpls experimental** コマンドでは、一致基準として使用する EXP フィールド値の名前を指定します。各パケットはこの基準に基づき、クラス マップによって指定されたクラスに属するかどうかをチェックされます。
- **match mpls experimental** コマンドを使用するには、確立したい基準と一致するクラス名を指定するため、まず **class-map** コマンドを入力する必要があります。クラスを特定してから、**match mpls experimental** コマンドを使用して一致基準を設定できます。
- 1 つのクラス マップで複数のコマンドを指定すると、最後に入力したコマンドだけが適用されます。最後のコマンドは、それ以前に入力したコマンドを上書きします。

入力ポートでの MPLS パケットの信頼状態の設定

no mls qos mpls trust exp コマンドを使用すると、レイヤ 2 パケットに適用する場合と同様に、MPLS パケットにポートまたはポリシーの信頼状態を適用できます。

入力ポートの MPLS パケット信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type slot/port} | {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 2	`Router(config-if)# no mls qos mpls trust exp`	信頼できるすべてのトラフィック（trust cos、trust dscp、trust ip-precedence）が trust-cos として扱われるように、MPLS パケットの信頼状態を設定します。
	`Router(config-if)# mls qos mpls trust exp`	着信パケット内の EXP 値だけが信頼されるように、デフォルトの信頼状態に戻します。
ステップ 3	`Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls qos`	設定を確認します。

次の例では、着信 MPLS パケットが着信レイヤ 2 パケットと同様に動作するように、MPLS パケットの信頼状態を untrusted に設定します。

```
Router(config)# interface fastethernet 3/27
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

制約事項および使用上の注意事項

no mls qos mpls trust exp コマンドを使用して、入力ポートでの MPLS パケットの信頼状態を設定する場合は、以下の制約事項および注意事項に従ってください。

- このコマンドは、レイヤ 2 パケットにもレイヤ 3 パケットにも影響を与えます。したがって、このコマンドはレイヤ 2 パケットがスイッチングされるインターフェイスのみで使用してください。
- **no mls qos mpls trust exp** コマンドは入力マーキングに影響を与えますが、分類には影響はありません。

ポリシー マップの設定

1 つのインターフェイスに付加できるポリシー マップは、1 つに限られます。ポリシー マップには、ポリシー マップ コマンドがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

インターフェイスで受信するトラフィック タイプごとに、個別のポリシー マップ クラスをポリシー マップ内に設定します。各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。PFC3BXL または PFC3B MPLS QoS は、一致したトラフィックに複数のポリシー マップ クラスのコマンドを適用することはありません。

インポーズしたラベルすべてで EXP 値を設定するためのポリシー マップの設定

インポーズしたラベル エントリのすべてで MPLS EXP フィールドの値を設定するには、QoS ポリシー マップ クラス コンフィギュレーション モードで **set mpls experimental imposition** コマンドを使用します。設定をディセーブルにするには、このコマンドの no 形式を使用します。

（注）　**set mpls experimental** コマンドが **set mpls experimental imposition** コマンドに置き換えられます。

	コマンド	目的
ステップ 1	`Router(config)# policy-map policy_name`	ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class-map name [match-all | match-any]`	QoS クラス マップを設定するため、QoS クラス マップ コンフィギュレーション モードにアクセスします。
ステップ 3	`Router(config-pmap-c)# set mpls experimental imposition {mpls-exp-value | from-field [table table-map-name]}`	インポーズしたラベル エントリすべてで MPLS EXP フィールドの値を設定します。
ステップ 4	`Router(config-pmap-c)# exit`	クラスマップ コンフィギュレーション モードを終了します。

次に、MPLS EXP 値 3 で定義された DSCP 値に従って、MPLS EXP インポジション値を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# access-l 101 p tcp any any
Router(config)# class-map iptcp
Router(config-cmap)# match acc 101
Router(config-cmap)# exit
Router(config)#
Router(config-cmap)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# set mpls exp imposition 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
Router#
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# show policy-map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
```

```
Router# show class iptcp
 Class Map match-all iptcp (id 62)
   Match access-group101

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
Routers
1w4d: %SYS-5-CONFIG_I: Configured from console by console
Router# show pol ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
Router# show class-map iptcp
 Class Map match-all iptcp (id 62)
   Match access-group  101

Router# show access-l 101
Extended IP access list 101
    10 permit tcp any any
Router# show mls qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
------------------------------------------------------------------------------
    Fa3/27  5  In      iptcp   24    2     No  0              0              0
     Vl300  5  In          x   44    1     No  0              0              0

       All  5   -    Default    0    0*    No  0     3466448105              0
Router#
Router# show policy-map interface fastethernet 3/27
 FastEthernet3/27

  Service-policy input: ip2tag

    class-map: iptcp (match-all)
      Match: access-group 101
      set mpls experimental 3:
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes

    class-map: class-default (match-any)
      Match: any

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

次に、設定を確認する例を示します。

```
Router# show policy map ip2tag
  Policy Map ip2tag
    Class iptcp
      set mpls experimental imposition 3
```

EXP 値のインポジションに関する注意事項および制約事項

インポーズしたすべてのラベルに EXP 値を設定する場合は、次の注意事項および制約事項に従います。

- ラベルのインポジション中は **set mpls experimental imposition** コマンドを使用します。このコマンドは、インポーズされたすべてのラベル エントリの MPLS EXP フィールドを設定します。
- **set mpls experimental imposition** コマンドは、入力インターフェイス（インポジション）でのみサポートされます。
- **set mpls experimental imposition** コマンドは EXP 値を直接マーキングしません。代わりに、内部 DSCP/EXP グローバル マップを通じて EXP にマッピングされる内部 DSCP をマーキングします。
- 分類（元の受信 IP ヘッダーに基づく）とマーキング（内部 DSCP に対して行われる）においては、IP/IP トラフィックと IP/MPLS トラフィックとが区別されないことに注意してください。IP ToS および EXP のマーキングに使用するコマンドの実行結果は、内部 DSCP をマーキングした場合と同じです。
- プッシュされたラベル エントリ値をデフォルト値とは異なる値に設定するには、**set mpls experimental imposition** コマンドを使用します。
- IP precedence、DSCP フィールド、または QoS IP ACL で **set mpls experimental imposition** コマンドを任意で使用すると、インポーズされたラベル エントリすべてで MPLS EXP フィールドを設定できます。
- PFC3BXL または PFC3B で受信 IP トラフィックにラベルをインポーズする場合、**set mpls experimental imposition** コマンドを使用して、EXP フィールドをマーキングできます。

このコマンドの詳細については、次の URL にある『*Cisco IOS Switching Services Command Reference*』Release 12.3 を参照してください。

http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_s1.html#set_mpls_experimental_imposition

police コマンドを使用したポリシー マップの設定

ポリシングは、特定のトラフィック クラスを固有のレートに制限する、PFC3BXL または PFC3B ハードウェアの機能です。PFC3BXL または PFC3B は、集約ポリシングおよびマイクロフロー ポリシングをサポートします。

集約ポリシングは、異なる送信元、宛先、プロトコル、送信元ポート、または宛先ポートに関係なく、ポートに入るトラフィックをすべて測定します。マイクロフロー ポリシングは、ポートに入るトラフィックすべてをフロー単位で（送信元、宛先、プロトコル、送信元ポート、または宛先ポート単位で）測定します。集約ポリシングおよびマイクロフロー ポリシングの詳細については、「ポリサー」（P.41-20）を参照してください。

トラフィック ポリシングを設定するには、**police** コマンドを使用します。このコマンドの詳細については、『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

	コマンド	目的
ステップ 1	`Router(config)# policy-map policy_name`	ポリシー マップを作成します。
ステップ 2	`Router(config-pmap)# class-map name [match-all | match-any]`	QoS クラス マップを設定するため、QoS クラス マップ コンフィギュレーション モードにアクセスします。
ステップ 3	`Router(config-pmap-c)# police {aggregate name}`	共有集約ポリサーにクラスを追加します。
ステップ 4	`Router(config-pmap-c)# police bps burst_normal burst_max conform-action action exceed-action action violate-action action`	クラス別インターフェイス別のポリサーを作成します。

	コマンド	目的
ステップ 5	`Router(config-pmap-c)# police flow {bps [burst_normal] | [conform-action action] [exceed-action action]`	入力フロー ポリサーを作成します（出力ポリシーではサポートされません）。
ステップ 6	`Router(config-pmap-c)# exit`	クラスマップ コンフィギュレーション モードを終了します。

次に、ポリサーでポリシー マップを作成する例を示します。

```
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# no set mpls exp topmost 3
Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp?
set-mpls-exp-imposition-transmit

Router(config-pmap-c)# police 1000000 1000000 c set-mpls-exp-imposit 3 e d
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 3/27
Router(config-if)# ser in ip2tag
Router(config-if)#
```

次に、設定を確認する例を示します。

```
Router# show pol ip2tag
  Policy Map ip2tag
    Class iptcp
     police cir 1000000 bc 1000000 be 1000000 conform-action
set-mpls-exp-imposition-transmit 3 exceed-action drop
Router# show running-config interface fastethernet 3/27
Building configuration...

Current configuration : 202 bytes
!
interface FastEthernet3/27
  logging event link-status
  service-policy input ip2tag
end

Router# show mls qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/27  5  In      iptcp   24    2     No  0              0              0
     Vl300  5  In          x   44    1     No  0              0              0

       All  5   -    Default    0    0*    No  0     3468105262              0
Router# show policy interface fastethernet 3/27
 FastEthernet3/27

  Service-policy input: ip2tag

    class-map: iptcp (match-all)
      Match: access-group 101
      police :
        1000000 bps 1000000 limit 1000000 extended limit
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: set-mpls-exp-imposition-transmit
```

```
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

    class-map: class-default (match-any)
      Match: any

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
R7# show mls qos ip
 QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
-------------------------------------------------------------------------------
    Fa3/27  5  In      iptcp   24    2     No  0              0              0
     Vl300  5  In          x   44    1     No  0              0              0

       All  5   -    Default    0    0*    No  0     3468161522              0
```

制約事項および使用上の注意事項

police コマンドを使用してポリシー マップを設定する場合は、次の制約事項および注意事項が適用されます。

- MPLS では、**exceed-action** *action* コマンドと **violate-action** *action* コマンドは、IP を使用する場合と同様に動作します。パケットが廃棄されるか、または EXP 値がマークダウンされます。これらのアクションが IP/IP トラフィックに与える影響については、「ポリシー マップの設定」（P.41-80）を参照してください。
- MPLS では、**set-dscp transmit** *action* コマンドと **set-prec-transmit** *action* コマンドは、CoS ビットにマッピングされる内部 DSCP を設定します。内部 DSCP はキューイングに影響します。ただし、インポジション以外の EXP 値は変更されません。
- PFC3BXL または PFC3B で受信 MPLS トラフィックのラベルをスワップする場合、**police** コマンドの **exceed-action policed-dscp-transmit** および **violate-action policed-dscp-transmit** キーワードを使用して、不適合トラフィックをマークダウンできます。PFC3BXL または PFC3B は、適合するトラフィックをマーキングしません。不適合トラフィックをマークダウンする場合、PFC3BXL または PFC3B は発信最上位ラベルをマーキングします。PFC3BXL または PFC3B は、ラベル スタック内でマークダウンを伝播しません。
- MPLS では、フロー キーはラベルおよび EXP 値に基づきます。フローマスク オプションはありません。それ以外の場合、フロー キー操作は IP/IP と同様です。「ポリシー マップの設定」（P.41-80）を参照してください。
- **police** コマンドを使用すると、プッシュしたラベル エントリ値を、ラベル インポジション中のデフォルト値とは異なる値に設定できます。
- PFC3BXL または PFC3B で受信 IP トラフィックにラベルをインポーズする場合、**conform-action set-mpls-exp-imposition-transmit** キーワードを使用して、EXP フィールドをマーキングできます。
- IP/MPLS インポジション中、IP ToS マーキングはサポートされません。IP ToS をマーキングするようにポリシーを設定すると、PFC3BXL または PFC3B は EXP 値をマーキングします。

ポリシー マップの表示

ポリシー マップの表示では、MPLS QoS クラスのインターフェイス サマリーを表示するか、または指定したインターフェイス上のサービス ポリシーすべてに対して設定された全クラスの設定を表示できます。

PFC3BXL または PFC3B モード MPLS QoS ポリシー マップのクラス サマリーの表示

PFC3BXL または PFC3B モード MPLS QoS ポリシー マップのクラス サマリーを表示するには、次の作業を行います。

コマンド	目的
Router# **show mls qos mpls** [{**interface** *interface_type interface_number*} | {**module** *slot*}	PFC3BXL または PFC3B モード MPLS QoS ポリシー マップのクラス サマリーを表示します。

次に、PFC3BXL または PFC3B モード MPLS QoS ポリシー マップのクラス サマリーを表示する例を示します。

```
Router# show mls qos mpls
 QoS Summary [MPLS]:      (* - shared aggregates, Mod - switch module)
      Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                   Id         Id
------------------------------------------------------------------------------
    Fa3/27  5  In       exp3    0    2   dscp  0              0              0
       All  5   -    Default    0    0*    No  0     3466140423              0
```

すべてのクラスの設定の表示

指定したインターフェイス上のすべてのサービス ポリシーに対して設定された、すべてのクラスの設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show policy interface** *interface_type interface_number*	指定したインターフェイス上のすべてのポリシー マップに設定された、すべてのクラスの設定を表示します。

次に、ファスト イーサネット インターフェイス 3/27 の全クラスの設定を表示する例を示します。

```
Router# show policy interface fastethernet 3/27
 FastEthernet3/27

  Service-policy input: ip2tag

    class-map: iptcp (match-all)
      Match: access-group 101
      police :
        1000000 bps 1000000 limit 1000000 extended limit
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: set-mpls-exp-imposition-transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
```

```
class-map: class-default (match-any)
  Match: any

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

PFC3BXL または PFC3B モード MPLS QoS の出力 EXP 変換の設定

ここでは、PFC3BXL または PFC3B モード MPLS QoS の出力 EXP 変換を設定する手順について説明します。

- 「名前付き EXP 変換マップの設定」（P.42-31）
- 「インターフェイスへの出力 EXP 変換マップの付加」（P.42-32）

名前付き EXP 変換マップの設定

名前付き EXP 変換マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos map exp-mutation` *name mutated_exp1 mutated_exp2 mutated_exp3 mutated_exp4 mutated_exp5 mutated_exp6 mutated_exp7 mutated_exp8*	名前付き EXP 変換マップを設定します。
	`Router(config)# no mls qos map exp-mutation` *name*	デフォルトのマッピングに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos maps`	設定を確認します。

名前付き EXP 変換マップを設定する場合は、次の点に注意してください。

- 変換された EXP 値にマッピングする、最大 8 つの入力 EXP 値を入力できます。
- 複数のコマンドを入力して、変換された EXP 値に追加の EXP 値をマッピングできます。
- 変換された EXP 値ごとに個別のコマンドを入力できます。
- 内部 EXP 値が入力 EXP 値として書き込まれる前に、内部 EXP 値を変換する入力 EXP 変換マップを最大 15 個設定できます。入力 EXP 変換 マップは、PFC QoS がサポートする任意のインターフェイスに付加できます。
- PFC QoS は、内部 DSCP 値に基づいて出力 EXP 値を作成します。入力 EXP 変換を設定する場合は、PFC QoS は変換した EXP 値から入力 EXP 値を作成しません。

インターフェイスへの出力 EXP 変換マップの付加

出力 EXP 変換マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID}	{type[1] slot/port[.subinterface]}	{port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos exp-mutation exp-mutation-table-name` `Router(config-if)# no mls qos exp-mutation`	出力 EXP 変換マップをインターフェイスに付加します。 インターフェイスから出力 DSCP 変換マップを削除します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show running-config interface {{vlan vlan_ID}	{type slot/port}	{port-channel number}}`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、mutemap2 という名前の出力 EXP 変換マップを付加する例を示します。

```
Router(config)# interface fastethernet 3/26
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)# end
```

EXP 値マッピングの設定

ここでは、EXP 値を他の値にマッピングする方法について説明します。

- 「入力 EXP/内部 DSCP マップの設定」（P.42-33）
- 「名前付き出力 DSCP/出力 EXP マップの設定」（P.42-33）

入力 EXP/内部 DSCP マップの設定

入力 EXP/内部 DSCP マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos map exp-dscp values`	入力 EXP 値から内部 DSCP 値へのマッピングを設定します。EXP 値に対応する DSCP 値を 8 個入力する必要があります。有効値は 0 ～ 63 です。
	`Router(config)# no mls qos map exp-dscp`	デフォルトのマッピングに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos maps`	設定を確認します。

次に、入力 EXP/内部 DSCP マップを設定する例を示します。

```
Router(config)# mls qos map exp-dscp 43 43 43 43 43 43 43 43
Router(config)#
```

次に、設定を確認する例を示します。

```
Router(config)# show mls qos map exp-dscp
   Exp-dscp map:
         exp:   0  1  2  3  4  5  6  7
      ------------------------------------
         dscp:  43 43 43 43 43 43 43 43
```

名前付き出力 DSCP/出力 EXP マップの設定

名前付き出力 DSCP/出力 EXP マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos map dscp-exp dscp_values to exp_values`	名前付き出力 DSCP/出力 EXP マップを設定します。1 つの EXP 値には、一度に最大 8 個の DSCP 値を入力できます。有効値は 0 ～ 7 です。
	`Router(config)# no mls qos map dscp-exp`	デフォルトのマッピングに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos maps`	設定を確認します。

次に、名前付き出力 DSCP/出力 EXP マップを設定する例を示します。

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

MPLS DiffServ トンネリング モード

トンネリングでは、ネットワークの一方のエッジから他方のエッジまで、QoS を透過的にできます。トンネルは、ラベルがインポーズされたところから開始します。トンネルは、ラベルがディスポーズされたところで終了します。つまり、ここではラベルがスタックから取り外され、パケットは下位に位置する別の Per-Hop Behavior（PHB）レイヤでの MPLS パケットとして、または IP PHB レイヤでの IP パケットとして出力されます。

PFC3BXL または PFC3B では、ネットワーク上でパケットを転送する方法が 2 つあります。

- Short Pipe モード - Short Pipe モードでは、出力 PE ルータは中間プロバイダー（P）ルータによるマーキングではなく、元のパケット マーキングを使用します。EXP マーキングは、パケット ToS バイトに伝播しません。

  このモードの詳細については、「Short Pipe モード」（P.42-35）を参照してください。

  設定の詳細については、「Short Pipe モードの設定」（P.42-38）を参照してください。

- Uniform モード - Uniform モードでは、IP パケットのマーキングを操作して、サービス プロバイダーの QoS マーキングをコアに反映できます。このモードでは、CE ルータやコア ルータを含め、ネットワーク全体で一貫した QoS 分類およびマーキングを実行できます。EXP マーキングは基本 ToS バイトに伝播されます。

  詳細については、「Uniform モード」（P.42-36）を参照してください。

  設定手順の詳細については、「Uniform モードの設定」（P.42-43）を参照してください。

いずれのトンネリング モードも、エッジ LSR および直前 LSR の動作に影響します。ここではラベルのパケットへの付加、およびパケットからの削除が行われます。これらのモードは、中間ルータでのラベル スワップには影響しません。サービス プロバイダーは、カスタマーごとに異なるタイプのトンネリング モードを選択できます。

詳細については、次の URL にある「MPLS DiffServ Tunneling Modes」を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftdtmode.html

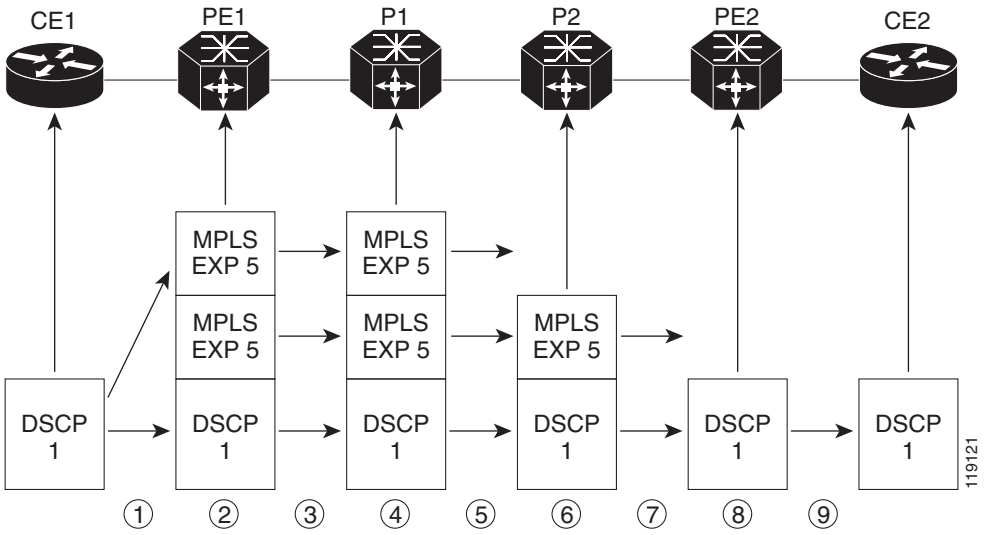
Short Pipe モード

Short Pipe モードは、カスタマーとサービス プロバイダーの DiffServ ドメインが異なる場合に使用します。これにより、サービス プロバイダーは独自の DiffServ ポリシーを実行しつつ、カスタマーの DiffServ 情報を保存できます。この結果、サービス プロバイダー ネットワーク全体において、DiffServ の透過性を維持できます。

コアで実装された QoS ポリシーは、パケットの ToS バイトに伝播しません。MPLS EXP 値に基づいた分類は、カスタマー方向の出力 PE インターフェイスで終了します。カスタマー方向の出力 PE インターフェイスでの分類は、MPLS ヘッダーではなく、元の IP パケット ヘッダーに基づきます。

（注） 出力 IP ポリシー（プロバイダーの PHB マーキングではなく、カスタマーの PHB マーキングに基づく）が存在する場合は、自動的に Short Pipe モードであることを意味します。

図 42-2　VPN での Short Pipe モードの動作



Short Pipe モードは次のように機能します。

1. CE1 は IP パケットを、IP DSCP 値 1 の PE1 に送信します。
2. PE1 は MPLS EXP フィールドをインポーズ ラベル エントリの 5 に設定します。
3. PE1 はパケットを P1 に送信します。
4. P1 は MPLS EXP フィールド値をスワップ ラベル エントリの 5 に設定します。
5. P1 はパケットを P2 に送信します。
6. P2 は IGP ラベル エントリをポップします。
7. P2 はパケットを PE2 に送信します。
8. PE2 は BGP ラベルをポップします。
9. PE2 はパケットを CE2 に送信しますが、IP DSCP 値に基づいて QoS を送信しません。

詳細については、次の URL にある「MPLS DiffServ Tunneling Modes」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftdtmode.html

Short Pipe モードの制約事項および注意事項

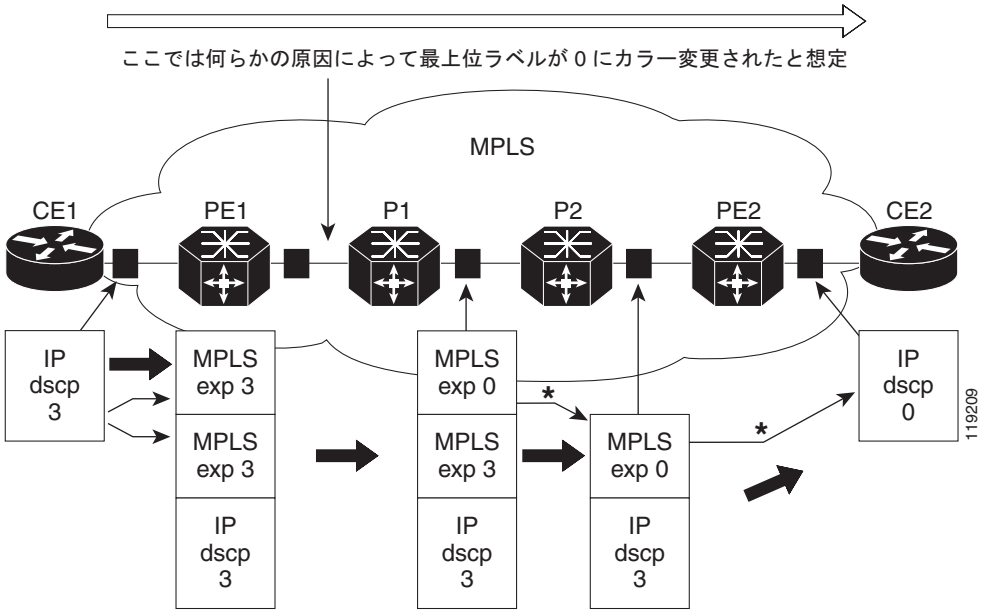
次の制約事項が Short Pipe モードに適用されます。

- MPLS/IP 出力インターフェイスが EoMPLS である（隣接に End of Marker（EoM）ビットが設定されている）場合、Short Pipe モードはサポートされません。

Uniform モード

Uniform モードでは、パケットは IP および MPLS ネットワークで均一に処理されます。つまり、IP precedence 値および MPLS EXP ビットは、常に同じ PHB に対応します。ルータがパケットの PHB を変更またはリカラーするつど、その変更は、カプセル化のマーキングすべてに伝播される必要があります。ルータによる伝播が行われるのは、パケットのパス上にあるいずれかのルータでラベルのインポジションまたはディスポジションが行われたため、PHB が追加またはエクスポーズされた場合のみです。カラーは、全レベルのあらゆる場所に反映する必要があります。たとえば、パケットの QoS マーキングが MPLS ネットワークで変更された場合、IP QoS マーキングはその変更を反映します。

図 42-3　　Uniform モードでの操作



*MPLS-to-MPLS、MPLS-to-IP のいずれの場合もラベルが残っていない場合は、
最上位の PHB ポップ ラベルが新規最上位ラベルまたは IP DSCP にコピーされます。

このアクションは、IP precedence ビット マーキングまたは DSCP マーキングのどちらが存在するかによって異なります。

IP precedence ビット マーキングが存在する場合は、次のアクションが行われます。

1. IP パケットが、MPLS ネットワーク内の PE1（サービス プロバイダーのエッジ ルータ）に着信します。
2. ラベルがパケットにコピーされます。
3. MPLS EXP フィールド値がリカラーされる場合は（送信されるパケット数が多すぎたためにパケットがレート超過になる場合など）、その値が IGP ラベルにコピーされます。BGP ラベル値は変更されません。

4. 直前ホップでは、IGP ラベルは削除されます。この値は、次に低いレベルのラベルにコピーされます。
5. すべての MPLS ラベルが IP パケットとして送信されるパケットから削除されると、IP precedence 値または DSCP 値は、コアで最後に変更された EXP 値に設定されます。

次に、IP precedence ビット マーキングが存在する場合の例を示します。

1. CE1（カスタマー装置 1）では、IP パケットの IP precedence 値が 3 となっています。
2. パケットが MPLS ネットワーク内の PE1（サービス プロバイダーのエッジ ルータ）に着信すると、パケットにインポーズされたラベル エントリに IP precedence 値 3 がコピーされます。
3. IGP ラベル ヘッダーの MPLS EXP フィールドは、マークダウンすることで MPLS コア内（P1 など）で変更できます。

（注）　IP precedence ビットが 3 であり、Uniform モードではラベルが常に同じなので、BGP ラベルおよび IGP ラベルの値も 3 となります。パケットは IP および MPLS ネットワークで均一に処理されます。

Uniform モードの制約事項および注意事項

次の制約事項は Uniform モードに適用されます。

- 出力 IP ACL またはサービス ポリシーが MPLS/IP 終了ポイントで設定されている場合、Uniform モードは再循環されるので常に実行されます。

MPLS DiffServ トンネリングの制限事項および使用上の注意事項

MPLS DiffServ トンネリングの 制限事項および使用上の注意事項は次のとおりです。

- MPLS EXP フィールドは 3 ビット フィールドなので、1 個の LSP では、最大 8 個のトラフィック クラス（つまり 8 個の PHB）をサポートできます。
- MPLS DiffServ トンネリング モードは E-LSP をサポートします。E-LSP は、ノードが MPLS ヘッダーの EXP ビットからのみ、MPLS パケットに対する QoS 処理を決定する LSP です。

次の機能は、MPLS DiffServ トンネリング モードでサポートされます。

- MPLS Per-Hop Behavior（PHB）レイヤ管理 （レイヤ管理は、パケットにマーキングする PHB のレイヤを追加する機能です）
- 管理 CE ルータ上での制御による、MPLS レイヤ管理の向上したスケーラビリティ
- MPLS がパケットの QoS をトンネリング可能（QoS がエッジからエッジまで透過的）。QoS の透過性では、IP パケットの IP マーキングは MPLS ネットワーク上で保持されます。
- MPLS EXP フィールドは、IP precedence フィールドまたは DSCP フィールドでマーキングされた PHB とは別々にマーキングされます。

Short Pipe モードの設定

ここでは、Short Pipe モードの設定方法について説明します。

（注）
- 次のステップは、Short Pipe モードを設定する方法を示しますが、これが唯一の方法ではありません。
- IP クラスを含んだ出力サービス ポリシーをインターフェイスに付加する場合、出力 PE（または PHP）の Short Pipe モードは自動設定されます。

入力 PE ルータ - カスタマー方向インターフェイス

この手順では、MPLS EXP フィールドをインポーズ ラベル エントリに設定するようポリシー マップを設定します。

EXP 値を設定するには、入力 LAN または OSM ポートが信頼不可（untrusted）である必要があります。FlexWAN ポートには信頼性の概念がありませんが、従来の Cisco IOS ルータと同様、入力 ToS は変更されません（マーキング ポリシーが設定されていない限り）。

MPLS および VPN では、入力 PE はすべての入力 PFC3BXL または PFC3B IP ポリシーをサポートします。IP ACL/DSCP/precedence に基づいた PFC IP ポリシーの分類の詳細については、http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/qos.html を参照してください。

MPLS EXP フィールドをインポーズ ラベル エントリに設定するようにポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# access-list` *ipv4_acl_number_or_name* `permit any`	IPv4 アクセス リストを作成します。
ステップ 3	`Router(config)# class-map` *class_name*	クラス マップを作成します。
ステップ 4	`Router(config-cmap)# match access-group` *ipv4_acl_number_or_name*	ステップ 2 で作成した ACL に基づくフィルタリングを行うように、クラス マップを設定します。
ステップ 5	`Router(config)# policy-map` *policy_map_name*	名前付き QoS ポリシーを作成します。
ステップ 6	`Router(config-pmap)# class` *class_name*	ステップ 3 で作成したクラス マップを使用するように、ポリシーを設定します。

	コマンド	目的
ステップ 7	`Router(config-pmap-c)# police bits_per_second [normal_burst_bytes] conform-action set-mpls-exp-transmit exp_value exceed-action drop`	ポリシングを設定します。ここでは、次を設定します。 • Service Level Agreement（SLA; サービス レベル契約）で指定されたレート制限に準拠するパケットに対して実行するアクション。 • SLA で指定されたレート制限を超えるパケットに対して実行するアクション。 *exp_value* は、MPLS EXP フィールドを設定します。
ステップ 8	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# no mls qos trust`	インターフェイスを untrusted として設定します。
ステップ 10	`Router(config-if)# service-policy input policy_map_name`	ステップ 5 で作成したポリシー マップを、入力サービス ポリシーとしてインターフェイスに付加します。

設定例

次に、MPLS EXP フィールドをインポーズ ラベル エントリに設定するようポリシー マップを設定する例を示します。

```
Router(config)# mls qos
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map set-MPLS-PHB
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action set-mpls-exp-transmit 4
exceed-action drop
Router(config)# interface GE-WAN 3/1
Router(config-if)# no mls qos trust
Router(config)# interface GE-WAN 3/1.31
Router(config-if)# service-policy input set-MPLS-PHB
```

入力 PE ルータの設定 - P 方向インターフェイス

この手順では、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行います。

（注）　ここで示す QoS 機能は、OSM、FlexWAN、拡張 FlexWAN モジュールでのみ利用できます。

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# class-map class_name`	パケットがマッピングされる（パケットと一致する）クラス マップを指定します。トラフィック クラスを作成します。
ステップ 3	`Router(config-c-map)# match mpls experimental exp_list`	パケットがクラスに属するかを判別するための照合で一致基準として使用される、MPLS EXP フィールド値を指定します。
ステップ 4	`Router(config)# policy-map name`	クラスと一致するパケットに QoS ポリシーを設定します。
ステップ 5	`Router(config-p-map)# class class_name`	トラフィック クラスとサービス ポリシーを関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに対する最小帯域幅保証を指定します。最小帯域幅保証は、kbps 単位または帯域幅全体の割合で指定できます。
ステップ 7	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 8	`Router(config-p-map-c)# random-detect`	帯域幅保証のあるトラフィック クラスに対し、WRED 廃棄ポリシーをイネーブルにします。
ステップ 9	`Router(config)# interface type slot/port`	設定するインターフェイスを選択します。
ステップ 10	`Router(config-if)# service-policy output name`	QoS ポリシーをインターフェイスに付加し、インターフェイスから送信されるパケット上に適用するポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行う例を示します。

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

P ルータの設定 - 出力インターフェイス

（注）　ここで示す QoS 機能は、OSM、FlexWAN、拡張 FlexWAN モジュールでのみ利用できます。

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# class-map` *class_name*	パケットがマッピングされる（パケットと一致する）クラス マップを指定します。トラフィック クラスを作成します。
ステップ 3	`Router(config-c-map)# match mpls experimental` *exp_list*	パケットがクラスに属するかを判別するための照合で一致基準として使用される、MPLS EXP フィールド値を指定します。
ステップ 4	`Router(config)# policy-map` *name*	クラスと一致するパケットに QoS ポリシーを設定します。
ステップ 5	`Router(config-p-map)# class` *class_name*	トラフィック クラスとサービス ポリシーを関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth` {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに対する最小帯域幅保証を指定します。最小帯域幅保証は、kbps 単位または帯域幅全体の割合で指定できます。
ステップ 7	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 8	`Router(config-p-map-c)# random-detect`	IP precedence または MPLS EXP フィールド値に基づいて、WRED をポリシーに適用します。
ステップ 9	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 10	`Router(config-if)# service-policy output` *name*	QoS ポリシーをインターフェイスに付加し、インターフェイスから送信されるパケット上に適用するポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行う例を示します。

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-4
Router(config-c-map)# match mpls experimental 4
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 2/1
Router(config-if)# service-policy output output-qos
```

出力 PE ルータの設定 - カスタマー方向インターフェイス

（注）　ここで示す QoS 機能は、OSM、FlexWAN、拡張 FlexWAN モジュールでのみ利用できます。

IP DSCP 値に基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# class-map` *class_name*	パケットがマッピングされる（パケットと一致する）クラス マップを指定します。トラフィック クラスを作成します。
ステップ 3	`Router(config-c-map)# match ip dscp` *dscp_values*	DSCP 値を一致基準として使用します。
ステップ 4	`Router(config)# policy-map` *name*	クラスと一致するパケットに QoS ポリシーを設定します。
ステップ 5	`Router(config-p-map)# class` *class_name*	トラフィック クラスとサービス ポリシーを関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth` {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに対する最小帯域幅保証を指定します。最小帯域幅保証は、kbps 単位または帯域幅全体の割合で指定できます。
ステップ 7	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 8	`Router(config-p-map-c)# random-detect dscp-based`	帯域幅保証のあるトラフィック クラスに対し、WRED 廃棄ポリシーをイネーブルにします。
ステップ 9	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 10	`Router(config-if)# service-policy output` *name*	QoS ポリシーをインターフェイスに付加し、インターフェイスから送信されるパケット上に適用するポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、IP DSCP 値に基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行う例を示します。

```
Router(config)# mls qos
Router(config)# class-map IP-PREC-4
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface GE-WAN 3/2.32
Router(config-if)# service-policy output output-qos
```

Uniform モードの設定

ここでは、次を設定する手順について説明します。

- 「入力 PE ルータ - カスタマー方向インターフェイスの設定」（P.42-44）
- 「入力 PE ルータ - P 方向インターフェイスの設定」（P.42-45）
- 「出力 PE ルータの設定 - カスタマー方向インターフェイス」（P.42-46）

（注）　次のステップは、Uniform モードを設定する方法を示しますが、これが唯一の方法ではありません。

入力 PE ルータ - カスタマー方向インターフェイスの設定

Uniform モードで、IP precedence または IP DSCP に信頼状態を設定すると、PFC3BXL または PFC3B は IP PHB を MPLS PHB にコピーできます。

（注）　この説明は、LAN または OSM ポートの PFC3BXL または PFC3B に適用されます。FlexWAN および拡張 FlexWAN QoS の詳細については、次の URL にある『FlexWAN and Enhanced FlexWAN Modules Installation and Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

MPLS EXP フィールドをインポーズ ラベル エントリに設定するようポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# access-list` *ipv4_acl_number_or_name* `permit any`	IPv4 アクセス リストを作成します。
ステップ 3	`Router(config)# class-map` *class_name*	クラス マップを作成します。
ステップ 4	`Router(config-cmap)# match access-group` *ipv4_acl_number_or_name*	ステップ 2 で作成した ACL に基づくフィルタリングを行うように、クラス マップを設定します。
ステップ 5	`Router(config)# policy-map` *policy_map_name*	名前付き QoS ポリシーを作成します。
ステップ 6	`Router(config-pmap)# class` *class_name*	ステップ 3 で作成したクラス マップを使用するように、ポリシーを設定します。
ステップ 7	`Router(config-pmap-c)# police` *bits_per_second* `[`*normal_burst_bytes*`] conform-action transmit exceed-action drop`	ポリシングを設定します。ここでは、次を設定します。 • SLA で指定されたレート制限に準拠するパケットに対して実行するアクション。 • SLA で指定されたレート制限を超えるパケットに対して実行するアクション。
ステップ 8	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 9	`Router(config-if)# mls qos trust dscp`	受信した DSCP を、全ポートの入力トラフィックに対する内部 DSCP 基準値として設定します。
ステップ 10	`Router(config-if)# service-policy input` *policy_map_name*	ステップ 5 で作成したポリシー マップを、入力サービス ポリシーとしてインターフェイスに付加します。

設定例

次に、MPLS EXP フィールドをインポーズ ラベル エントリに設定するようポリシー マップを設定する例を示します。

```
Router(config)# mls qos
Router(config)# access-list 1 permit any
Router(config)# class-map CUSTOMER-A
Router(config-cmap)# match access-group 1
Router(config)# policy-map SLA-A
Router(config-pmap)# class CUSTOMER-A
Router(config-pmap-c)# police 50000000 conform-action transmit exceed-action drop
Router(config)# interface GE-WAN 3/1
Router(config-if)# mls qos trust dscp
Router(config)# interface GE-WAN 3/1.31
Router(config-if)# service-policy input SLA-A
```

入力 PE ルータ - P 方向インターフェイスの設定

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# class-map` *class_name*	パケットがマッピングされる（パケットと一致する）クラス マップを指定します。トラフィック クラスを作成します。
ステップ 3	`Router(config-c-map)# match mpls experimental` *exp_list*	パケットがクラスに属するかを判別するための照合で一致基準として使用される、MPLS EXP フィールド値を指定します。
ステップ 4	`Router(config)# policy-map` *name*	クラスと一致するパケットに QoS ポリシーを設定します。
ステップ 5	`Router(config-p-map)# class` *class_name*	トラフィック クラスとサービス ポリシーを関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth` {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに対する最小帯域幅保証を指定します。最小帯域幅保証は、kbps 単位または帯域幅全体の割合で指定できます。
ステップ 7	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 8	`Router(config-p-map-c)# random-detect`	帯域幅保証のあるトラフィック クラスに対し、WRED 廃棄ポリシーをイネーブルにします。
ステップ 9	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 10	`Router(config-if)# service-policy output` *name*	QoS ポリシーをインターフェイスに付加し、インターフェイスから送信されるパケット上に適用するポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄処理およびスケジューリング処理を行う例を示します。

```
Router(config)# mls qos
Router(config)# class-map MPLS-EXP-3
Router(config-c-map)# match mpls experimental 3
Router(config)# policy-map output-qos
Router(config-p-map)# class MPLS-EXP-3
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface pos 4/1
Router(config-if)# service-policy output output-qos
```

出力 PE ルータの設定 - カスタマー方向インターフェイス

カスタマー方向インターフェイスで出力 PE ルータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	QoS 機能をイネーブルにします。
ステップ 2	`Router(config)# class-map` *class_name*	パケットがマッピングされる（パケットと一致する）クラス マップを指定します。トラフィック クラスを作成します。
ステップ 3	`Router(config-c-map)# match ip precedence` ***precedence-value***	IP precedence 値を一致基準として確認します。
ステップ 4	`Router(config)# policy-map` *name*	クラスと一致するパケットに QoS ポリシーを設定します。
ステップ 5	`Router(config-p-map)# class` *class_name*	トラフィック クラスとサービス ポリシーを関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth` {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに対する最小帯域幅保証を指定します。最小帯域幅保証は、kbps 単位または帯域幅全体の割合で指定できます。
ステップ 7	`Router(config-p-map)# class class-default`	ポリシーを設定または変更できるようにデフォルト クラスを指定します。
ステップ 8	`Router(config-p-map-c)# random-detect`	IP precedence または MPLS EXP フィールド値に基づいて、WRED をポリシーに適用します。
ステップ 9	`Router(config)# interface` *type slot/port*	設定するインターフェイスを選択します。
ステップ 10	`Router(config-if) mpls propagate-cos`	MPLS ドメイン終了 LER 出力ポートで、基本 IP DSCP への EXP 値の伝播機能をイネーブルにします。
ステップ 11	`Router(config-if)# service-policy output` *name*	QoS ポリシーをインターフェイスに付加し、インターフェイスに着信するパケットに適用するポリシーを指定します。

（注）　**bandwidth** コマンドおよび **random-detect** コマンドは、LAN ポートではサポートされません。

設定例

次に、カスタマー方向インターフェイスで出力 PE ルータを設定する例を示します。

```
Router(config)# mls qos
Router(config)# class-map IP-PREC-4
Router(config-c-map)# match ip precedence 4
Router(config)# policy-map output-qos
Router(config-p-map)# class IP-PREC-4
Router(config-p-map-c)# bandwidth percent 40
Router(config-p-map)# class class-default
Router(config-p-map-c)# random-detect
Router(config)# interface GE-WAN 3/2.32
Router(config-if) mpls propagate-cos
Router(config-if)# service-policy output output-qos
```

CHAPTER 43

PFC QoS 統計データ エクスポートの設定

ここでは、Catalyst 6500 シリーズ スイッチに PFC QoS 統計データ エクスポートを設定する方法について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

PFC QoS 統計データ エクスポートの概要

PFC QoS 統計データ エクスポート機能により、LAN ポート別および集約ポリサー別に利用率に関する情報を作成し、UDP パケットに格納して、トラフィックのモニタ、計画、アカウンティング用アプリケーションに転送できます。PFC QoS 統計情報データ エクスポートは、LAN ポート別および集約ポリサー別にイネーブルにできます。ポート別に生成された統計データは、入力パケット数と出力パケット数、およびバイト数で構成されます。集約ポリサー別に生成された統計データは、許可されたパケット数、およびポリシーで設定された速度を超えるパケット数で構成されます。

PFC QoS 統計データは一定の間隔で定期的に収集されますが、データがエクスポートされる間隔を設定できます。Catalyst 6500 シリーズ スイッチに設定されているすべてのポートおよび集約ポリサーに対するデフォルト設定では、PFC QoS 統計の収集はイネーブルに、データ エクスポート機能はディセーブルになっています。

（注） PFC QoS 統計データ エクスポート機能は、NetFlow Data Export（NDE; NetFlow データ エクスポート）から完全に独立していて、相互作用はありません。

PFC QoS 統計データ エクスポートのデフォルト設定

表 43-1 は、PFC QoS 統計データ エクスポートのデフォルト設定を示します。

表 43-1　PFC QoS のデフォルト設定

機能	デフォルト値
PFC QoS データ エクスポート	
グローバルな PFC QoS データ エクスポート	ディセーブル
ポート別の PFC QoS データ エクスポート	ディセーブル
名前付き集約ポリサー別の PFC QoS データ エクスポート	ディセーブル
クラス マップ ポリサー別の PFC QoS データ エクスポート	ディセーブル
PFC QoS データ エクスポート間隔	300 秒
エクスポート先	未設定
PFC QoS データ エクスポート フィールド デリミタ	パイプ文字（|）

PFC QoS 統計データ エクスポートの設定

ここでは、PFC QoS 統計データ エクスポートの設定方法について説明します。

- 「PFC QoS 統計データ エクスポートのグローバルなイネーブル化」（P.43-2）
- 「ポートの PFC QoS 統計データ エクスポートのイネーブル化」（P.43-3）
- 「名前付き集約ポリサーの PFC QoS 統計データ エクスポートのイネーブル化」（P.43-4）
- 「クラス マップの PFC QoS 統計データ エクスポートのイネーブル化」（P.43-5）
- 「PFC QoS 統計データ エクスポート間隔の設定」（P.43-7）
- 「PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポートの設定」（P.43-8）
- 「PFC QoS 統計データ エクスポートのフィールド デリミタの設定」（P.43-10）

PFC QoS 統計データ エクスポートのグローバルなイネーブル化

PFC QoS 統計データ エクスポートをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos statistics-export`	PFC QoS 統計データ エクスポートをグローバルにイネーブルにします。
	`Router(config)# no mls qos statistics-export`	PFC QoS 統計データ エクスポートをグローバルにディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos statistics-export info`	設定を確認します。

次に、PFC QoS 統計データ エクスポートをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export
Router(config)# end
% Warning: Export destination not set.
% Use 'mls qos statistics-export destination' command to configure the export destination
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured
Router#
```

（注） その他の PFC QoS 統計データ エクスポートの設定を有効にするには、PFC QoS 統計データ エクスポートをグローバルにイネーブルにする必要があります。

ポートの PFC QoS 統計データ エクスポートのイネーブル化

特定のポートの PFC QoS 統計データのエクスポートをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos statistics-export`	指定したポートの PFC QoS 統計データ エクスポートをイネーブルにします。
	`Router(config-if)# no mls qos statistics-export`	指定したポートの PFC QoS 統計データ エクスポートをディセーブルにします。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls qos statistics-export info`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/24 で PFC QoS 統計データのエクスポートをイネーブルにし、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos statistics-export
Router(config-if)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24
Router#
```

ポートの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポートされたデータには次に示すフィールドがデリミタ文字で区切られて格納されます。

- エクスポート タイプ（ポートの場合は「1」）
- スロット/ポート
- 入力パケット数
- 入力バイト数
- 出力パケット数
- 出力バイト数
- タイム スタンプ

名前付き集約ポリサーの PFC QoS 統計データ エクスポートのイネーブル化

名前付き集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos statistics-export aggregate-policer` *aggregate_policer_name*	名前付き集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにします。
	`Router(config)# no mls qos statistics-export aggregate-policer` *aggregate_policer_name*	名前付き集約ポリサーの PFC QoS 統計データ エクスポートをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos statistics-export info`	設定を確認します。

次に、aggr1M という名前の集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにして、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M
Router#
```

名前付き集約ポリサーの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポートされたデータには次に示すフィールドがデリミタ文字で区切られて格納されます。

- エクスポート タイプ（集約ポリサーの場合は「3」）
- 集約ポリサー名
- 方向（[in]）
- PFC または DFC スロット番号
- 適合するバイト数
- Committed Information Rate（CIR; 認定情報速度）を超えるバイト数
- Peak Information Rate（PIR; 最大情報レート）を超えるバイト数
- タイム スタンプ

クラス マップの PFC QoS 統計データ エクスポートのイネーブル化

クラス マップの PFC QoS 統計データ エクスポートをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos statistics-export class-map` *classmap_name*	クラス マップの PFC QoS 統計データ エクスポートをイネーブルにします。
	`Router(config)# no mls qos statistics-export class-map` *classmap_name*	クラス マップの PFC QoS 統計データ エクスポートをディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos statistics-export info`	設定を確認します。

次に、class3 という名前のクラス マップの PFC QoS 統計データ エクスポートをイネーブルにして、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export class-map class3
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
Router#
```

クラス マップの PFC QoS 統計データ エクスポートをイネーブルにすると、エクスポート データには次に示すフィールドがデリミタで区切られて格納されます。

- 物理ポートからのデータ：
  - エクスポート タイプ（クラスマップおよびポートの場合は「4」）
  - クラス マップ名
  - 方向（[in]）
  - スロット/ポート
  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ
- VLAN インターフェイスからのデータ：
  - エクスポート タイプ（クラス マップおよび VLAN の場合は「5」）
  - クラス マップ名
  - 方向（[in]）
  - PFC または DFC スロット番号
  - VLAN ID
  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ
- ポート チャネル インターフェイスからのデータ：
  - エクスポート タイプ（クラス マップおよびポート チャネルの場合は「6」）
  - クラス マップ名
  - 方向（[in]）
  - PFC または DFC スロット番号
  - ポート チャネル ID
  - 適合するバイト数
  - CIR を超えるバイト数
  - PIR を超えるバイト数
  - タイム スタンプ

PFC QoS 統計データ エクスポート間隔の設定

PFC QoS 統計データ エクスポートの間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos statistics-export interval` *interval_in_seconds*	PFC QoS 統計データ エクスポートの間隔を設定します。 **（注）** 間隔は、使用している設定内のアクティビティにカウンタ ラップアラウンドが発生しない程度に短くする必要があります。ただし、PFC QoS 統計データ エクスポートを実行するとスイッチにかなりの負荷が発生するため、間隔を小さくするときは注意してください。
	`Router(config)# no mls qos statistics-export interval` *interval_in_seconds*	PFC QoS 統計データ エクスポートの間隔をデフォルト値に戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos statistics-export info`	設定を確認します。

次に、PFC QoS 統計データ エクスポートの間隔を設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export interval 250
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
Router#
```

PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポートの設定

PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos statistics-export destination {host_name | host_ip_address} {port port_number | syslog [facility facility_name] [severity severity_value]}`	PFC QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定します。
	`Router(config)# no mls qos statistics-export destination`	設定された値を消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos statistics-export info`	設定を確認します。

（注）　PFC QoS データ エクスポートの宛先を Syslog サーバにした場合、エクスポート データの先頭に Syslog ヘッダーが付きます。

表 43-2 に、サポートされている PFC QoS データ エクスポート機能と重大度パラメータ値を示します。

表 43-2　サポートされている PFC QoS データ エクスポート機能パラメータ値

名前	定義	名前	定義
kern	カーネル メッセージ	cron	cron/at サブシステム
user	ランダムなユーザレベル メッセージ	local0	ローカルで使用するために予約
mail	メール システム	local1	ローカルで使用するために予約
daemon	システム デーモン	local2	ローカルで使用するために予約
auth	セキュリティ /認証メッセージ	local3	ローカルで使用するために予約
syslog	内部 Syslog メッセージ	local4	ローカルで使用するために予約
lpr	ライン プリンタ サブシステム	local5	ローカルで使用するために予約
news	ネットニュース サブシステム	local6	ローカルで使用するために予約
uucp	uucp サブシステム	local7	ローカルで使用するために予約

表 43-3 に、サポートされている PFC QoS データ エクスポートの重大度パラメータ値を示します。

表 43-3　サポートされている PFC QoS データ エクスポートの重大度パラメータ値

重大度パラメータ		
名前	**番号**	**定義**
emerg	0	システムは使用不能
alert	1	即時対処が必要
crit	2	クリティカル
err	3	エラー
warning	4	警告
notice	5	正常だが重大な状態
info	6	通知
debug	7	デバッグレベル メッセージ

次に、172.20.52.3 を宛先ホストとして、Syslog を UDP ポート番号として設定し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
```

PFC QoS 統計データ エクスポートのフィールド デリミタの設定

PFC QoS 統計データ エクスポートのフィールド デリミタを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos statistics-export delimiter** *delimiter_character*	PFC QoS 統計データ エクスポートのフィールド デリミタを設定します。
	Router(config)# **no mls qos statistics-export delimiter**	PFC QoS 統計データ エクスポートのフィールド デリミタをデフォルト値に戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos statistics-export info**	設定を確認します。

次に、PFC QoS 統計データ エクスポートのフィールド デリミタを設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos statistics-export delimiter ,
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : ,
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
```

CHAPTER 44

Cisco IOS ファイアウォール フィーチャ セットの設定

この章では、Catalyst 6500 シリーズ スイッチで Cisco IOS ファイアウォール フィーチャ セットを設定する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。

Cisco IOS ファイアウォール フィーチャ セットのサポートの概要

ファイアウォール フィーチャ セット イメージは、次の Cisco IOS ファイアウォール機能をサポートします。

- Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）- PFC は、CBAC が MSFC ソフトウェアに適用されている MSFC に対して CBAC を必要とするフローを方向付ける NetFlow テーブルにエントリを追加します。
- 認証プロキシ - MSFC での認証後、PFC は認証ポリシー用の TCAM サポートを提供します。
- Port-to-Application Mapping（PAM; ポート ツー アプリケーション マッピング）- PAM は MSFC のソフトウェアで実行されます。

Cisco IOS ファイアウォール機能については、次のマニュアルを参照してください。

- 『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」の章および次のセクション
  - 次の URL にある「Cisco IOS Firewall Overview」

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scffiwl.htm
  - 次の URL にある「Configuring Context-Based Access Control」

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfcac.htm
  - 次の URL にある「Configuring Authentication Proxy」

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfahp.htm

- 次の URL にある『*Cisco IOS Security Command Reference*』
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

Cisco IOS ファイアウォール イメージを使用するかどうかに関係なく、次の機能がサポートされます。

- 標準アクセス リストおよびスタティック拡張アクセス リスト
- Lock-and-Key（ダイナミックアクセス リスト）
- IP セッション フィルタリング（再帰アクセス リスト）
- TCP インターセプト
- セキュリティ サーバ サポート
- Network Address Translation（NAT; ネットワーク アドレス変換）
- 近接ルータ認証
- イベント ログ機能
- ユーザ認証および許可

（注） Catalyst 6500 シリーズ スイッチは、Intrusion Detection System Module（IDSM）（WS-X6381-IDS）をサポートしています。Catalyst 6500 シリーズ スイッチは、**ip audit** コマンドで設定される Cisco IOS ファイアウォール IDS 機能はサポートしていません。

Cisco IOS ファイアウォールの注意事項および制約事項

Cisco IOS ファイアウォール機能を設定する場合は、次の注意事項および制約事項に従ってください。

- 他のプラットフォームで、特定のポートに関して **ip inspect** コマンドを入力すると、CBAC は、検査されたトラフィックがネットワーク装置を通過できるように、他のポートの Access Control List（ACL; アクセス制御リスト）を変更します。他のポート経由のトラフィックを拒否する ACL で、トラフィックの通過を許可するには、Catalyst 6500 シリーズ スイッチ上で、**mls ip inspect** コマンドを入力する必要があります。詳細については、「追加の CBAC 設定」（P.44-3）を参照してください。
- 再帰 ACL および CBAC には、矛盾するフロー マスク要件があります。再帰 ACL は、MSFC のソフトウェアで処理されます。
- CBAC は VACL と互換性がありません。CBAC および VACL はスイッチ上に設定できますが、同じサブネット（Virtual LAN（VLAN; 仮想 LAN））内には設定できません。

  （注） IDSM は、VACL を使ってトラフィックを選択します。CBAC が設定されているサブネット内で IDSM を使用するには、**mls ip ids** *acl_name* インターフェイス コマンドを入力します。*acl_name* は、IDSM のトラフィックを選択する場合に設定します。

- Microsoft NetMeeting（2.0 以降）のトラフィックを検査するには、**h323** および **tcp** の両方の検査をオンにします。
- Web トラフィックを検査するには、**tcp** 検査をオンにします。パフォーマンスの低下を回避するには、**http** 検査をオフにして、Java をブロックします。
- Quality of Service（QoS; サービス品質）および CBAC は相互に作用したり、干渉したりすることはありません。

- CBAC は、レイヤ 3 インターフェイスとして設定された物理ポート、および VLAN インターフェイスに設定できます。
- 同じインターフェイスに VACL と CBAC を設定することはできません。

追加の CBAC 設定

Catalyst 6500 シリーズ スイッチに、追加の CBAC 設定をする必要があります。Catalyst 6500 シリーズ スイッチ以外のネットワーク装置で、ポートがトラフィックを拒否するように設定されている場合に、CBAC を使用すると、**ip inspect** コマンドで設定されたポートであれば、そのポートを経由してトラフィックを双方向に送信できます。同じ状況が、トラフィックが通過する必要がある別のポートにも適用されます（次の例を参照）。

```
Router(config)# ip inspect name permit_ftp ftp
Router(config)# interface vlan 100
Router(config-if)# ip inspect permit_ftp in
Router(config-if)# ip access-group deny_ftp_a in
Router(config-if)# ip access-group deny_ftp_b out
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# ip access-group deny_ftp_c in
Router(config-if)# ip access-group deny_ftp_d out
Router(config-if)# exit
Router(config)# interface vlan 300
Router(config-if)# ip access-group deny_ftp_e in
Router(config-if)# ip access-group deny_ftp_f out
Router(config-if)# end
```

VLAN 100 で開始した File Transfer Protocol（FTP; ファイル転送プロトコル）セッションを VLAN 200 で終了する必要がある場合、CBAC を使用すると、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_c、および deny_ftp_d を経由して FTP トラフィックを送信できます。VLAN 100 で開始した FTP セッションを VLAN 300 で終了する必要がある場合、CBAC を使用すると、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_e、および deny_ftp_f を経由して FTP トラフィックを送信できます。

Catalyst 6500 シリーズ スイッチのポートがトラフィックを拒否するように設定されている場合、CBAC を使用すると、**ip inspect** コマンドで設定されたポートのみを経由してトラフィックを双方向に送信できます。他のポートは、**mls ip inspect** コマンドを使用して設定する必要があります。

VLAN 100 で開始した FTP セッションを VLAN 200 で終了する必要がある場合、Catalyst 6500 シリーズ スイッチ上で CBAC を使用すると、FTP トラフィックは ACL の deny_ftp_a および deny_ftp_b だけを通過します。ACL の deny_ftp_c および deny_ftp_d をトラフィックが通過するようにするには、次の例のように、**mls ip inspect deny_ftp_c** コマンドおよび **mls ip inspect deny_ftp_d** コマンドを入力する必要があります。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)# mls ip inspect deny_ftp_d
```

VLAN 300 で FTP トラフィックを終了するには、**mls ip inspect deny_ftp_e** および **mls ip inspect deny_ftp_f** コマンドを入力する必要があります。設定を確認するには、**show fm insp** [**detail**] コマンドを入力します。

show fm insp [**detail**] コマンドを実行すると、ACL のリスト、および CBAC が設定されているポートやステータス（**ACTIVE** または **INACTIVE**）が表示されます（次の例を参照）。

```
Router# show fm insp
         interface:Vlan305(in) status :ACTIVE
         acl name:deny
           interfaces:
              Vlan305(out):status ACTIVE
```

VLAN 305 では、着信方向の検査がアクティブで、ACL は設定されていません。VLAN 305 では、ACL **deny** が発信方向に適用されていて、検査がアクティブです。

すべてのフロー情報を表示するには、**detail** キーワードを使用します。

CBAC を設定する前にポートに VACL を設定した場合は、表示されるステータスは INACTIVE となります。それ以外の場合は ACTIVE です。PFC リソースがなくなっている場合にこのコマンドを実行すると、「BRIDGE」と表示され、続いて、処理のために MSFC に送信された NetFlow 要求のうち過去に失敗したが現在アクティブな NetFlow 要求の数が表示されます。

CHAPTER 45

Network Admission Control（NAC）の設定

この章では、Catalyst 6500 シリーズ スイッチで Network Admission Control（NAC）を設定する手順を説明します。PFC3 を使用する場合は、NAC は Release12.2(18)SXF2 以降のリリースでサポートされます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS Master Command List*, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある『*Network Admission Control*』フィーチャ モジュール
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_nac.htm
- 次の URL にある『*Cisco IOS Security Command Reference*』Release 12.3
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/

この章で説明する内容は、次のとおりです。

NAC の概要

ここでは NAC について説明します。

NAC の概要

NAC はシスコの自己防衛型ネットワーク イニシアティブの一部であり、ネットワーク上でのセキュリティ脅威の識別、阻止、および適合に役立ちます。ネットワーク化したビジネス環境において、ワームやウイルスの脅威や影響が強まっています。NAC を使用すると、こうした脅威にネットワーク アクセスを許可する前に、エンドポイントやクライアントのアンチウイルス ステータスを検査および検証できます。

Catalyst 6500 シリーズ スイッチは、NAC によるレイヤ 2 IP 検証をサポートします。NAC レイヤ 2 IP 検証はエッジ スイッチに対して実行されますが、NAC Layer 2 IEEE802.1x とは別の方法によって検証の開始、メッセージ交換、およびポリシーの適用を行います。ホスト PC 上では、LAN ポート IP に対する IEEE802.1x のサポートは必要ありません。NAC をサポートするすべての装置の一覧については、NAC のリリース ノートを参照してください。

（注）
- 特に明記していない限り、*スイッチ*という用語は Catalyst 6500 シリーズ スイッチを意味します。
- Release12.2(18)SXF は、NAC Layer 2 IEEE 802.1x をサポートしません。

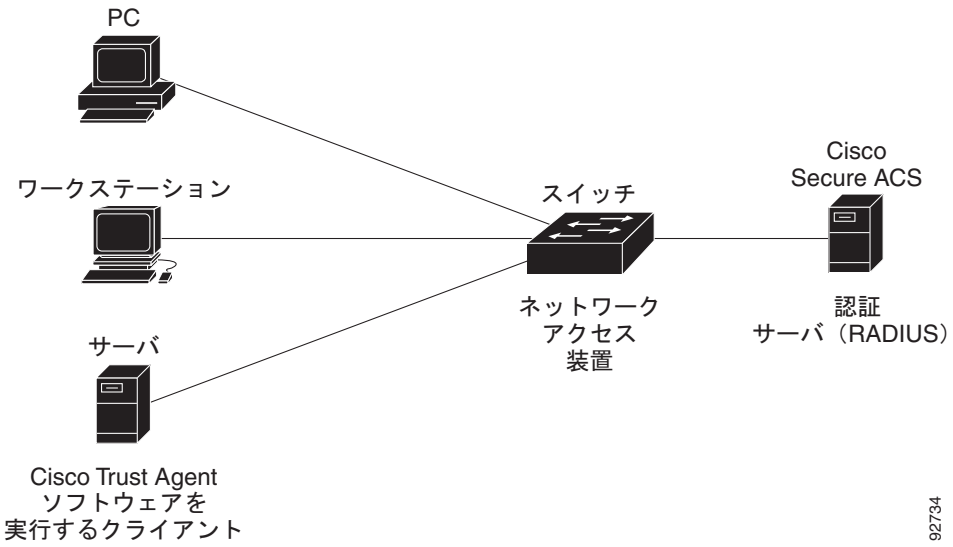
NAC は Catalyst 6500 シリーズ スイッチ上でルーティングされたトラフィックに対し、*ポスチャ検証*を行います。ポスチャ検証を行うことで、ウイルスによるネットワークの被害を低減できます。この機能は、ネットワーク アクセスを要求するネットワーク装置のアンチウイルス クレデンシャルに基づき、ネットワーク アクセスを許可します。このクレデンシャルには、アンチウイルス ソフトウェア、ウイルス定義ファイル、または特定のウイルス スキャン エンジンのバージョンを使用できます。ホストのアンチウイルス クレデンシャルに基づき、要求を行う装置はネットワークへのアクセスを許可または制限されます。

クライアント ホストのクレデンシャル検証が失敗した場合は、*復旧*機能を使用することで、ネットワークへの部分的なアクセスが許可されます。この復旧プロセスにより、クライアント ホストからの HTTP トラフィックは、最新のアンチウイルス ファイルへのアクセスを提供する Web ページの URL にリダイレクトされます。復旧プロセスによって使用される URL は、ネットワーク アクセス ポリシーの一部として定義された復旧サーバのアドレスを解決します。復旧サーバとは、最新のアンチウイルス ファイルが保存されるサーバです。ここから、アンチウイルス ファイルをダウンロードまたはアップグレードできます。

NAC 装置の役割

図 45-1 に示すように NAC を使用する場合、ネットワーク上の各装置は、それぞれ特定の役割を担います。

図 45-1　　ポスチャ検証装置



ネットワーク上で NAC をサポートする装置は、それぞれ次の役割を実行します。

- エンドポイント システムまたはクライアント - PC、ワークステーション、サーバなどのネットワーク上の装置（ホスト）です。直接接続、または IP Phone やワイヤレス アクセス ポイントを経由して、スイッチのアクセス ポートに接続されています。ホストは Cisco Trust Agent ソフトウェアを実行し、LAN へのアクセスおよびスイッチ サービスを要求し、スイッチからの要求に応答します。このエンドポイント システムはウイルス感染元となりうるので、ホストにネットワーク アクセスを許可する前に、そのアンチウイルス ステータスを検証する必要があります。

  Cisco Trust Agent ソフトウェアは、*ポスチャ エージェント*または*アンチウイルス クライアント*とも呼びます。

- スイッチ（エッジ スイッチ）- ネットワーク エッジで、検証サービスの提供とポリシーの適用を行うネットワーク アクセス装置です。また、クライアントのアクセス ポリシーに基づき、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、エンドポイントと認証サーバとの間で Extensible Authentication Protocol（EAP）メッセージをリレーします。

  Catalyst 6500 シリーズ スイッチでは、EAP メッセージ内のカプセル化情報は、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を基にすることができます。UDP を使用する場合は、スイッチは EAP over UDP （EAPoUDP）フレームを使用します。これは EoU フレームと呼ばれることもあります。

- 認証サーバ - 実際のクライアント認証を行う装置です。認証サーバはクライアントのアンチウイルス ステータスを検証し、アクセス ポリシーを決定し、LAN およびスイッチ サービスへのアクセスがクライアントに許可されているかどうかををスイッチに通知します。スイッチはプロキシの役割を果たすため、スイッチと認証サーバ間の EAP メッセージ交換は、スイッチには透過的です。

  このリリースでは、スイッチは Remote Authentication Dial-In User Service（RADIUS）、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）、および EAP 拡張を備えた Cisco Secure Access Control Server（ACS）Version 4.0 以降をサポートします。

  認証サーバは、*ポスチャ サーバ*とも呼ばれます。

AAA ダウン ポリシー

AAA ダウン ポリシーは、AAA サーバが使用できないときであっても、ホストのネットワーク接続を維持するための機能です。NAC の一般的な展開では、Cisco Secure ACS を使用してクライアントの状態（ポスチャ）を検証し、ポリシーを Network Access Device（NAD; ネットワーク アクセス装置）に返します。ポスチャ検証の実行時に AAA サーバが到達不可能になっている場合は、ユーザを拒否する（ネットワークへのアクセスを提供しない）のではなく、管理者はホストに適用可能なデフォルトの AAA ダウン ポリシーを設定できます。

このポリシーには、次のような利点があります。

- AAA が使用不可能である場合、ホストは拒否されることはあっても、ネットワークへの接続は維持できます。
- AAA サーバが再稼動すると、ユーザは再検証を受けることが可能であり、ユーザのポリシーを ACS からダウンロードできます。

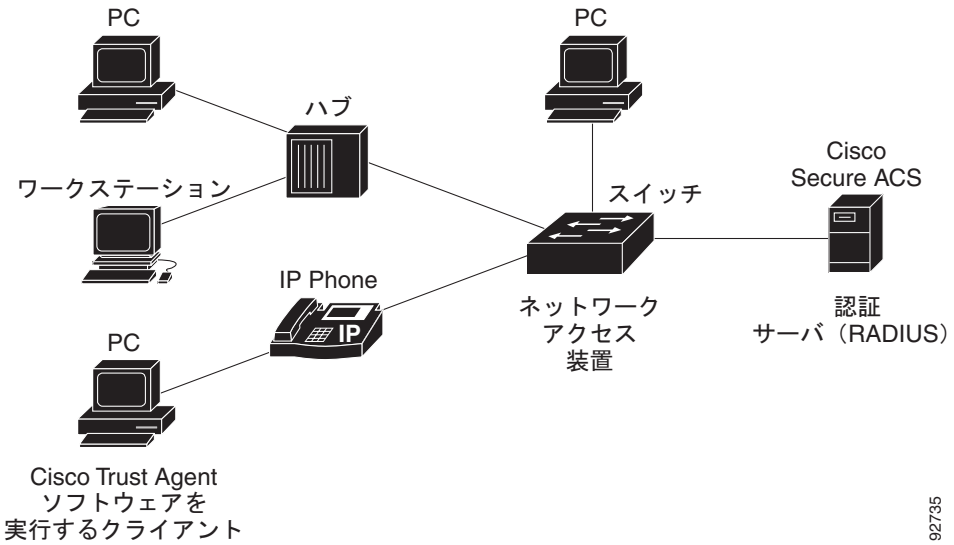
（注）　AAA サーバの停止時には、ホストに他の既存のポリシーが関連付けられていない場合に限り、AAA ダウン ポリシーが適用されます。通常、AAA サーバが停止した場合の再検証時には、ホストに使用されていたポリシーは維持されます。

NAC レイヤ 2 IP 検証

エンドポイント システムまたはクライアントが接続されているエッジ スイッチのアクセス ポートでは、NAC レイヤ 2 IP を使用できます。装置（ホストまたはクライアント）は、PC、ワークステーション、またはサーバです。これらは図 45-2 に示すように、直接接続、または IP Phone やワイヤレス アクセス ポイントを経由して、スイッチのアクセス ポートに接続されています。

NAC レイヤ 2 IP をイネーブルにすると、EAPoUDP は IPv4 トラフィックだけに対して機能します。スイッチはエンドポイント装置またはクライアントのアンチウイルス ステータスを検査して、アクセス制御ポリシーを適用します。

図 45-2　NAC レイヤ 2 IP を使用するネットワーク



ここでは、NAC レイヤ 2 IP 検証について説明します。

- 「ポスチャ検証」（P.45-5）
- 「Cisco Secure ACS と AV ペア」（P.45-7）
- 「監査サーバ」（P.45-8）
- 「ACL」（P.45-9）
- 「NAC タイマー」（P.45-10）
- 「NAC レイヤ 2 IP 検証と冗長スーパーバイザ エンジン」（P.45-12）

ポスチャ検証

NAC レイヤ 2 IP は、図 45-2 に示すように、同一スイッチ ポートに接続された複数のホストのポスチャ検証をサポートします。

ホストが接続されているスイッチ ポートで NAC レイヤ 2 IP 検証をイネーブルにすると、スイッチは Dynamic Host Configuration Protocol（DHCP）スヌーピングおよび Address Resolution Protocol（ARP; アドレス解決プロトコル）スヌーピングを使用して、接続されたホストを識別できるようになります。スイッチは、ARP パケットを受信したあと、または DHCP スヌーピングのバインディング エントリを作成したあとに、ポスチャ検証を開始します。NAC レイヤ 2 IP 検証をイネーブルにすると、接続ホストを検出するデフォルトの手段は ARP スヌーピングとなります。DHCP スヌーピング バインディング エントリの作成時にスイッチがホストを検出するようにするには、DHCP スヌーピングをイネーブルにする必要があります。

DHCP スヌーピングの実行によって開始されたポスチャ検証は、ARP スヌーピングの実行によって開始されるポスチャ検証よりも優先されます。スイッチ ポートに割り当てられたアクセス VLAN で、ダイナミック ARP 検査だけをイネーブルにしている場合は、ARP パケットがダイナミック ARP 検査を通過したときにポスチャ検証が開始されます。ただし、DHCP スヌーピングとダイナミック ARP 検査の両方をイネーブルにしている場合は、DHCP スヌーピング バインディング エントリの作成時に、DHCP によってポスチャ検証が開始されます。

ポスチャ検証が開始されると、スイッチはセッション テーブル内にエントリを作成して、ホストのポスチャ検証ステータスを追跡し、次のプロセスに従って NAC ポリシーを決定します。

1. ホストが例外リスト内に含まれている場合は、スイッチはユーザ設定の NAC ポリシーをこのホストに適用します。
2. EoU バイパスをイネーブルにしている場合は、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをホストに適用します。スイッチは要求の中に RADIUS Attribute-Value（AV; 属性値）ペアを挿入し、この要求が非応答ホストのものであることを指定します。
3. EoU バイパスがディセーブルの場合は、スイッチは EAPoUDP hello パケットをホストに送信し、ホストのアンチウイルス状態を要求します。指定の回数だけ試行してもホストから応答が得られない場合は、スイッチはこのホストをクライアントレスとして分類し、非応答ホストと見なします。スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをホストに適用します。

例外リスト

例外リストには、ローカル プロファイルとポリシー設定が指定されています。アイデンティティ プロファイルは、IP アドレス、Media Access Control（メディア アクセス制御）アドレス、または装置タイプに基づき、装置をスタティックに許可または検証するために使用します。アイデンティティ プロファイルは、アクセス制御属性を指定するローカル ポリシーに関連付けられています。

特定のホストを例外リストに指定し、このホストにユーザ設定ポリシーを適用することで、このホストのポスチャ検証をバイパスできます。EAPoUDP セッション テーブルにエントリが追加されると、スイッチはこのホスト情報を例外リストに照合します。ホストが例外リスト内に含まれている場合は、スイッチは設定された NAC ポリシーをホストに適用します。また、スイッチはクライアントの検証ステータスを POSTURE ESTAB と指定して、EAPoUDP セッション テーブルを更新します。

EoU バイパス

スイッチは EoU バイパス機能を使用することで、Cisco Trust Agent を使用していないホストのポスチャ検証を迅速に行うことができます。EoU バイパスがイネーブルの場合は、スイッチはアンチウイルス ステータスを要求するメッセージをホストに送信しません。代わりに、スイッチは Cisco Secure ACS に対し、このホストの IP アドレス、MAC アドレス、サービス タイプ、および EAPoUDP セッション ID を含めた要求を送信します。Cisco Secure ACS はこのホストに対するアクセス制御を判断し、ポリシーをスイッチに送信します。

EoU バイパスがイネーブルであり、ホストが非応答の場合は、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをこのホストに適用します。

EoU バイパスがイネーブルだと、ホストが Cisco Trust Agent を使用している場合も、スイッチは非応答ホスト要求を Cisco Secure ACS に送信し、サーバからのアクセス ポリシーをホストに適用します。

EAPoUDP セッション

EoU バイパスがディセーブルの場合は、スイッチは EAPoUDP パケットを送信し、ポスチャ検証を開始します。ポスチャ検証の実行中は、スイッチはデフォルトのアクセス ポリシーを適用します。スイッチが EAPoUDP メッセージをホストに送信し、これに対してホストがアンチウイルス状態の要求に応答すると、スイッチはこの EAPoUDP 応答を Cisco Secure ACS に転送します。所定の回数だけ試行してもホストから応答が得られない場合には、スイッチはこのホストを非応答として分類します。ACS がクレデンシャルを確認したあと、認証サーバはポスチャ トークンとポリシー属性を含めた Access-Accept メッセージをスイッチに返します。スイッチは EAPoUDP セッション テーブルを更新し、アクセス制限を適用します。これにより、不適切なポスチャのクライアントを区分および検疫するか、またはネットワーク アクセスを拒否します。

ポスチャ検証の実行中に適用されるポリシーには、次の 2 タイプがあります。

- ホスト ポリシー - このポリシーは、ポスチャ検証の結果に基づいて判断されたアクセス制限を適用する Access Control List（ACL; アクセス制御リスト）を使用します。
- URL リダイレクト ポリシー - このポリシーは、すべての HTTP または HTTPS トラフィックを復旧サーバにリダイレクトする機能を持ちます。これにより、非適合ホストは、適合ホストとなるために必要なアップグレード アクションを実行できます。

（通常は HTTP トラフィックの復旧サーバ宛てのリダイレクトをバイパスする目的で行われる）URL リダイレクトの拒否 Access Control Entry（ACE; アクセス制御エントリ）は、これらの ACE 宛てのトラフィックをハードウェアで転送します。デフォルトのインターフェイス ポリシー、およびダウンロードしたホスト ポリシーは適用されません。このトラフィック（URL リダイレクト の拒否 ACE と一致するトラフィック）をフィルタリングするには、スイッチ ポートのアクセス VLAN で、VLAN ACL を定義する必要があります。

URL リダイレクト ポリシーは、次の要素で構成されます。

- 復旧サーバをポイントする URL
- ホストからのすべての HTTP または HTTPS パケット（復旧サーバ アドレス宛てのものを除く）をキャプチャし、スイッチ ソフトウェアにリダイレクトして、適切な HTTP リダイレクションを実行するためのスイッチ ACL

ホスト ポリシーの ACL 名、リダイレクト URL、および URL リダイレクト ACL は、RADIUS の Attribute-Value オブジェクトを使用して伝送されます。

（注） クライアントに対する DHCP スヌーピング バインディング エントリを削除すると、スイッチはセッション テーブルからのこのクライアントのエントリを削除します。以降は、このクライアントは認証されません。

Cisco Secure ACS と AV ペア

NAC レイヤ 2 IP 検証をイネーブルにすると、Cisco Secure ACS は RADIUS を使用した NAC AAA サービスを提供します。Cisco Secure ACS はエンドポイント システムのアンチウイルス ステータス情報を取得し、エンドポイントのアンチウイルス状態を検証します。

RADIUS の Vendor-Specific Attribute（VSA; ベンダー固有属性）である *cisco-av-pair* を使用すると、Cisco Secure ACS で次の属性値（AV）ペアを設定できます。

- CiscoSecure-Defined-ACL - Cisco Secure ACS 上のダウンロード可能な ACL の名前を指定します。スイッチは ACL 名を、次の形式の CiscoSecure-Defined-ACL AV ペアから取得します。

  #ACL#-IP-*name-number*

  name は ACL の名前、*number* は 3f783768 などのバージョン番号を表します。

  Auth-Proxy ポスチャ コードは、指定のダウンロード可能 ACL のアクセス制御エントリ（ACE）が、以前にダウンロード済みかどうかを調べます。まだダウンロードされていない場合は、Auth-Proxy ポスチャ コードはダウンロード可能 ACL 名をユーザ名として指定した AAA 要求を送信し、この ACE がダウンロードされるようにします。これで、このダウンロード可能 ACL が、名前付き ACL としてスイッチ上に作成されます。この ACL には、送信元アドレスが「any」の ACE が含まれます。リストの最後に暗黙的な deny ステートメントは含まれません。ポスチャ検証の完了後に、ダウンロード可能 ACL がインターフェイスに適用されると、送信元アドレスが「any」からホストの送信元 IP アドレスに変更されます。これらの ACE は、エンドポイント装置が接続されたスイッチ インターフェイスに適用された、ダウンロード可能 ACL に追加されます。トラフィックが CiscoSecure-Defined-ACL ACE に一致すると、適切な NAC アクションが実行されます。

- url-redirect および url-redirect-acl - スイッチ上のローカル URL ポリシーを指定します。スイッチは、これらの cisco-av-pair VSA を次の形式で使用します。
  - url-redirect = <HTTP または HTTPS URL>
  - url-redirect-acl = スイッチ ACL の名前または番号

  これらの AV ペアを使用すると、スイッチはエンドポイント装置からの HTTP または HTTPS 要求を代行受信して、指定のリダイレクト アドレスにクライアントの Web ブラウザを転送します。リダイレクト先のサイトでは、クライアントは最新のアンチウイルス ファイルをダウンロードできます。Cisco Secure ACS の url-redirect AV ペアには、Web ブラウザのリダイレクト先となる URL が含まれます。url-redirect-acl AV ペアは、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号を示します。ACL はスイッチ上に定義しておく必要があります。この結果、リダイレクト ACL 内の許可エントリに一致するトラフィックがリダイレクトされます。

  ホストのポスチャが適切でない場合は、状況に応じてこれらの AV ペアが送信されます。

（注） HTTP または HTTPS トラフィック用に URL をリダイレクトできますが、両方を同時にリダイレクトすることはできません。スイッチまたは HTTP サーバ上の Cisco IOS は、HTTP ポートまたは HTTPS ポートを待ち受けることができますが、両方を同時に待ち受けることはできないためです。

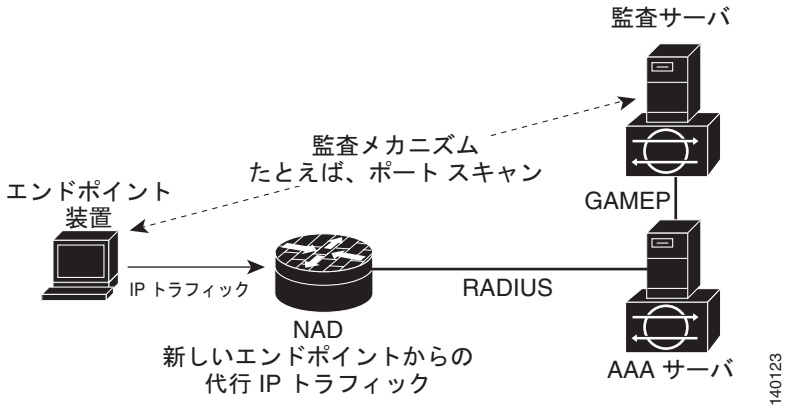
Cisco IOS ソフトウェアのサポートする AV ペアの詳細については、AAA クライアント上で実行されるソフトウェア リリースについての ACS コンフィギュレーションおよびコマンド リファレンス マニュアルを参照してください。

監査サーバ

Cisco Trust Agent（CTA）を実行していないエンド デバイスは、ネットワーク アクセス装置から確認を受けたときに、クレデンシャルを提供できません。このような装置を、*エージェントレス*または*非応答*と表現します。NAC のアーキテクチャは、監査サーバを組み込めるように拡張されています。監査サーバとは、CTA が実装されていないホストのセキュリティ適合性を調査、スキャン、および判別できるサードパーティ製サーバです。監査サーバの検査結果はアクセス サーバに反映させることができるので、すべての非応答ホストに対して共通の制限ポリシーを適用するのではなく、ホスト固有のネットワーク アクセス ポリシーを判断できます。任意のサードパーティ製監査処理を NAC アーキテクチャに統合することで、より堅牢なホスト監査および検査機能を構築できます。

図 45-3 は、一般的なトポロジに監査サーバを組み込む方法を示します。

図 45-3　NAC 装置の役割



このアーキテクチャでは、ホストが監査サーバと通信できるように、監査サーバが到達可能であることを前提としています。ホスト（エンドポイント装置）がポスチャ検査用に設定された NAD を介してネットワーク アクセスを行うと、最終的に NAD は AAA サーバ（Cisco Secure ACS）に対し、このホストに適用するアクセス ポリシーを要求します。AAA サーバは、外部の監査サーバによるホストのスキャンをトリガーするように設定できます。監査サーバによるスキャンは非同期に行われ、完了までに数秒かかることがあります。監査サーバによるスキャンの実行中は、AAA サーバは NAD に対し、適用する最小限の制限セキュリティ ポリシー、および短いポーリング タイマー（セッション タイムアウト）を伝送します。監査サーバから結果が返されるまで、NAD は所定の時間間隔で AAA サーバに対してポーリングを行います。AAA サーバは監査結果を受け取ると、監査結果に基づいてアクセス ポリシーを計算し、次に要求を受けたときに NAD にこのポリシーを送信し、適用を依頼します。

ACL

スイッチ ポートで NAC レイヤ 2 IP 検証を設定する場合は、スイッチ ポートにデフォルトのポート ACL も設定しておく必要があります。また、ポスチャ検証を完了していないホストからの IP トラフィックに対しては、デフォルトの ACL を適用する必要があります。

スイッチにデフォルトの ACL を設定している場合に、Cisco Secure ACS がホストのアクセス ポリシーをスイッチに送信すると、スイッチはスイッチ ポートに接続されたホストからのトラフィックに対し、このポリシーを適用します。ポリシーがトラフィックに適用されると、スイッチはこのトラフィックを転送します。ポリシーがトラフィックに適用されない場合は、スイッチはデフォルトの ACL を適用します。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信した場合に、デフォルト ACL が設定されていないと、NAC レイヤ 2 IP 設定は効力を持ちません。

Cisco Secure ACS がスイッチに対し、ポリシーマップ アクションとしてリダイレクト URL を指定したダウンロード可能 ACL を送信した場合は、スイッチ ポートに設定されたデフォルトの ACL より、このダウンロード可能 ACL の方が優先されます。また、リダイレクト URL ACL ポリシーは、ホストにすでに設定されたポリシーよりも優先されます。スイッチにデフォルトのポート ACL が設定されていない場合であっても、スイッチは Cisco Secure ACS からのダウンロード可能 ACL を適用できます。

NAC タイマー

スイッチは、次のタイマーをサポートします。

ホールド タイマー

ホールド タイマーは、EAPoUDP セッションを検証しようとする試みが失敗したあとに、次の新規セッションがすぐに開始されないように抑制します。このタイマーは、Cisco Secure ACS がスイッチに Accept-Reject メッセージを送信した場合だけに使用されます。

ホールド タイマーのデフォルト値は 180 秒（3 分）です。

EAPoUDP セッションの検証が失敗するのは、ホストのポスチャ検証が失敗した場合、セッション タイマーが満了した場合、スイッチまたは Cisco Secure ACS が無効なメッセージを受信した場合などです。スイッチまたは認証サーバが無効なメッセージを連続して受信する場合は、悪意あるユーザが Denial of Service（DoS; サービス拒絶）攻撃を仕掛けようとしている可能性もあります。

アイドル タイマー

アイドル タイマーは、ポスチャ検証を行っているホストから ARP パケットが送信されるまで、または IP 装置追跡テーブル内のエントリが更新されるまでの待機時間を制御し、ホストが接続されているかどうかを確認します。アイドル タイマーは既知のホスト リストを使用して、ポスチャ検証を開始したホスト、および IP 装置追跡テーブルを追跡します。

アイドル タイマーは、スイッチが ARP パケットを受信した時点、または IP 装置追跡テーブル内のエントリが更新された時点でリセットされます。アイドル タイマーが満了すると、スイッチはこのホストに対する EAPoUDP セッションを終了し、このホストは検証されなくなります。

アイドル タイマーのデフォルト値は、プローブの実行間隔に、プローブの再試行数を掛けた値として計算されます。デフォルトでは、アイドル タイマーのデフォルト値は 90 秒であり、これはプローブの実行間隔である 30 秒に、プローブの再試行数 3 を掛けた値です。

スイッチは既知のホスト リストを維持し、ポスチャ検証を開始したホストを追跡します。スイッチは ARP パケットを受信すると、このリストのエージング タイマー、およびアイドル タイマーをリセットします。リストのエージング時間が満了すると、スイッチは ARP プローブを送信し、このホストが存在するかどうかを確認します。ホストが存在する場合は、ホストはスイッチに対して応答メッセージを送信します。スイッチはこれを受け、既知のホスト リストの該当エントリを更新します。さらに、リストのエージング タイマーおよびアイドル タイマーをリセットします。応答がない場合は、スイッチは Cisco Secure ACS とのセッションを終了し、このホストの検証も中止されます。

スイッチは IP 装置追跡テーブルを使用して、スイッチに接続されているホストを検出および管理します。また、ホストの検出には ARP または DHCP スヌーピングも使用されます。デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。NAC レイヤ 2 IP 検証を使用するには、IP 装置追跡機能をイネーブルにする必要があります。

IP 装置追跡をイネーブルにした場合、ホストが検出されると、スイッチは IP 装置追跡テーブルにエントリを追加します。このエントリには、次の情報が含まれます。

- ホストの IP および MAC アドレス
- スイッチがホストを検出したインターフェイス
- ホストの検出時に ACTIVE に設定されるホスト状態

インターフェイスで NAC レイヤ 2 IP 検証をイネーブルにしている場合は、IP 装置追跡テーブルにエントリが追加されると、ポスチャ検証が開始されます。

IP 装置追跡テーブルでは、テーブルからエントリを削除する前に、スイッチがこのエントリに対して ARP プローブを送信する回数を設定できます。また、スイッチが ARP プローブを再送信するまでの待機時間（秒単位）も設定できます。IP 装置追跡テーブルのデフォルト設定を使用する場合は、スイッチはすべてのエントリに対し、30 秒おきに ARP プローブを送信します。ホストがプローブに応答すると、このホストの状態が更新され、アクティブの状態で維持されます。応答がない場合、スイッチはさらに 3 つの ARP プローブを 30 秒おきに送信できます。スイッチは最大数の ARP プローブを送信したあと、テーブルからこのホスト エントリを削除します。EAPoUDP セッションがセットアップされている場合は、スイッチはこのホストのセッションを終了します。

IP 装置追跡を行うことで、DHCP の限界を克服し、ホストをタイムリーに検出できます。リンクが停止した場合は、このインターフェイスに関連付けられた IP 装置追跡エントリは削除されず、これらのエントリの状態は非アクティブに変わります。IP 装置追跡テーブル内のエントリ数に制限はありませんが、非アクティブ エントリを削除するための上限が適用されます。この上限値を超えない限り、すべてのエントリは IP 装置追跡テーブル内に維持されます。非アクティブ エントリの削除が開始される上限に達した場合は、非アクティブ エントリが含まれるテーブルに新たなエントリが追加されると、スイッチは非アクティブ エントリを削除します。テーブル内に非アクティブ エントリが含まれない場合は、IP 装置追跡テーブル内のエントリ数は単純に増加します。ホストが*非アクティブ*になると、スイッチはこのホスト セッションを終了します。Catalyst 3750、3560、3550、2970、2960、2955、2950、2940 スイッチ、および Cisco EtherSwitch サービス モジュールでは、非アクティブ エントリが削除されるまでの上限値は 512 です。Cisco 7600 シリーズ ルータ、および Catalyst 4000/6000 スイッチでは、この上限値は 2048 です。

インターフェイス リンクが復元されると、スイッチはこのインターフェイスに関連付けられたエントリに対して ARP プローブを送信します。ARP プローブに応答しないホストのエントリは期限切れとなります。スイッチは、応答のあったホストの状態をアクティブに変更し、ポスチャ検証を開始します。

再送信タイマー

再送信タイマーは、ポスチャ検証の実行中に、スイッチが要求を再送信する前にクライアントからの応答を待機する時間を制御します。このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くなる可能性があります。

再送信タイマーのデフォルト値は 3 秒です。

再検証タイマー

再検証タイマーは、ポスチャ検証の実行中に EAPoUDP メッセージを使用していたクライアントに対し、NAC ポリシーが適用される期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。ホストが再検証されると、このタイマーはリセットされます。再検証タイマーのデフォルト値は 36000 秒（10 時間）です。

スイッチに再検証タイマーの値を指定するには、**eou timeout revalidation** *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。また、インターフェイスに再検証タイマーの値を指定するには、**eou timeout revalidation** *seconds* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　再検証タイマーはスイッチ上でローカルに設定することも、コントロール サーバからダウンロードすることもできます。

再検証タイマーは、AAA を実行する Cisco Secure ACS からの Access-Accept メッセージに含まれる Session-Timeout RADIUS 属性（属性 [27]）、および Termination-Action RADIUS 属性（属性 [29]）に基づいて動作します。スイッチが Session-Timeout 値を受信した場合は、この値はスイッチ上の再検証タイマー値よりも優先されます。

再検証タイマーが満了した場合のスイッチのアクションは、次の Termination-Action 属性値のいずれかに応じて異なります。

- Termination-Action RADIUS 属性値がデフォルト値の場合は、セッションは終了します。
- スイッチが受信した Termination-Action 属性値がデフォルト以外の場合は、ポスチャ検証の実行中、EAPoUDP セッションおよび現在のアクセス ポリシーは有効な状態を維持します。
- Termination-Action 属性値が RADIUS の場合は、スイッチはクライアントを再検証します。
- サーバからのパケットに Termination-Action 属性が含まれない場合は、EAPoUDP セッションは終了します。

ステータス クエリー タイマー

ステータス クエリー タイマーは、以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、スイッチの待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。ステータス クエリー タイマーのデフォルト値は 300 秒（5 分）です。

ホストが再認証されると、このタイマーはリセットされます。このタイマーが満了すると、スイッチはホストに Status-Query メッセージを送信して、ホストのポスチャ検証の状態を確認します。スイッチは、ホストからポスチャが変更されたことを示すメッセージを受信すると、ホストのポスチャを再検証します。

NAC レイヤ 2 IP 検証と冗長スーパーバイザ エンジン

冗長スーパーバイザ エンジンを搭載した Catalyst 6500 シリーズ スイッチでは、Route Processor Redundancy（RPR）モードの冗長性を設定している場合、スイッチオーバーの発生時に、現在ポスチャを検証されているホストの情報がすべて失われます。SSO モードの冗長性を設定している場合は、スイッチオーバーが発生すると、現在ポスチャを検証されているホストはすべて、ポスチャを再検証されます。

NAC レイヤ 2 IP 検証と冗長モジュラ型スイッチ

RPR モードの冗長性を設定している場合は、スイッチオーバーが発生すると、現在ポスチャを検証されているホストの情報がすべて失われます。SSO モードの冗長性を設定している場合は、スイッチオーバーが発生すると、現在ポスチャを検証されているホストはすべて、ポスチャを再検証されます。

NAC レイヤ 2 IP 検証での AAA ダウン ポリシー

AAA ダウン ポリシー機能とともに使用すると、検証プロセスは次の順序で行われます。

1. 新規セッションが検出されます。
2. ポスチャ検証がトリガーされる前に、AAA サーバが到達不可能な場合は、AAA ダウン ポリシーが適用され、セッション状態は AAA DOWN として維持されます。
3. AAA サーバが再度利用可能になると、ホストに対する再検証が再度トリガーされます。

（注）　AAA サーバの停止時には、ホストに他の既存のポリシーが関連付けられていない場合に限り、AAA ダウン ポリシーが適用されます。AAA サーバが停止した場合の再検証時には、ホストに使用されていたポリシーは維持されます。

NAC の設定

ここでは、次の設定情報について説明します。

NAC のデフォルト設定

デフォルトでは、NAC レイヤ 2 IP 検証はディセーブルにされています。

NAC レイヤ 2 IP 検証に関する注意事項、制限事項、および制約事項

NAC レイヤ 2 IP 検証を設定する場合、次の注意事項、制限事項、および制約事項に従ってください。

- レイヤ 2 IP 検証が正しく実行されるには、スイッチからホストへのレイヤ 3 ルートを設定する必要があります。
- ポートの親 VLAN に VLAN Access Control List（VACL; VLAN アクセス制御リスト）キャプチャまたは Cisco IOS ファイアウォール（CBAC）が設定されている場合は、レイヤ 2 IP 検証は実行されません。
- CPU にリダイレクトされた LAN Port IP（LPIP; LAN ポート IP）ARP トラフィックは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能によってスパニングされません。
- NAC レイヤ 2 IP 検証は、トランク ポート、トンネル ポート、EtherChannel メンバ、またはルーティングされたポートではサポートされません。Catalyst 6500 シリーズ スイッチは、EtherChannel 上でレイヤ 2 IP をサポートします。
- NAC レイヤ 2 IP 検証をイネーブルにしている場合は、ホストが接続されたスイッチ ポート上で ACL を設定する必要があります。
- LPIP が正しく動作するためには、EAPoUDP トラフィックが ACL によって許可される必要があります。

- NAC レイヤ 2 IP 検証では、IPv6 トラフィックのポスチャは検証されず、IPv6 トラフィックにはアクセス ポリシーは適用されません。
- スイッチ ポートがプライベート VLAN の一部である場合は、NAC レイヤ 2 IP はサポートされません。
- CPU にリダイレクトされた NAC レイヤ 2 IP ARP トラフィックは、SPAN 機能によってスパニングされません。
- 送信元 IP アドレスの異なる大量の ARP パケットがスイッチに送信される場合は、サービス拒絶攻撃が行われている可能性があります。この問題を回避するには、**mls rate-limit layer2 ip-admission** コマンドを使用して、IP アドミッション MLS レート制限機能を設定する必要があります。
- スイッチ ポートの親 VLAN 上で Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）もイネーブルにされている場合は、CPU に転送される ARP パケットの IP アドミッション レート制限は無効になります。この状況では、ARP 検査によるレート制限が機能します。ARP 検査によるレート制限はソフトウェアで行われ、IP アドミッション レート制限はハードウェアで行われます。
- スイッチで DHCP リース許可を使用して接続ホストを識別するには、DHCP スヌーピングをイネーブルにする必要があります。DHCP 環境では、DHCP パケットはデフォルト インターフェイス、およびダウンロードされたホスト ポリシーの両方で許可されます。
- ポスチャ検証が行われる前に、エンド ステーションが Domain Name System（DNS; ドメイン ネーム システム）要求を送信できるようにするには、スイッチ ポート上で名前付きのダウンロード可能 ACL を設定し、ACE で DNS パケットを許可する必要があります。
- エンドポイント装置からの HTTP および HTTPS 要求を指定の URL に転送するには、HTTP サーバ機能をイネーブルにする必要があります。url-redirect-acl AV ペアを、URL ACL 名として定義してください。この ACL には、**deny tcp any** *remediation server address* **eq www** コマンドに続けて、リダイレクトする HTTP トラフィックに対する許可 ACE を指定する必要があります。
- 音声 VLAN に属するスイッチ ポートに NAC レイヤ 2 IP 検証が設定されている場合は、このスイッチは IP Phone のポスチャを検証しません。IP Phone が例外リストに指定されていることを確認してください。
- NAC レイヤ 2 IP 検証がイネーブルにされている場合は、入力インターフェイス上に設定されている VLAN ACL およびルータ ACL より、NAC レイヤ 2 IP 設定の方が優先されます。たとえば、VLAN ACL とルータ ACL が設定されている場合は、各ポリシーは LPIP ポリシー、VLAN ACL、ルータ ACL の順に 1 つずつ適用されます。次のポリシーは、トラフィックが 1 つ前のポリシー検査を通過した場合にのみ適用されます。順次適用されるポリシーのいずれかでトラフィックが拒否された場合は、このトラフィックはアクセスを拒否されます。ダウンロードされた LPIP ホスト ポリシーは、デフォルトのインターフェイス ポリシーを常に上書きします。
- DHCP スヌーピングが正しく動作するには、インターフェイスのデフォルト ACL およびホスト ポリシーで DHCP トラフィックが許可される必要があります。
- 入力 VLAN でダイナミック ARP 検査をイネーブルにしている場合は、ARP パケットの検証後のみにポスチャ検証が開始されます。
- URL リダイレクトの拒否 ACE に送信されたトラフィックは、ハードウェアで転送され、デフォルト インターフェイス ポリシーおよびダウンロードされたホスト ポリシーは適用されません。このトラフィック（URL リダイレクト の拒否 ACE と一致するトラフィック）をフィルタリングするには、スイッチ ポートのアクセス VLAN で、VLAN ACL を定義する必要があります。このように設定することで、復旧サーバ宛ての HTTP トラフィックのリダイレクションをバイパスできます。

NAC レイヤ 2 IP 検証の設定

NAC レイヤ 2 IP 検証を設定するには、イネーブル EXEC モードで、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip admission name` *rule_name* `eapoudp`	ルール名を指定して、IP NAC ルールを作成および設定します。 IP NAC ルールをスイッチから削除するには、**no ip admission name** *rule-name* **eapoudp** グローバル 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 3	`Router(config)# mls ratelimit layer2 ip ip-admission` *pps* (*burst*)	CPU 宛ての IP アドミッション トラフィックのレート制限をイネーブルにします。
ステップ 4	`Router(config)# access-list` *access_list_number* {**deny** | **permit**} *source* [*source_wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して、ACL を定義します。 *access_list_number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、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であり、次の形式で指定されます。 • 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* 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。*source_wildcard* を入力する必要はありません。 • *source*、および source-wildcard **source** 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source_wildcard* を指定すると、ワイルドカード ビットが送信元アドレスに適用されます。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 5	`Router(config)# interface` *interface_id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	`Router(config)# ip access-group` {*access_list_number* | *name*} **in**	指定のインターフェイス宛てのアクセスを制御します。
ステップ 7	`Router(config)# ip admission name` *rule_name*	指定の IP NAC ルールをインターフェイスに適用します。 指定のインターフェイスに適用された IP NAC ルールを削除するには、**no ip admission** *rule-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。

	コマンド	目的
ステップ 8	`Router(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 10	`Router(config)# aaa authentication eou default group radius`	EAPoUDP の認証方法を設定します。 EAPoUDP 認証方法を削除するには、**no aaa authentication eou 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。
ステップ 11	`Router(config)# ip device tracking`	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡テーブルをディセーブルにするには、**no 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 12	`Router(config)# ip device tracking probe {count` *count* `|` `interval` *interval*`}`	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **count** *count* - スイッチが ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **interval** *interval* - スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。
ステップ 13	`Router(config)# radius-server host {`*hostname* `|` *ip_address*`} key` *string*	（任意）RADIUS サーバの各パラメータを設定します。 *hostname* | *ip_address* 値には、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。 **key** *string* 値には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチ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）** 鍵は、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、鍵のストリング内または末尾のスペースは使用されるためです。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。鍵は RADIUS デーモンで使用する暗号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は、このコマンドを再度入力します。
ステップ 14	`Router(config)# radius-server attribute 8 include-in-access-req`	スイッチが非応答ホストに接続されている場合は、アクセス要求パケットまたはアカウンティング要求パケット内で、Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。
ステップ 15	`Router(config)# radius-server vsa send authentication`	VSA を認識および使用するようにネットワーク アクセス サーバを設定します。

	コマンド	目的
ステップ 16	`Router(config)# ip device tracking [probe {count count | interval interval}]`	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **probe count** *count* - IP 装置追跡テーブルからエントリを削除する前に、スイッチがエントリに対する ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **probe interval** *interval* - スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。
ステップ 17	`Router(config)# eou logging`	（任意）EAPoUDP システム ロギング イベントをイネーブルにします。
ステップ 18	`end`	イネーブル EXEC モードに戻ります。
ステップ 19	`Router# show ip admission {[cache] [configuration] [eapoudp]}`	NAC 設定またはネットワーク アドミッション キャッシュ エントリを表示します。
ステップ 20	`Router# show ip device tracking {all | interface interface_id | ip ip_address | mac mac_address}`	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 21	`Router# show ip access lists interface interface`	Cisco IOS ソフトウェアの設定において、ダウンロードされたホスト ポリシーを表示します。
ステップ 22	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

IP NAC ルールをスイッチから削除するには、**no ip admission name** *rule_name* **eapoudp** グローバル コンフィギュレーション コマンドを使用します。指定のインターフェイスに適用された IP NAC ルールを削除するには、**no ip admission** *admission_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。

EAPoUDP 認証方法を削除するには、**no aaa authentication eou 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。AAA サーバからセキュリティ アソシエーションを取得しないように auth-proxy ポスチャ コードを設定するには、**no aaa authorization auth-proxy 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。

IP 装置追跡テーブルをディセーブルにし、テーブルの各パラメータをデフォルト値に戻すには、**no device tracking** および **no device tracking probe** {**count** | **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。

Framed-IP-Address 属性を送信しないようにスイッチを設定するには、**no radius-server attribute 8 include-in-access-req** グローバル コンフィギュレーション コマンドを使用します。

EAPoUDP システム イベントのロギングをディセーブルにするには、**no eou logging** グローバル コンフィギュレーション コマンドを使用します。

スイッチまたは指定のインターフェイスから、すべての NAC クライアント装置エントリを消去するには、**clear eou** イネーブル EXEC コマンドを使用します。IP 装置追跡テーブル内のエントリを消去するには、**clear ip device tracking** イネーブル EXEC コマンドを使用します。

次に、スイッチ インターフェイス上で NAC レイヤ 2 IP 検証を設定する例を示します。

```
Router# configure terminal
Router(config)# ip admission nac eapoudp
Router(config)# access-list 5 permit any any
Router(config)# interface gigabitethernet 2/0/1
Router(config-if)# ip access-group 5 in
Router(config-if)# ip admission name nac
Router(config-if)# exit
Router(config)# aaa new-model
Router(config)# aaa authentication eou default group radius
Router(config)# radius-server host admin key rad123
Router(config)# radius-server vsa send authentication
Router(config)# ip device tracking probe count 2
Router(config)# eou logging
Router(config)# end
```

EAPoUDP の設定

EAPoUDP を設定するには、イネーブル EXEC モードから開始して、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	`Router(config)# eou allow {clientless | ip-station-id}`
	`eou default`
	`eou logging`
	`eou max-retry number`
	`eou port port_number`
	`eou ratelimit number`
	`eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status-query seconds}`
	`eou revalidate`
		EAPoUDP 値を指定します。
		allow、**default**、**logging**、**max-retry**、**port**、**rate-limit**、**revalidate**、および **timeout** の各キーワードの詳細については、このリリースおよび『*Network Admission Control*』フィーチャ モジュールのコマンド リファレンスを参照してください。

ステップ 3	`Router(config)# interface interface_id`	インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	`Router(config)# eou default`
	`eou max-retry number`
	`eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status-query seconds}`
	`eou revalidate`
		指定のインターフェイスに対し、EAPoUDP の関連付けをイネーブル化および設定します。
		default、**max-retry**、**revalidate**、および **timeout** の各キーワードの詳細については、このリリースおよび『*Network Admission Control*』フィーチャ モジュールのコマンド リファレンスを参照してください。

ステップ 5	`end`	イネーブル EXEC モードに戻ります。
ステップ 6	`Router# show eou {all | authentication {clientless | eap | static} | interface interface_id | ip ip_address | mac mac_address | posturetoken name}`	EAPoUDP 設定またはセッション キャッシュ エントリについての情報を表示します。
ステップ 7	`Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

グローバルなデフォルトの EAPoUDP 値に戻すには、**eou** グローバル コンフィギュレーション コマンドの **no** 形式を使用します。EAPoUDP 関連付けをディセーブルにするには、**eou** インターフェイス コンフィギュレーション コマンドの **no** 形式を使用します。

アイデンティティ プロファイルおよびアイデンティティ ポリシーの設定

アイデンティティ プロファイルおよびアイデンティティ ポリシーを設定するには、イネーブル EXEC モードから開始して、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Router(config)# **identity policy** *policy_name*	アイデンティティ ポリシーを作成し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
ステップ 3	Router(config-identity-policy)# **access-group** *access_group*	アイデンティティ ポリシーに対するネットワーク アクセス属性を定義します。
ステップ 4	Router(config)# **identity profile eapoudp**	アイデンティティ プロファイルを作成し、アイデンティティ 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。
ステップ 5	Router(config-identity-prof)# **device** {**authorize** | **not-authorize**} {**ip-address** *ip_address* | **mac-address** *mac_address* | **type cisco ip phone**} [**policy** *policy_name*]	指定の IP 装置を許可し、この装置に指定のポリシーを適用します。
ステップ 6	Router(config)# **exit**	アイデンティティ プロファイル 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 7	Router# **end**	イネーブル EXEC モードに戻ります。
ステップ 8	Router# **show running-config**	設定を確認します。
ステップ 9	Router# **copy running-config startup-config**	（任意）エントリをコンフィギュレーション ファイルに保存します。

スイッチからアイデンティティ ポリシーを削除するには、**no identity-policy** *policy_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。アイデンティティ プロファイルを削除するには、**no identity profile eapoudp** グローバル コンフィギュレーション コマンドを使用します。指定の IP 装置を許可しないようにし、この装置から指定のポリシーを削除するには、**no device** {**authorize** | **not-authorize**} {**ip-address** *ip_address* | **mac-address** *mac_address* | **type cisco ip phone**} [**policy** *policy_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、アイデンティティ プロファイルおよびアイデンティティ ポリシーを設定する例を示します。

```
Router# configure terminal
Router(config)# identity policy policy1
Router(config-identity-policy)# access-group group1
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip address 10.10.142.25 policy policy1
Router(config-identity-prof)# exit
Router(config)# end
```

NAC AAA ダウン ポリシーの設定

（注）　この機能は、Catalyst 6500 シリーズ スイッチおよび Catalyst 7600 ルータのみで使用できます。

NAC AAA ダウン ポリシーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip admission name` *rule-name* `eapoudp event timeout aaa policy identity` *identity_policy_name*	NAC ルールを作成し、AAA サーバが到達不可能な場合にセッションに適用するアイデンティティ ポリシーを関連付けます。 ルールをスイッチから削除するには、**no ip admission name** *rule-name* **eapoudp event timeout aaa policy identity** グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	`Router(config)# access-list` *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 *access-list-number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、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であり、次の形式で指定されます。 • 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* 値 0.0.0.0 255.255.255.255 の略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 *source* 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source-wildcard* を使用して、ワイルドカード ビットを送信元アドレスに適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 4	`Router(config-if)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	`Router(config-if)# ip access-group` {*access-list-number* | *name*} **in**	指定のインターフェイス宛てのアクセスを制御します。

	コマンド	目的
ステップ 6	`Router(config-if)# ip admission name rule-name`	指定の IP NAC ルールをインターフェイスに適用します。 指定のインターフェイスに適用された IP NAC ルールを削除するには、**no ip admission** *rule-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。
ステップ 7	`Router(config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 9	`Router(config)# aaa authentication eou default group radius`	EAPoUDP の認証方法を設定します。 EAPoUDP 認証方法を削除するには、**no aaa authentication eou 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。
ステップ 10	`Router(config)# aaa authorization network default local`	認証方法をローカルに設定します。認証方法を削除するには、**no aaa authorization network default local** コマンドを使用します。
ステップ 11	`Router(config)# ip device tracking`	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡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 12	`Router(config)# ip device tracking [probe {count count | interval interval}]`	（任意）IP 装置追跡テーブルに対し、次のパラメータを設定します。 • **count** *count* - スイッチが ARP プローブを送信する回数を設定します。有効値の範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **interval** *interval* - スイッチが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効値の範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。

	コマンド	目的
ステップ 13	`Router(config)# radius-server host {hostname | ip-address} test username username idle-time 1 key string`	（任意）RADIUS サーバの各パラメータを設定します。 *hostname* または *ip-address* 値には、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。 **key** *string* 値には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチ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）** 鍵は、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、鍵のストリング内または末尾のスペースは使用されるためです。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。鍵は RADIUS デーモンで使用する暗号に一致している必要があります。 **test username** パラメータは、AAA サーバがアクティブかどうかをテストするための、ダミーのユーザ名の設定に使用します。 **idle-time** パラメータは、サーバの動作ステータスを確認するために行うサーバ テストの実行頻度を設定します。RADIUS サーバへのトラフィックがない場合は、NAD はこの idle-time 値に基づき、RADIUS サーバにダミーの RADIUS パケットを送信します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 14	`Router(config)# radius-server attribute 8 include-in-access-req`	（任意）スイッチが非応答ホストに接続されている場合に、アクセス要求パケットまたはアカウンティング要求パケット内で、Framed-IP-Address RADIUS 属性（属性 [8]）を送信するようにスイッチを設定します。 Framed-IP-Address 属性を送信しないようにスイッチを設定するには、**no radius-server attribute 8 include-in-access-req** グローバル 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 15	`Router(config)# radius-server vsa send authentication`	VSA を認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 16	`Router(config)# radius-server dead-criteria {tries | time} value`	1 つまたは両方の基準値（RADIUS サーバを停止状態としてマーキングするために使用）を、指定の定数値に強制的に設定します。
ステップ 17	`Router(config)# eou logging`	（任意）EAPoUDP システム ロギング イベントをイネーブルにします。 EAPoUDP システム イベントのロギングをディセーブルにするには、**no eou logging** グローバル コンフィギュレーション コマンドを使用します。

	コマンド	目的
ステップ 18	Router(config)# **end**	イネーブル EXEC モードに戻ります。
ステップ 19	Router# **show ip admission** {[**cache**] [**configuration**] [**eapoudp**]}	NAC 設定またはネットワーク アドミッション キャッシュ エントリを表示します。
ステップ 20	Router# **show ip device tracking** {**all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 21	Router(# **copy running-config startup-config**	（任意）エントリをコンフィギュレーション ファイルに保存します。

次に、AAA ダウン ポリシーを適用する例を示します。

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Router(config)# aaa new-model
Router(config)# aaa authorization network default local
Router(config)# aaa authentication eou default group radius
Router(config)# identity policy global_policy
Router(config-identity-policy)# ac
Router(config-identity-policy)# access-group global_acl
Router(config)# ip access-list extended global_acl
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# radius-server host 40.0.0.4 test username administrator idle-time 1 key
cisco
Router(config)# radius-server dead-criteria tries 3
Router(config)# radius-server vsa send authentication
Router(config)# radius-server attribute 8 include-in-access-req
Router(config)# int fastEthernet 2/13
Router(config-if)# ip admission AAA_DOWN
Router(config-if)# exit
Router# show ip admission configuration

Show running output
-------------------
aaa new-model
aaa authentication eou default group radius
aaa authorization network default local

ip admission name AAA_DOWN eapoudp event timeout aaa policy identity global_policy


identity policy global_policy
 access-group global_acl

interface FastEthernet2/13
 switchport
 switchport access vlan 222
 switchport mode access
 no ip address
 ip access-group 115 in
 ip admission AAA_DOWN
!
ip access-list extended global_acl
 permit ip any any
```

```
radius-server dead-criteria tries 3
radius-server attribute 8 include-in-access-req
radius-server host 40.0.0.4 auth-port 1645 acct-port 1646 test username administrator
idle-time 1 key cisco
radius-server vsa send authentication


Router# show ip admission configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Auth-proxy name AAA_DOWN
   eapoudp list not specified auth-cache-time 60 minutes
   Identity policy name global_policy for AAA fail policy
```

NAC のモニタおよびメンテナンス

ここでは、NAC をモニタおよびメンテナンスするために行う作業について説明します。

- 「テーブル エントリの消去」（P.45-24）
- 「NAC 情報の表示」（P.45-24）

テーブル エントリの消去

EAPoUDP セッション テーブル内のクライアント エントリを消去するには、**clear eou** イネーブル EXEC コマンドを使用します。エントリの削除後、新たにエントリが作成されるのは、スイッチがホストから ARP パケットを受信したあと、またはスイッチがホストに対する DHCP バインディング エントリを作成したあとのみです。

スイッチの IP 装置追跡テーブル内のエントリを消去するには、**clear ip device tracking** イネーブル EXEC コマンドを使用します。

NAC 情報の表示

NAC 情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
Router# **show dot1x** [**all** | **interface** *interface_id* | **statistics interface** *interface_id*]	IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示します。
Router# **show eou** {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface_id* | **ip** *ip_address* | **mac** *mac_address* | **posturetoken** *name*}	EAPoUDP 設定またはセッション キャッシュ エントリについての情報を表示します。
Router# **show ip admission** {[**cache**] [**configuration**] [**eapoudp**]}	NAC 設定またはネットワーク アドミッション キャッシュ エントリを表示します。
Router# **show ip device tracking** {**all** | **interface** *interface_id* | **ip** *ip_address* | **mac** *mac_address*}	IP 装置追跡テーブル内の各エントリの情報を表示します。

CHAPTER 46

IEEE 802.1X ポートベースの認証の設定

この章では、許可されていない装置（クライアント）がネットワークにアクセスするのを防止するために、IEEE 802.1X ポートベースの認証を設定する手順を説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

802.1X ポートベースの認証の概要

IEEE 802.1X 標準は、クライアント サーバ ベースのアクセス制御と認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、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、スイッチや LAN によって提供されるサービスを利用できるようにします。

802.1X アクセス制御では、クライアントが認証されるまで、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）トラフィックしか許可されません。認証に成功すると、通常のトラフィックをポート経由で送受信することができます。

ここでは、IEEE 802.1X ポートベースの認証について説明します。

装置の役割

802.1X ポート ベースの認証では、図 46-1 に示すように、ネットワーク上の装置にはそれぞれ特定の役割があります。

図 46-1　802.1X 装置の役割

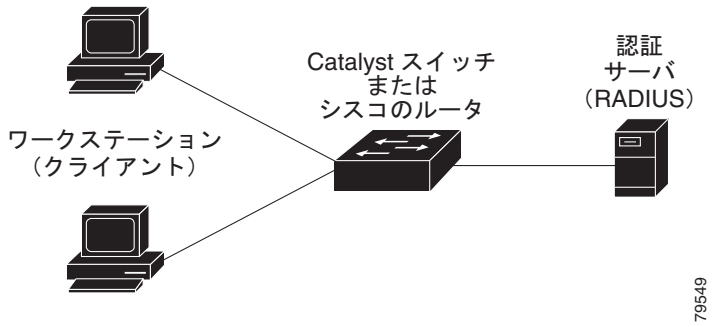


図 46-1 に示す特定の役割は、次のとおりです。

- *クライアント* - LAN および スイッチサービスへのアクセスを要求し、スイッチの要求に応答する装置（ワークステーション）。ワークステーション上では、802.1X に準拠するクライアント ソフトウェア（Microsoft Windows XP オペレーティング システムで提供されるクライアント ソフトウェアなど）が稼動している必要があります （クライアントは、IEEE 802.1X 規格では *supplicant* といいます）。

  （注） Windows XP のネットワーク接続および 802.1X ポートベースの認証に関しては、次の URL にある Microsoft サポート技術情報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は透過的に行われます。認証サーバとして、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 システムだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。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*（*認証者*または*バックエンド認証者*とも呼ばれます）- 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装置（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/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。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする際、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 フレームの変更または検証は行われず、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。

認証の開始およびメッセージ交換

スイッチまたはクライアントのどちらからも、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移行したと判断した時点で、認証を開始しなければなりません。その場合、スイッチは EAP 要求/アイデンティティ フレームをクライアントに送信して識別情報を要求します（スイッチは通常、最初のアイデンティティ/要求フレームに続いて、認証情報に関する 1 つまたは複数の要求を送信します）。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

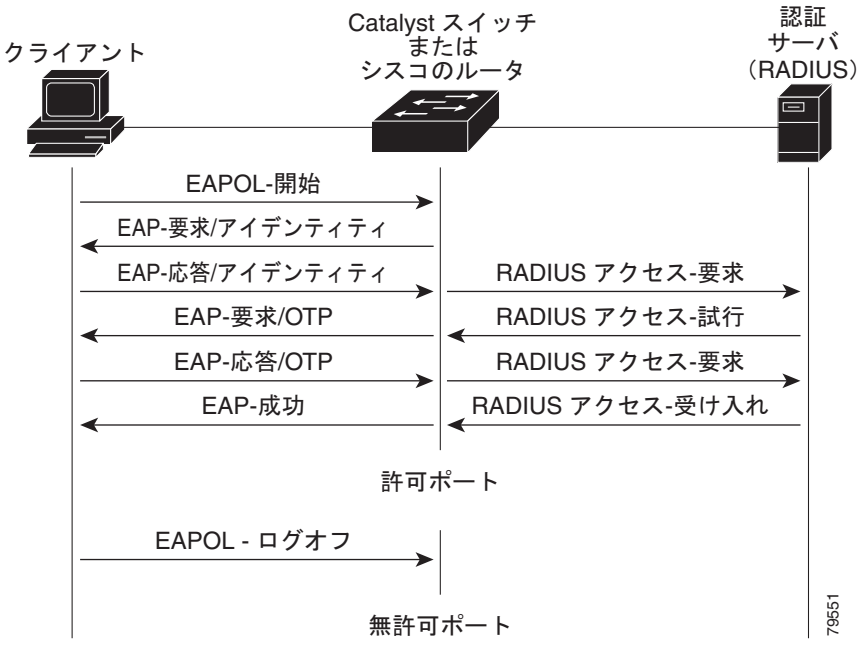
ただし、クライアントがブートアップ時にスイッチから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス装置で 802.1X 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 要求/アイデンティティ 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.46-4）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、スイッチは仲介装置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。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.46-4）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 46-2 に、クライアントが RADIUS サーバとの間で One-Time-Password（OTP; ワンタイム パスワード）認証方式を使用する場合に行われるメッセージ交換を示します。

図 46-2　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

スイッチのポート ステートは、クライアントがネットワーク アクセスを許可されたかどうかを表します。ポートは最初、*無許可*ステートです。このステートでは、ポートは 802.1X プロトコル 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*ステートに移行し、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。

802.1X をサポートしていないクライアントが、無許可ステートの 802.1X ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1X 対応のクライアントが、802.1X プロトコルの稼動していないポートに接続すると、クライアントは EAPOL 開始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。応答がないので、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** - 802.1X ポートベースの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移行させます。ポートはクライアントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- **force-unauthorized** - クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、インターフェイスを介してクライアントに認証サービスを提供することができません。
- **auto** - 802.1X ポートベースの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移行したとき、または EAPOL 開始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全フレームがポート経由での送受信を許可されます。認証が失敗すると、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できます。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 ログオフ メッセージを送信します。このメッセージによって、スイッチポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ 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。

サポートされるトポロジ

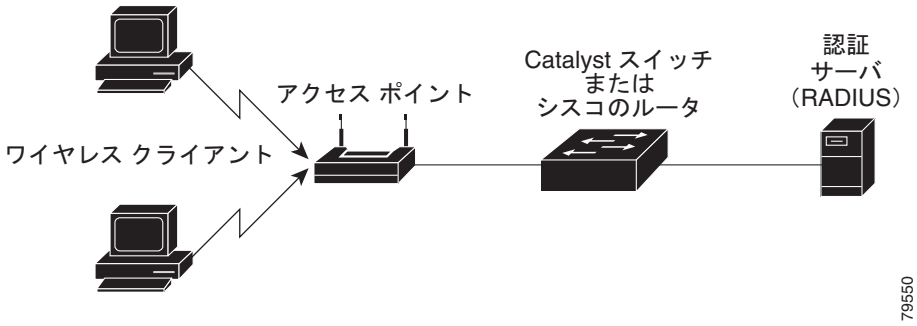
802.1X ポート ベース認証は、次の 2 つのトポロジでサポートされます。

- ポイントツーポイント
- ワイヤレス LAN

ポイントツーポイント構成（図 46-1（P.46-2）を参照）では、802.1X 対応のスイッチ ポートには、クライアントが 1 つしか接続できません。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、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。

図 46-3 に、ワイヤレス LAN における 802.1X ポート ベースの認証を示します。802.1X ポートは複数ホスト ポートとして設定されており、いずれか 1 つのクライアントが認証された時点で許可ステートになります。ポートが許可ステートになると、そのポートに間接的に接続している他のすべてのホストが、ネットワーク アクセスを許可されます。ポートが無許可ステートになると（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、スイッチはすべての接続先クライアントのネットワーク アクセスを禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続先クライアントの認証を処理し、スイッチに対するクライアントとしての役割を果たします。

図 46-3　　ワイヤレス LAN の例



802.1X ポートベースの認証のデフォルト設定

表 46-1 に、802.1X のデフォルト設定を示します。

表 46-1　802.1X のデフォルト設定

機能	デフォルト設定
AAA（Authentication, Authorization, and Accounting; 認証、許可、アカウンティング）	ディセーブル
RADIUS サーバの IP アドレス	指定なし
RADIUS サーバの UDP 認証ポート	1812
RADIUS サーバ キー	指定なし
インターフェイス単位の 802.1X プロトコル イネーブル ステート	ディセーブル（force-authorized） **（注）** ポートはクライアントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
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）
再送信時間	30 秒（スイッチが EAP 要求/アイデンティティ 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までに、EAP 要求/アイデンティティ フレームを送信する回数）
複数ホストのサポート	ディセーブル
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、スイッチが応答を待ち、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、サーバに応答を再送信するまでの時間）

802.1X ポートベースの認証時の注意事項および制約事項

802.1X ポートベースの認証を設定する際の注意事項および制約事項は、次のとおりです。

- 802.1X をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1X プロトコルは、レイヤ 2 のスタティック アクセス ポートおよびレイヤ 3 ルーテッド ポート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 ポートで 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、802.1X はイネーブルになりません。802.1X 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
  - EtherChannel ポート - ポート上で 802.1X をイネーブルにする前に、EtherChannel のポート チャネル インターフェイスから 802.1X を削除する必要があります。EtherChannel のポート チャネル インターフェイス上または EtherChannel 上の個々のアクティブ ポートで 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、802.1X はイネーブルになりません。まだアクティブになっていない EtherChannel 上の個々のポートで 802.1X をイネーブルにしても、そのポートは EtherChannel に加入しません。
  - セキュア ポート - セキュア ポートは 802.1X ポートにできません。セキュア ポートで 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、802.1X はイネーブルになりません。802.1X 対応ポートをセキュア ポートに変更しようとしても、エラー メッセージが表示され、セキュリティ設定は変更されません。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポート - SPAN 宛先ポートであるポートで 802.1X をイネーブルにすることができます。ただし、ポートが SPAN 宛先として削除されるまで、802.1X はディセーブルになります。SPAN 送信元ポートでは 802.1X をイネーブルにできます。
- 802.1X プロトコルは、音声 VLAN に設定されているポートではサポートされていません。

802.1X ポートベースの認証の設定

ここでは、802.1X ポートベースの認証の設定方法を説明します。

802.1X ポートベース認証のイネーブル化

802.1X ポート ベース認証をイネーブルにするには、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。

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認証方式を選択します。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。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

802.1X ポート ベースの認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA をイネーブルにします。
	`Router(config)# no aaa new-model`	AAA をディセーブルにします。
ステップ 2	`Router(config)# aaa authentication dot1x {default} method1 [method2...]`	802.1X ポート ベース認証方式リストを作成します。
	`Router(config)# no aaa authentication dot1x {default | list_name}`	設定されている方式リストを消去します。
ステップ 3	`Router(config)# dot1x system-auth-control`	802.1X ポートベースの認証をグローバルにイネーブルにします。
	`Router(config)# no dot1x system-auth-control`	802.1X ポートベースの認証をグローバルにディセーブルにします。
ステップ 4	`Router(config)# interface type[1] slot/port`	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、802.1X ポートベースの認証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 5	`Router(config-if)# dot1x port-control auto`	インターフェイス上で 802.1X ポートベースの認証をイネーブルにします。
	`Router(config-if)# no dot1x port-control auto`	インターフェイス上で 802.1X ポートベースの認証をディセーブルにします。
ステップ 6	`Router(config)# end`	イネーブル EXEC モードに戻ります。
ステップ 7	`Router# show dot1x all`	設定を確認します。 表示の 802.1X Port Summary セクションの Status カラムを確認してください。*enabled* というステータスは、ポート制御値が、**auto** または **force-unauthorized** に設定されていることを意味します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

802.1X ポートベースの認証をイネーブルにする場合、次の点に注意してください。

- **authentication** コマンドに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、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。
- 次のキーワードのうち、少なくとも 1 つを指定します。
  - **group radius** - すべての RADIUS サーバのリストを使用して認証します。
  - **none** - 認証を使用しません。クライアントから提供される情報を使用することなく、クライアントはスイッチにより自動的に認証されます。

次に、ファスト イーサネット ポート 5/1 で AAA と 802.1X をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show dot1x all

Dot1x Info for interface FastEthernet5/1
----------------------------------------------------
AuthSM State      = FORCE UNAUTHORIZED
BendSM State      = IDLE
PortStatus        = UNAUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
Port Control      = Force UnAuthorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

スイッチと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の 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（たとえば認証など）を設定した場合、2 番目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。

RADIUS サーバ パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
	`Router(config)# no ip radius source-interface`	RADIUS パケットが、以前に指定されたインターフェイスの IP アドレスを含まないようにします。
ステップ 2	`Router(config)# radius-server host {hostname | ip_address}`	スイッチに RADIUS サーバ ホスト名または IP アドレスを設定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
	`Router(config)# no radius-server host {hostname | ip_address}`	指定した RADIUS サーバを削除します。
ステップ 3	`Router(config)# radius-server key string`	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、認証鍵および暗号鍵を設定します。
ステップ 4	`Router(config)# end`	イネーブル EXEC モードに戻ります。

RADIUS サーバ パラメータを設定する場合、次の点に注意してください。

- *hostname* または *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。
- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証鍵および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、鍵の途中および末尾のスペースが利用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号に一致している必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号鍵の値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2、『*Cisco IOS Security Command Reference*』Release 12.2 を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

（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。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Router# configure terminal
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46
Router(config)# radius-server key rad123
Router(config)# end
```

定期的な再認証のイネーブル化

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。再認証をイネーブルにする前にその間隔を指定しない場合、3,600 秒おきに再認証が試みられます。

802.1X クライアントの自動的な再認証はグローバルな設定であり、個々のポートに接続するクライアント別に設定することはできません。特定のポートに接続するクライアントを手動で再認証する方法については、「手動によるポート接続クライアントの再認証」（P.46-11）を参照してください。

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）を設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x reauthentication`	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルに設定されています。
	`Router(config-if)# no dot1x reauthentication`	クライアントの定期的な再認証をディセーブルにします。
ステップ 3	`Router(config-if)# dot1x timeout reauth-period seconds`	再認証の間隔（秒）を設定します。 指定できる範囲は 1 ～ 65535 です。デフォルトは 3,600 秒です。 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。
	`Router(config-if)# no dot1x timeout reauth-period`	デフォルトの再認証の間隔に戻します。
ステップ 4	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4,000 秒に設定する例を示します。

```
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 4000
```

手動によるポート接続クライアントの再認証

（注）　再認証は、すでに許可されているポートのステータスには影響しません。

特定のポートに接続されているクライアントを手動で再認証するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dot1x re-authenticate interface type[1] slot/port`	ポートに接続されているクライアントを手動で再認証します。
ステップ 2	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/1 に接続されているクライアントを手動で再認証する例を示します。

```
Router# dot1x re-authenticate interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
```

ポート接続クライアント認証の初期化

（注）　認証の初期化により、既存の認証はディセーブルにしてから、ポートに接続されているクライアントを認証します。

ポートに接続されているクライアントの認証を初期化するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dot1x initialize interface` *type*[1] *slot/port*	ポートに接続されているクライアントの認証を初期化します。
ステップ 2	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/1 に接続されているクライアントに対する認証を初期化する例を示します。

```
Router# dot1x initialize interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
```

待機時間の変更

スイッチがクライアントを認証できなかった場合は、スイッチは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。このアイドル時間は、待機時間の値によって決定されます。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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# 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 0 ～ 65535 です。デフォルトは 60 秒です。
	`Router(config-if)# no dot1x timeout quiet-period`	デフォルトの待機時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

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。

```
Router(config-if)# dot1x timeout quiet-period 30
```

スイッチとクライアント間の再送信時間の変更

クライアントはスイッチからの EAP 要求/アイデンティティ フレームに対し、EAP 応答/アイデンティティ 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下した場合や、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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout tx-period` *seconds*	スイッチが EAP 要求/アイデンティティ 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 です。デフォルトは 30 秒です。
	`Router(config-if)# dot1x timeout tx-period`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、スイッチが EAP 要求/アイデンティティ 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。

```
Router(config)# dot1x timeout tx-period 60
```

スイッチとクライアント間の EAP 要求フレーム再送信時間の設定

クライアントは EAP 要求フレームを受信したことをスイッチに通知します。スイッチがこの通知を受信できなかった場合、スイッチは所定の時間だけ待機し、そのあとフレームを再送信します。スイッチが通知を待機する時間は、1 ～ 65,535 秒の範囲に指定できます （デフォルトは 30 秒です）。

スイッチからクライアントへの EAP 要求フレーム再送信時間を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout supp-timeout` *seconds*	スイッチからクライアントへの EAP 要求フレームの再送信時間を設定します。
	`Router(config-if)# no dot1x timeout supp-timeout`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、スイッチからクライアントへの EAP 要求フレームの再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout supp-timeout 25
```

スイッチと認証サーバ間のレイヤ 4 パケット再送信時間の設定

認証サーバは、レイヤ 4 パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後、通知を受信できない場合、スイッチは所定の時間だけ待機し、そのあとパケットを再送信します。スイッチが通知を待機する時間は、1 ～ 65,535 秒の範囲に指定できます （デフォルトは 30 秒です）。

スイッチから認証サーバへのレイヤ 4 パケットの再送信値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x timeout server-timeout` *seconds*	スイッチから認証サーバへのレイヤ 4 パケットの再送信時間を設定します。
	`Router(config-if)# no dot1x timeout server-timeout`	デフォルトの再送信時間に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、スイッチから認証サーバへのレイヤ 4 パケットの再送信時間を 25 秒に設定する例を示します。

```
Router(config-if)# dot1x timeout server-timeout 25
```

スイッチとクライアント間のフレーム再送信回数の設定

スイッチとクライアント間の再送信時間を変更できるだけでなく、スイッチが（クライアントから応答が得られなかった場合に）認証プロセスを再開する前に、クライアントに EAP 要求/アイデンティティ フレームを送信する回数を変更することができます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x max-req` *count*	スイッチが認証プロセスを再開するまでに、EAP 要求/アイデンティティ フレームをクライアントに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。
	`Router(config-if)# no dot1x max-req`	デフォルトの再送信回数に戻ります。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、スイッチが認証プロセスを再開する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定する例を示します。

```
Router(config-if)# dot1x max-req 5
```

複数ホストのイネーブル化

図 46-3（P.46-5）に示すように、1 つの 802.1X 対応ポートに複数のホストを接続することができます。このモードでは、接続されたホストのうち 1 つが認証に成功すれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、および EAPOL ログオフ メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

dot1x port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている 802.1X 許可ポートに、複数のホスト（クライアント）が接続できるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x host-mode multi-host`	802.1X 許可ポートで複数ホスト（クライアント）を許可します。 **（注）** 指定するインターフェイスでは、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。
	`Router(config-if)# dot1x host-mode single-host`	ポート上の複数のホストをディセーブルにします。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x interface` *type*[1] *slot/port*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット インターフェイス 5/1 で 802.1X をイネーブルにし、複数のホストを許可する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x host-mode multi-host
```

802.1X 設定のデフォルト値へのリセット

802.1X 設定をデフォルト値に戻すには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# dot1x default`	設定可能な 802.1X パラメータをデフォルト値にリセットします。
ステップ 3	`Router(config-if)# end`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

802.1X ステータスの表示

スイッチのグローバルな 802.1X の管理ステータスおよび動作ステータスを表示するには、**show dot1x** イネーブル EXEC コマンドを使用します。特定のインターフェイスに関する 802.1X の管理ステータスおよび動作ステータスを表示するには、**show dot1x interface** *interface-id* イネーブル EXEC コマンドを使用します。

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

CHAPTER 47

ポート セキュリティの設定

この章では、ポート セキュリティ機能を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

ポート セキュリティの概要

ここでは、ポート セキュリティについて説明します。

ダイナミックに学習される MAC アドレスとスタティック MAC アドレスによるポート セキュリティ

ダイナミックに学習される MAC（メディア アクセス制御）アドレス、およびスタティック MAC アドレスを使用したポート セキュリティでは、ポートへのトラフィック送信を許可する MAC アドレスを制限できるので、入力トラフィックを制限できます。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入力トラフィックを転送しません。セキュア MAC アドレスの数を 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ている装置はそのポートの全帯域を使用できます。

セキュリティ違反は、次のいずれかの状況で発生します。

- セキュア ポートでセキュア MAC アドレスの最大数に達したあと、入力トラフィックの送信元 MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なる場合は、設定済みの違反モードが適用されます。
- あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つトラフィックが、同一 Virtual LAN（VLAN; 仮想 LAN）内の別のセキュア ポートにアクセスしようとすると、ポート セキュリティはこの違反に対し、次のいずれかの方法で対応します。
  - Release 12.2(18)SXF5 以降のリリースでは、設定済みの違反モードが適用されます。
  - Release 12.2(18)SXF5 よりも前のリリースでは、シャットダウン違反モードが適用されます。

（注） あるセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同じ VLAN 内の別のポート上でこのセキュア MAC アドレスが検出された場合に発生する一連のイベントを、MAC の移行違反と呼びます。

違反モードの詳細情報については、「ポートでのポート セキュリティ違反モードの設定」（P.47-7）を参照してください。

ポートでセキュア MAC アドレスの最大数を設定したあと、セキュア アドレスは、次のいずれかの方法でアドレス テーブルに組み込まれます。

- すべてのセキュア MAC アドレスを、**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スタティックに設定できます。
- 接続されている装置の MAC アドレスによって、ポートがセキュア MAC アドレスをダイナミックに設定するように指定できます。
- 多数のアドレスをスタティックに設定し、残りのアドレスはダイナミックに設定されるように指定できます。

ポートがリンクダウン状態になると、ダイナミックに学習されたアドレスはすべて削除されます。

ブートアップ、リロード、またはリンクダウン状態のあとは、ポートが入力トラフィックを受信するまで、ダイナミックに学習された MAC アドレスはアドレス テーブルに書き込まれません。

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た時点で、アドレス テーブルにはない MAC アドレスからのトラフィックをポートが受信すると、セキュリティ違反となります。

ポートには、protect、restrict、または shutdown のいずれかの違反モードを設定できます。「ポート セキュリティの設定」（P.47-5）を参照してください。

アドレスの最大数を 1 に設定し、接続された装置の MAC アドレスを設定すると、その装置にはポートの全帯域幅が保証されます。

sticky MAC アドレスによるポート セキュリティ

Release12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポート セキュリティがサポートされます。sticky MAC アドレスを使用するポート セキュリティには、スタティック MAC アドレスによるポート セキュリティと同様の多数の利点がありますが、さらに、sticky MAC アドレスはダイナミックに学習できます。sticky MAC アドレスを使用したポート セキュリティでは、リンクダウン状態の発生中も、ダイナミックに学習された MAC アドレスを維持します。

sticky MAC アドレスによるポート セキュリティでは、**write memory** または **copy running-config startup-config** コマンドを実行すると、ダイナミックに学習された MAC アドレスは startup-config ファイルに保存されます。したがって、ブートアップ後または再起動後に、ポートが入力トラフィックからアドレスを学習する必要がありません。

ポート セキュリティのデフォルト設定

表 47-1 に、インターフェイス用のデフォルトのポート セキュリティ設定を示します。

表 47-1　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	ディセーブル
セキュア MAC アドレスの最大数	1.
違反モード	shutdown。セキュア MAC アドレスが最大数を超過した場合、ポートはシャットダウンし、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップ通知が送信されます。

ポートセキュリティに関する注意事項および制約事項

ポート セキュリティを設定する場合は、次の注意事項に従ってください。

- ポート セキュリティのデフォルト設定を使用して errdisable ステートからセキュア ポートを回復するには、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力します。または、**shutdown** および **no shut down** 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、手動でセキュア ポートを再びイネーブルに戻すことができます。
- ダイナミックに学習されたすべてのセキュア アドレスを消去するには、**clear port-security dynamic** 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。構文の詳細については、*Cisco IOS Master Command List*, Release 12.2SX を参照してください。
- 無許可の MAC アドレスは、特定のビット セットとともに学習されます。このビット セットにより、このアドレスから送信されるトラフィック、およびこのアドレス宛てに送信されるトラフィックはいずれも廃棄されます。**show mac-address-table** コマンドを使用すると、無許可の MAC アドレスを表示できますが、ビット ステートは表示されません （CSCeb76844）。
- sticky MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、ブートアップまたはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。

- Release12.2(18)SXE 以降のリリースでは、ポート セキュリティで プライベート VLAN（PVLAN）ポートがサポートされます。
- Release12.2(18)SXE よりも前のリリースでは、ポート セキュリティでPVLAN ポートはサポートされません。
- Release12.2(18)SXE 以降のリリースでは、ポート セキュリティで非交渉トランクがサポートされます。
  - ポート セキュリティは、次のコマンドで設定したトランクだけをサポートします。

    switchport
    switchport trunk encapsulation
    switchport mode trunk
    switchport nonegotiate

  - セキュア アクセス ポートをトランクとして再設定すると、アクセス VLAN でダイナミックに学習された、このポートのすべての sticky およびスタティック セキュア アドレスが、トランクのネイティブ VLAN 上の sticky およびスタティック セキュア アドレスに変換されます。アクセス ポートの音声 VLAN では、すべてのセキュア アドレスが削除されます。
  - セキュア トランクをアクセス ポートとして再設定すると、ネイティブ VLAN で学習されたすべての sticky およびスタティック アドレスは、アクセス ポートのアクセス VLAN で学習されたアドレスに変換されます。ネイティブ VLAN 以外の VLAN で学習されたすべてのアドレスは削除されます。

（注）　ポート セキュリティでは、IEEE 802.1Q トランクおよび Inter-Switch Link（ISL; スイッチ間リンク）トランク双方に対し、**switchport trunk native vlan** コマンドで設定した VLAN ID が使用されます。

- Release12.2(18)SXE よりも前のリリースでは、トランクはポート セキュリティでサポートされません。
- Release12.2(18)SXE 以降のリリースでは、ポート セキュリティで IEEE 802.1Q トンネル ポートがサポートされます。
- Release12.2(18)SXE よりも前のリリースでは、IEEE 802.1Q トンネル ポートはポート セキュリティでサポートされません。
- ポート セキュリティでは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）宛先ポートはサポートされません。
- ポート セキュリティでは、EtherChannel のポートチャネル インターフェイスはサポートされません。
- Release 12.2(33)SXH よりも前のリリースでは、ポート セキュリティ、および 802.1X ポート ベースの認証は、同一ポート上には設定できません。
  - セキュア ポートで 802.1X ポート ベース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、このポートで802.1X ポート ベース認証はイネーブルになりません。
  - 802.1X ポート ベース認証用に設定したポートでポート セキュリティ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、このポートでポート セキュリティはイネーブルになりません。
- 隣接するスイッチに接続されているポートのポート セキュリティをイネーブルにする場合は注意してください。スイッチ間で実行中の冗長リンクがある場合、ポート セキュリティ違反が原因で、ポート セキュリティによってポートが errdisable ステートになる可能性があります。

ポート セキュリティの設定

ここでは、ポート セキュリティを設定する手順について説明します。

ポート セキュリティのイネーブル化

ここでは、ポート セキュリティをイネーブル化する手順について説明します。

トランクでのポート セキュリティのイネーブル化

Release12.2(18)SXE 以降のリリースでは、ポート セキュリティで非交渉トランクがサポートされます。

注意　セキュア アドレス数はデフォルトで 1 であり、違反に対するデフォルト アクションはポートのシャットダウンであるため、トランクでポート セキュリティをイネーブルにする前に、このポートのセキュア MAC アドレスの最大数を設定します（「セキュア MAC アドレスの最大数をポートに設定」（P.47-9）を参照）。

トランクでポート セキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチポートとして設定します。
ステップ 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	カプセル化を設定して、レイヤ 2 スイッチング ポートを ISL または 802.1Q トランクとして設定します。
ステップ 4	`Router(config-if)# switchport mode trunk`	無条件にポートをトランクに設定します。
ステップ 5	`Router(config-if)# switchport nonegotiate`	Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）を使用しないようにトランクを設定します。
ステップ 6	`Router(config-if)# switchport port-security` `Router(config-if)# no switchport port-security`	トランクでポート セキュリティをイネーブルにします。 トランクでポート セキュリティをディセーブルにします。
ステップ 7	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include Port Security`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/36 を非交渉トランクとして設定し、ポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface fastethernet 5/36 | include Port Security
Port Security              : Enabled
```

アクセス ポートでのポート セキュリティのイネーブル化

アクセス ポートでポート セキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。 （注）　Release12.2(18)SXE 以降のリリースでは、ポートをトンネル ポートまたは PVLAN ポートとして使用できます。
ステップ 2	`Router(config-if)# switchport`	ポートをレイヤ 2 スイッチポートとして設定します。
ステップ 3	`Router(config-if)# switchport mode access`	ポートをレイヤ 2 アクセス ポートとして設定します。 （注）　デフォルト モード（dynamic desirable）のポートは、セキュア ポートとして設定できません。
ステップ 4	`Router(config-if)# switchport port-security` `Router(config-if)# no switchport port-security`	ポートのポート セキュリティをイネーブルにします。 ポートのポート セキュリティをディセーブルにします。
ステップ 5	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include Port Security`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/12 でポート セキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface fastethernet 5/12 | include Port Security
Port Security              : Enabled
```

ポートでのポート セキュリティ違反モードの設定

ポートでポート セキュリティの違反モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security violation {protect | restrict | shutdown}`	（任意）違反モード、およびセキュリティ違反が検出されたときのアクションを設定します。
	`Router(config-if)# no switchport port-security violation`	デフォルト設定（**shutdown**）に戻します。
ステップ 3	`Router(config-if)# do show port-security interface type[1] slot/port | include violation_mode[2]`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
2. *violation_mode* = **protect**、**restrict**、または **shutdown**

ポート セキュリティの違反モードを設定する場合は、次の点に注意してください。

- **protect** - 最大値を下回るようにセキュア MAC アドレスを削除するまで、送信元アドレスが不明なパケットを廃棄します。
- **restrict** - 最大値を下回るようにセキュア MAC アドレスを削除するまで、送信元アドレスが不明なパケットを廃棄して、セキュリティ違反カウンタを増やします。
- **shutdown** - インターフェイスをただちに errdisable ステートにし、SNMP トラップ通知を送信します。

（注）

- errdisable ステートからセキュア ポートを回復するには、**errdisable recovery cause** *violation_mode* 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。または、**shutdown** および **no shut down** 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、手動でセキュア ポートを再びイネーブルに戻すことができます。
- CPU 使用率の過度な上昇を防止するため、protect または restrict 違反モードを設定する場合は、パケット廃棄レート リミッタを設定してください（「ポート セキュリティのレート リミッタの設定」（P.47-8）を参照）。

次の例では、ファスト イーサネット ポート 5/12 のセキュリティ違反モードを protect に設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface fastethernet 5/12 | include Protect
Violation Mode             : Protect
```

次の例では、ファスト イーサネット ポート 5/12 のセキュリティ違反モードを restrict に設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface fastethernet 5/12 | include Restrict
Violation Mode             : Restrict
```

ポート セキュリティのレート リミッタの設定

（注）
- PFC2 はポート セキュリティ レート リミッタをサポートしていません。
- truncated スイッチング モードでは、ポート セキュリティ レート リミッタはサポートされません。

ポート セキュリティはセキュア ポートで受信されたすべてのトラフィックを調べ、違反を検出し、新たなセキュア MAC アドレスを認識します。shutdown 違反モードを設定した場合は、違反が検出されたあとはトラフィックはセキュア ポートに入力できません。この結果、違反によって CPU に過剰な負荷がかかることがありません。

protect または restrict 違反モードを設定した場合は、違反が発生したあともポート セキュリティによるトラフィック処理は続行され、その結果 CPU の負荷が高まる可能性があります。protect または restrict 違反モードを設定した場合は、過剰な負荷から CPU を保護するため、ポート セキュリティ レート リミッタを設定してください。

ポート セキュリティ レート リミッタを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls rate-limit layer2 port-security** *rate_in_pps* [*burst_size*]	ポート セキュリティ レート リミッタを設定します。
	Router(config)# **no mls rate-limit layer2 port-security**	デフォルト設定に戻します。
ステップ 2	Router(config)# **do show mls rate-limit | include PORTSEC**	設定を確認します。

ポート セキュリティ レート リミッタを設定する場合は、次の点に注意してください。

- *rate_in_pps* 値に関する注意事項：
  - 有効値の範囲は 10 ～ 1,000,000（1000000 と入力）です。
  - デフォルト値はありません。
  - 設定値が低いほど、CPU の保護が強化されます。レート リミッタは、セキュリティ違反の発生前と発生後の両方でトラフィックに適用されます。正規のトラフィックがポート セキュリティ機能に到達できるように、適度な高さの値を設定するようにしてください。
  - 1,000（1000 と入力）未満の値は、十分な保護を提供できます。
- *burst_size* 値に関する注意事項：
  - 有効値の範囲は 1 ～ 255 です。
  - デフォルト値は 10 です。
  - デフォルト値で、十分な保護を提供できます。

次に、ポート セキュリティ レート リミッタを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls rate-limit layer2 port-security 1000
Router(config)# end
```

次に、設定を確認する例を示します。

```
Router# show mls rate-limit | include PORTSEC
LAYER_2 PORTSEC   On              1000       1  Not sharing
```

セキュア MAC アドレスの最大数をポートに設定

セキュア MAC アドレスの最大数をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security maximum` *number_of_addresses* `vlan` {*vlan_ID* | *vlan_range*}	ポートに対し、セキュア MAC アドレスの最大数を設定します（デフォルトは 1）。 **（注）** VLAN ごとの設定は、トランクだけでサポートされます。
	`Router(config-if)# no switchport port-security maximum`	デフォルト設定に戻します。
ステップ 3	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include Maximum`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

セキュア MAC アドレスの最大数をポートに設定する場合は、次の点に注意してください。

- Release 12.2(18)SXE 以降のリリースでは、*number_of_addresses* の有効範囲は 1 ～ 4,097 です。
- Release 12.2(18)SXE よりも前のリリースでは、*number_of_addresses* の有効範囲は 1 ～ 1,024 です。
- Release12.2(18)SXE 以降のリリースでは、ポート セキュリティでトランクがサポートされます。
  - トランクでは、トランクおよびトランク上のすべての VLAN に対し、セキュア MAC アドレスの最大数を設定できます。
  - セキュア MAC アドレスの最大数は、1 つの VLAN、または 特定の VLAN 範囲に対して設定できます。
  - 特定の VLAN 範囲を指定するには、複数組の VLAN 番号をダッシュ（-）でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次の例では、ファスト イーサネット ポート 5/12 に対し、セキュア MAC アドレスの最大数を 64 に設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface fastethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

sticky MAC アドレスによるポート セキュリティのポートでのイネーブル化

Release12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポート セキュリティがサポートされます。sticky MAC アドレスによるポート セキュリティをポートでイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security mac-address sticky`	sticky MAC アドレスによるポート セキュリティをポートでイネーブルにします。
	`Router(config-if)# no switchport port-security mac-address sticky`	sticky MAC アドレスによるポート セキュリティをポートでディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

sticky MAC アドレスによるポート セキュリティをイネーブルにする場合は、次の点に注意してください。

- **switchport port-security mac-address sticky** コマンドを入力すると、次のようになります。
  - ポートでダイナミックに学習されたすべてのセキュア MAC アドレスは、sticky セキュア MAC アドレスに変換されます。
  - スタティックなセキュア MAC アドレスは、sticky MAC アドレスに変換されません。
  - 音声 VLAN でダイナミックに学習されたセキュア MAC アドレスは、sticky MAC アドレスに変換されません。
  - ダイナミックに学習された新規のセキュア MAC アドレスは、sticky アドレスとなります。
- **no switchport port-security mac-address sticky** コマンドを入力すると、ポート上のすべての sticky セキュア MAC アドレスは、ダイナミックなセキュア MAC アドレスに変換されます。
- sticky MAC アドレスがダイナミックに学習されたあとに、このアドレスを保存して、ブートアップまたはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。

次に、sticky MAC アドレスによるポート セキュリティをファスト イーサネット ポート 5/12 でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security mac-address sticky
```

スタティック セキュア MAC アドレスのポートでの設定

スタティック セキュア MAC アドレスをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security mac-address [sticky]` *mac_address* `[vlan` *vlan_ID*`]`	ポートに対し、スタティック MAC アドレスをセキュア アドレスとして設定します。 （注）　VLAN ごとの設定は、トランクだけでサポートされます。
	`Router(config-if)# no switchport port-security mac-address [sticky]` *mac_address*	ポートからスタティック セキュア MAC アドレスを消去します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show port-security address`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

スタティック セキュア MAC アドレスをポートに設定する場合は、次の点に注意してください。

- Release12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポート セキュリティをイネーブルにしている場合に、sticky セキュア MAC アドレスを設定できます（「sticky MAC アドレスによるポート セキュリティのポートでのイネーブル化」（P.47-10）を参照）。
- **switchport port-security maximum** コマンドでポートに設定するセキュア MAC アドレスの最大数により、設定可能なセキュア MAC アドレスの数が定義されます。
- 最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習されます。
- Release12.2(18)SXE 以降のリリースでは、トランクでポート セキュリティがサポートされます。
  - トランクでは、VLAN 内でスタティック セキュア MAC アドレスを設定できます。
  - トランクでは、スタティック セキュア MAC アドレスに対応するように VLAN を設定していない場合、このアドレスは **switchport trunk native vlan** コマンドで設定した VLAN でセキュアとなります。

次に、ファスト イーサネット ポート 5/12 で MAC アドレス 1000.2000.3000 をセキュア アドレスとして設定し、その設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------

Vlan    Mac Address       Type                Ports
----    -----------       ----                -----
   1    1000.2000.3000    SecureConfigured     Fa5/12
```

ポートでのセキュア MAC アドレスのエージング設定

absolute キーワードを使用してエージング タイプを設定すると、ダイナミックに学習されるすべてのセキュア アドレスは、エージング タイムを過ぎると期限切れとなります。**inactivity** キーワードを使用してエージング タイプを設定すると、エージング タイムは、ダイナミックに学習されたすべてのセキュア アドレスが期限切れとなるまでの非アクティブ期間として定義されます。

（注）　スタティック セキュア MAC アドレスおよび sticky セキュア MAC アドレスは、期限切れとなりません。

ここでは、ポートでセキュア MAC アドレスのエージングを設定する方法について説明します。

- 「ポートでのセキュア MAC アドレスのエージング タイプの設定」（P.47-12）
- 「ポートでのセキュア MAC アドレスのエージング タイムの設定」（P.47-13）

ポートでのセキュア MAC アドレスのエージング タイプの設定

PFC3 および Release12.2(18)SXE 以降のリリースでは、セキュア MAC アドレスのエージング タイプをポートに設定できます。PFC2 では、セキュア MAC アドレスのエージング タイプは設定できません。PFC2 は、absolute エージングだけをサポートしています。

セキュア MAC アドレスのエージング タイプをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security aging type {absolute | inactivity}`	セキュア MAC アドレスのエージング タイプをポートに設定します（デフォルトは absolute）。
	`Router(config-if)# no switchport port-security aging type`	デフォルトの MAC アドレス エージング タイプに戻します。
ステップ 3	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include Time`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/12 のエージング タイプを inactivity に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security aging type inactivity
Router(config-if)# do show port-security interface fastethernet 5/12 | include Type
Aging Type                : Inactivity
```

ポートでのセキュア MAC アドレスのエージング タイムの設定

セキュア MAC アドレスのエージング タイムをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging time** *aging_time*	セキュア MAC アドレスのエージング タイムをポートに設定します。*aging_time* の有効範囲は 1 ～ 1440 分です（デフォルトは 0）。
	Router(config-if)# **no switchport port-security aging time**	セキュア MAC アドレスのエージング タイムをディセーブルにします。
ステップ 3	Router(config-if)# **do show port-security interface** *type*[1] *slot/port* **| include Time**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次の例では、ファスト イーサネット ポート 5/1 に対し、セキュア MAC アドレスのエージング タイムを 2 時間（120 分）に設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport port-security aging time 120
Router(config-if)# do show port-security interface fastethernet 5/12 | include Time
Aging Time                : 120 mins
```

ポート セキュリティ設定の表示

ポート セキュリティ設定を表示するには、次のコマンドを入力します。

コマンド	目的
Router# **show port-security** [**interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*}}] [**address**]	スイッチまたは指定のインターフェイスに対するポート セキュリティ設定を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ポート セキュリティ設定を表示する場合は、次の点に注意してください。

- ポート セキュリティでは、**vlan** キーワードはトランクだけでサポートされます。
- **address** キーワードを使用してセキュア MAC アドレスを表示すると、各アドレスのエージング情報（スイッチに対するグローバル情報、またはインターフェイスごとの情報）が表示されます。
- 次の値が表示されます。
  - 各インターフェイスで許可されるセキュア MAC アドレスの最大数
  - インターフェイスに設定されたセキュア 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

次に、インターフェイスを入力しない場合の **show port-security** コマンドの出力例を示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
------------------------------------------------------------------------------

     Fa5/1           11            11            0            Shutdown
     Fa5/5           15            5             0            Restrict
     Fa5/11          5             4             0            Protect
------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

次に、特定のインターフェイスに対する **show port-security** コマンドの出力例を示します。

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

次に、**show port-security address** イネーブル EXEC コマンドの出力例を示します。

```
Router# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0001.0001.0001    SecureDynamic       Fa5/1      15 (I)
   1    0001.0001.0002    SecureDynamic       Fa5/1      15 (I)
   1    0001.0001.1111    SecureConfigured    Fa5/1      16 (I)
   1    0001.0001.1112    SecureConfigured    Fa5/1      -
   1    0001.0001.1113    SecureConfigured    Fa5/1      -
   1    0005.0005.0001    SecureConfigured    Fa5/5      23
   1    0005.0005.0002    SecureConfigured    Fa5/5      23
   1    0005.0005.0003    SecureConfigured    Fa5/5      23
   1    0011.0011.0001    SecureConfigured    Fa5/11     25 (I)
   1    0011.0011.0002    SecureConfigured    Fa5/11     25 (I)
------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

CHAPTER 48

CDP の設定

この章では、Catalyst 6500 シリーズ スイッチに Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）を設定する手順について説明します。この情報は、次のマニュアルに記載されている情報を補足するものです。

- 次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』リリース 12.2、「System Management」および「Configuring Cisco Discovery Protocol（CDP）」

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf015.htm

- 次の URL にある『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 内の「System Management Commands」、「CDP Commands」

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf015.htm

この章で説明する内容は、次のとおりです。

CDP の機能概要

CDP は、すべてのシスコ ルータ、ブリッジ、アクセス サーバ、およびスイッチ上のレイヤ 2（データリンク層）で動作するプロトコルです。CDP を使用することにより、ネットワーク管理アプリケーションで、既知装置のネイバであるシスコ製の装置、特に下位レイヤの透過プロトコルを実行しているネイバを検索することができます。ネットワーク管理アプリケーションは CDP によって、近接装置の装置タイプおよび Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）エージェント アドレスを学習できます。この機能によって、アプリケーションから近接装置に 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 LAN および WAN メディアで稼動します。

CDP を設定した各装置は、マルチキャスト アドレスに対して定期的にメッセージを送信します。各装置は、SNMP メッセージを受信できる 1 つまたは複数のアドレスをアドバタイズします。このアドバタイズには、受信側装置で CDP 情報を廃棄する前に保持しておく時間を表す Time to Live（TTL）またはホールドタイム情報も含まれます。

CDP の設定

ここでは、CDP の設定手順について説明します。

CDP のグローバルなイネーブル化

CDP をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# cdp run`	CDP をグローバルにイネーブルにします。
`Router(config)# no cdp run`	CDP をグローバルにディセーブルにします。

次に、CDP をグローバルにイネーブルにする例を示します。

```
Router(config)# cdp run
```

CDP のグローバル設定の表示

CDP の設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show cdp`	CDP のグローバル情報を表示します。

次に、CDP の設定を表示する例を示します。

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
Router#
```

その他の CDP の 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.48-4）を参照してください。

ポートでの CDP のイネーブル化

特定のポート上で CDP をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	設定するポートを選択します。
ステップ 2	`Router(config-if)# cdp enable`	ポート上で CDP をイネーブルにします。
	`Router(config-if)# no cdp enable`	ポート上で CDP をディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/1 上で CDP をイネーブルにする例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# cdp enable
```

CDP インターフェイスの設定の表示

特定のポートについて CDP の設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show cdp interface [{{type[1] slot/port} | {port-channel number}}]`	CDP がイネーブルに設定されているポートに関する情報を表示します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ファスト イーサネット ポート 5/1 の CDP の設定を表示する例を示します。

```
Router# show cdp interface fastethernet 5/1
FastEthernet5/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 120 seconds
  Holdtime is 180 seconds
Router#
```

CDP のモニタおよびメンテナンス

装置上の CDP をモニタおよびメンテナンスするには、次の作業を 1 つまたは複数行います。

コマンド	目的
Router# **clear cdp counters**	トラフィック カウンタをゼロにリセットします。
Router# **clear cdp table**	CDP テーブルからネイバに関する情報を消去します。
Router# **show cdp**	送信の頻度、送信されたパケットの保持時間など、グローバルな情報を表示します。
Router# **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。プロトコル情報またはバージョン情報に出力を限定することができます。
Router# **show cdp interface** [*type*[1] *slot/port*}]	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。
Router# **show cdp neighbors** [*type*[1] *slot/port*] [**detail**]	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上のネイバに関する情報に出力を限定することも、より詳細な情報を要求することもできます。
Router# **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。
Router# **show debugging**	イネーブルになっているデバッグのタイプ情報を表示します。CDP **debug** コマンドの詳細については、『*Debug Command Reference*』を参照してください。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、CDP カウンタ設定を消去する例を示します。

```
Router# clear cdp counters
```

次に、近接装置に関する情報を表示する例を示します。

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
JAB023807H1      Fas 5/3            127         T S       WS-C2948  2/46
JAB023807H1      Fas 5/2            127         T S       WS-C2948  2/45
JAB023807H1      Fas 5/1            127         T S       WS-C2948  2/44
JAB023807H1      Gig 1/2            122         T S       WS-C2948  2/50
JAB023807H1      Gig 1/1            122         T S       WS-C2948  2/49
JAB03130104      Fas 5/8            167         T S       WS-C4003  2/47
JAB03130104      Fas 5/9            152         T S       WS-C4003  2/48
```

CHAPTER 49

単一方向リンク検出（UDLD）の設定

この章では、Catalyst 6500 シリーズ スイッチに Unidirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルを設定する方法について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

UDLD の機能概要

ここでは、UDLD の機能について説明します。

UDLD の概要

シスコシステムズ独自の UDLD プロトコルにより、LAN ポートに接続された光ファイバまたは銅製（カテゴリ 5 ケーブルなど）イーサネット ケーブルを使用して接続された装置で、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができます。単一方向リンクが検出されると、UDLD が関係のある LAN ポートをシャットダウンし、ユーザに通知します。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。

UDLD は、レイヤ 1 プロトコルと連動し、リンクの物理的ステータスを判別するレイヤ 2 プロトコルです。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、ネイバの ID の検知、誤って接続された LAN 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 とレイヤ 2 の検知機能が連動し、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。

UDLD のアルゴリズムの詳細については、RFC 5171 を参照してください。UDLD アルゴリズムでは、部分的な設定ミスが検知され、適切な修正措置が実施されるようにするために、同一の LAN セグメントに接続されたすべてのデバイスで UDLD プロトコルを実行する必要があります。

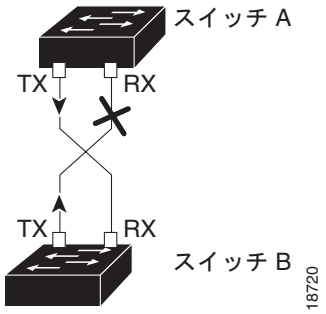
リンク上でローカル装置が送信したトラフィックをネイバが受信するのにネイバから送信されたトラフィックをローカル装置が受信しない場合に、単一方向リンクが発生します。対になっているファイバケーブルのどちらかの接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方のファイバが正常に稼動していれば、レイヤ 2 の UDLD はそれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバ間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で行われるので、このチェックは自動ネゴシエーションでは実行されません。

Catalyst 6500 シリーズ スイッチは、UDLD がイネーブルの LAN ポートの近接装置に、UDLD パケットを定期的に送信します。このパケットが一定時間内にエコー バックされ、かつ特定の確認応答（エコー）がない場合には、そのリンクは単一方向リンクとしてフラグ付けされ、LAN ポートがシャットダウンされます。プロトコルが単一方向リンクを正しく識別して使用を禁止するには、リンクの両端の装置で UDLD をサポートする必要があります。

（注） デフォルトでは、UDLD は銅製 LAN ポート上ではローカルにディセーブルに設定されています。このタイプのメディアは、アクセス ポートに使用されることが多いので、メディアに不要な制御トラフィックを送信しません。

図 49-1 に、単一方向リンク条件の例を示します。スイッチ B は、ポート上でスイッチ A から正常にトラフィックを受信しますが、スイッチ A は、同じポート上でスイッチ B からのトラフィックを受信しません。UDLD によって問題が検出され、ポートがディセーブルにされます。

図 49-1　単一方向リンク



UDLD アグレッシブ モード

UDLD アグレッシブ モ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。UDLD アグレッシブ モードは、そのモードをサポートするネットワーク装置間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブ モードをイネーブルに設定した場合、UDLD 近接関係が設定されている双方向リンク上のポートが UDLD パケットを受信しなくなったとき、UDLD はネイバとの接続を再確立しようとします。この試行に 8 回失敗すると、ポートはディセーブルになります。

スパニング ツリー ループを防止するために、デフォルトの 15 秒間隔を使用する通常の UDLD により、（デフォルトのスパニング ツリー パラメータを使用している場合）ブロッキング ポートがフォワーディング ステートに移行する前に、すみやかに単一方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードをイネーブルにすると、次のような状況でさらに利点をもたらします。

- リンクの一方の側でポート スタック（TX および RX 両方）を使用している場合
- リンクの一方の側がダウンしているにもかかわらず、もう一方の側がアップしたままの場合

このような状況では、UDLD アグレッシブ モードにより、リンク上のポートの 1 つがディセーブルになり、トラフィックの廃棄が防止されます。

（注）　通常モードでは、単一方向エラーが検出されたときにポートはディセーブルになりません。UDLD アグレッシブ モードでは、単一方向エラーが検出されたときにポートはディセーブルになります。

UDLD のデフォルト設定

表 49-1 に、UDLD のデフォルト設定を示します。

表 49-1　UDLD のデフォルト設定

機能	デフォルト値
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
UDLD アグレッシブ モード	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 LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル

UDLD の設定

ここでは、UDLD の設定手順について説明します。

UDLD のグローバルなイネーブル化

すべての光ファイバ LAN ポートで UDLD をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# udld {enable | aggressive}`	光ファイバ LAN ポート上で UDLD をグローバルにイネーブルにします。 **（注）** このコマンドで設定できるのは、光ファイバ LAN ポートだけです。このコマンドによる設定は、個々の LAN ポートの設定によって上書きされます。
`Router(config)# no udld {enable | aggressive}`	光ファイバ LAN ポート上で UDLD をグローバルにディセーブルにします。

個別の LAN インターフェイス上での UDLD のイネーブル化

個別の LAN ポート上で UDLD をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# udld port [aggressive]`	特定の LAN ポート上で UDLD をイネーブルにします。**aggressive** キーワードを入力して、アグレッシブ モードをイネーブルにします。光ファイバ LAN ポートの場合、このコマンドは **udld enable** 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。
	`Router(config-if)# no udld port [aggressive]`	光ファイバ以外の LAN ポート上で UDLD をディセーブルにします。 **（注）** 光ファイバ LAN ポートの場合、**no udld port** コマンドを使用すると、LAN ポートの設定は **udld enable** グローバル コンフィギュレーション コマンドによる設定に戻ります。
ステップ 3	`Router# show udld type[1] slot/number`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

光ファイバ LAN インターフェイス上での UDLD のディセーブル化

個別の光ファイバ LAN ポート上で UDLD をディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **udld port disable**	光ファイバの LAN ポート上で UDLD をディセーブルにします。
	Router(config-if)# **no udld port disable**	**udld enable** 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に戻します。 **（注）** このコマンドは、光ファイバ LAN ポートでだけサポートされています。
ステップ 3	Router# **show udld** *type*[1] *slot/number*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

UDLD プローブ メッセージ インターバルの設定

アドバタイズ モードにあり、現在双方向に設定されているポートで、UDLD プローブ メッセージの間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **udld message time** *interval*	アドバタイズ モードにあり、現在双方向に設定されているポートで、UDLD プローブ メッセージの間隔を設定します。有効値の範囲は 7 ～ 90 秒です。
	Router(config)# **no udld message**	デフォルト値（60 秒）に戻ります。
ステップ 2	Router# **show udld** *type*[1] *slot/number*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ディセーブルになった LAN インターフェイスの表示

ステートの LAN ポートのステータスを表示するには、次の作業を行います。

コマンド	目的
Router# **show udld neighbors** Port　Device Name　Device ID　Port ID　Neighbor State ----　-----------　---------　-------　-------------- Gi3/1　SAL0734K5R2　1　Gi4/1　Bidirectional Gi4/1　SAL0734K5R2　1　Gi3/1　Bidirectional	UDLD ネイバを表示します。

UDLD ネイバ インターフェイスの表示

UDLD-enabled ネイバを表示するには、次の作業を行います。

コマンド	目的
Router# **show udld neighbors** Port Device Name Device ID Port ID Neighbor State ---- ---------- --------- ------- -------------- Gi3/1 SAL0734K5R2 1 Gi4/1 Bidirectional Gi4/1 SAL0734K5R2 1 Gi3/1 Bidirectional	UDLD ネイバを表示します。

ディセーブルになった LAN インターフェイスのリセット

UDLD によってシャットダウンされたすべての LAN ポートをリセットするには、次の作業を行います。

コマンド	目的
Router# **udld reset**	UDLD によってシャットダウンされたすべての LAN ポートをリセットします。

CHAPTER 50

NetFlow の設定

この章では、Catalyst 6500 シリーズ スイッチに NetFlow 統計情報収集を設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『Cisco IOS NetFlow Command Reference』
  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/tsd_products_support_series_home.html

この章で説明する内容は、次のとおりです。

NetFlow の概要

ここでは、NetFlow の機能について説明します。

NetFlow の概要

NetFlow 機能は、スイッチを通過するパケットに関するトラフィック統計情報を収集し、NetFlow テーブルに統計情報を保存します。Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）の NetFlow テーブルは、ソフトウェアでルーティングされるフローの統計情報をキャプチャし、PFC（および各 DFC）の NetFlow テーブルは、ハードウェアでルーティングされるフローの統計情報をキャプチャします。

一部の機能では NetFlow テーブルを使用します。Network Address Translation（NAT; ネットワーク アドレス変換）などの機能は、NetFlow を使用して転送結果を変更し、その他の機能（Quality of Service（QoS; サービス品質）のマイクロフロー ポリシングなど）は、NetFlow テーブルの統計情報を使用して QoS ポリシーを適用します。NetFlow Data Export（NDE; NetFlow データ エクスポート）機能では、（NetFlow コレクタと呼ばれる）外部装置に統計情報をエクスポートできます。

Policy Feature Card（PFC; ポリシー フィーチャ カード）3A モードでは、NetFlow はルーテッド トラフィックのみの統計情報を収集します。PFC3B または PFC3BXL では、ルーテッド トラフィックとブリッジド トラフィックの両方の統計情報を収集するように NetFlow を設定できます。ブリッジド トラフィックの Netflow を使用するには、Release 12.2(18)SXE 以降が必要です。

大量の統計情報を収集してエクスポートすると、スーパーバイザ エンジンや MSFC プロセッサの使用率に重大な影響を及ぼす可能性があるため、NetFlow には統計情報量を制御するための設定オプションが用意されています。これらのオプションには、次のようなものがあります。

- NetFlow フロー マスクは、測定するフローの粒度を決定します。固有性の高いフロー マスクは、エクスポートするための多数の NetFlow テーブル エントリと大量の統計情報を生成します。固有性の低いフロー マスクは、トラフィック統計情報を少数の NetFlow テーブルに集約し、生成する統計情報量も少なくなります。
- サンプリングされた NetFlow は、フロー内のトラフィックのサブセットのデータをエクスポートしますが、これによってエクスポートされる統計情報量が大幅に減ることはありません。サンプリングされた NetFlow が、収集される統計情報の量を減らすことはありません。
- NetFlow アグリゲーションは、収集された統計情報を結合してエクスポートします。集約により、エクスポートするレコードの量は減りますが、収集する統計情報の量は減りません。NetFlow アグリゲーションにより、スイッチの CPU 使用率が増え、コレクタで使用できるデータが減ります。NetFlow アグリゲーションは、NetFlow バージョン 8 を使用します。

NetFlow は 3 つの設定可能なタイマーを定義し、テーブルから削除できる失効フローを識別します。NetFlow は失効エントリを削除し、新しいエントリのためにテーブルのスペースを確保します。

MSFC での NetFlow

MSFC の NetFlow テーブルは、ソフトウェアでルーティングされるフローの統計情報をキャプチャします。MSFC の NetFlow では、NetFlow アグリゲーションをサポートします。NetFlow アグリゲーション方式の詳細については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

MSFC での NetFlow アグリゲーションの設定の詳細については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

MSFC の NetFlow では、Type of Service（ToS; サービス タイプ）ベースのルータ アグリゲーションもサポートされます。次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

Release 12.2(18)SXF 以降のリリースでは、マルチキャスト IP に対する NetFlow をサポートします。マルチキャスト IP に対する NetFlow の詳細については、次のドキュメントにある NetFlow マルチキャスト サポートのマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

NetFlow マルチキャスト サポートのマニュアルでは、マルチキャスト ファスト スイッチング、または Multicast Distributed Fast Switching（MDFS; マルチキャスト ディストリビューティッド ファスト スイッチング）を設定する必要がないことが前提条件で指定されています。ただし、この前提条件は、Release12.2(18)SXF 以降の リリースで NetFlow マルチキャスト サポートを設定する場合には適用されません。

PFC での NetFlow

PFC の NetFlow テーブルは、ハードウェアでルーティングされるフローの統計情報をキャプチャします。PFC では、サンプリングされた NetFlow および NetFlow アグリゲーションをサポートします。PFC では、NetFlow ToS ベースのルータ アグリゲーションをサポートしません。

ここでは、PFC の NetFlow を詳細に説明します。

- 「フロー マスク」（P.50-3）
- 「フロー マスクの不一致」（P.50-4）

フロー マスク

フローとは、送信元と宛先の間でのパケットの単一方向ストリームです。フロー マスクは、NetFlow がフローの識別に使用する着信パケットのフィールドを指定します。NetFlow は、フロー マスクで定義された各フローの統計情報を収集します。

PFC は次のフロー マスクをサポートします。

- source-only - より固有性の低いフロー マスク。PFC は送信元 IP アドレスごとにエントリを 1 つ維持します。指定された送信元 IP アドレスからの全フローの統計情報は、このエントリに集約されます。
- destination - より固有性の低いフロー マスク。PFC は宛先 IP アドレスごとにエントリを 1 つ維持します。指定された宛先 IP アドレスへの全フローの統計情報は、このエントリに集約されます。
- destination-source - より固有性の高いフロー マスク。PFC は送信元および宛先 IP アドレスのペアごとにエントリを 1 つ維持します。同じ送信元 IP アドレスと宛先 IP アドレスの間の全フローの統計情報は、このエントリに集約されます。
- destination-source-interface - より固有性の高いフロー マスク。送信元 Virtual LAN（VLAN; 仮想 LAN）Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ifIndex を destination-source フロー マスク中の情報に追加します。
- full - より固有性の高いフロー マスク。PFC は IP フローごとにテーブル エントリを個別に作成し、維持します。full エントリには送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポートが格納されます。
- full-interface - 最も固有性の高いフロー マスク。送信元 VLAN SNMP ifIndex を full フロー マスク中の情報に追加します。

フロー マスクによって、収集する統計情報の粒度が決定します。これによって NetFlow テーブルのサイズを制御できます。固有性の低いフロー マスクでは、NetFlow テーブルのエントリ数が少なくなり、最も固有性の高いフロー マスクでは、NetFlow エントリ数が最大になります。

たとえば、フロー マスクが source-only に設定されている場合、NetFlow テーブルのエントリ数は送信元 IP アドレスごとに 1 つだけです。特定の送信元からの全フローの統計情報は、1 つのエントリに蓄積されます。ただし、フロー マスクが full に設定されている場合、NetFlow テーブルにはフル フローごとに 1 つのエントリが含まれます。1 つの送信元 IP アドレスに対して多くのエントリが存在することがあるため、NetFlow テーブルが非常に大きくなる可能性があります。NetFlow テーブルの容量については、「NetFlow 設定時の注意事項および制約事項」（P.50-6）を参照してください。

フロー マスクの不一致

一部の機能では、NetFlow テーブルを使用します。表 50-1 に、各機能のフロー マスク要件を示します。

表 50-1　フロー マスクに対する機能要件

機能	送信元	宛先	宛先送信元	宛先送信元インターフェイス	フル フロー	インターフェイス フル フロー	非インターフェイス フル フロー
再帰 ACL						X	
TCP インターセプト					X	X	
Context Based Access Control（CBAC; コンテキスト ベースのアクセス制御）					X		
Web キャッシュ リダイレクト（Web Cache Communication Protocol（WCCP））					X	X	
Server Load Balancing（SLB; サーバ ロード バランシング）					X	X	
ネットワーク アドレス変換（NAT）						X	X
NetFlow データ エクスポート（NDE）	X	X	X	X	X	X	
サンプリングされた NetFlow						X	
NetFlow アグリゲーション		X		X	X	X	
マイクロフロー ポリシング	X	X			X	X	

機能の要件が多岐にわたるため、フロー マスクに不一致が生じる可能性があります。次のフロー マスクの制約事項に注意してください。

- PFC2 では、すべての機能が同じグローバル フロー マスクを共有します。
- PFC3 では、すべての機能がフロー マスクの同じ制限付きセットを共有する必要があります。
- PFC では、各パケット検索に適用できるフロー マスクは 1 つだけです。

MSFC の Feature Manager は、機能間の不一致を解決するソフトウェアです。Feature Manager の主な戦略は、設定されているすべての NetFlow 機能に対応する共通のフロー マスクを選択することです。

ただし、一部の機能にはフロー マスクに対して非常に固有性の高い要件があるため、設定されている機能の共通のフロー マスクを見つけられないことがあります。機能間の不一致を解決するために、Feature Manager ソフトウェアは、機能の 1 つを MSFC 上のソフトウェアで処理するように指示することがあります。

極端な場合、Feature Manager ソフトウェアは、最初に設定された機能を優先し、以降に設定される機能の設定要求を拒否することもあります。あとから Feature Manager で対応できない機能を設定しようとすると、CLI でエラー メッセージを受信します。

機能の不一致に関する問題を回避するには、次の注意事項に従ってください。

- 最も優先度の高い機能を最初に設定してください。解決できない不一致が生じた場合、優先度の低い機能がブロックされます。
- 各機能は、可能な限り、その機能を必要とするインターフェイスだけに設定してください。
- 応答メッセージに注意してください。Feature Manager が、ある機能のハードウェア補助をオフにした場合、機能の処理によって RP プロセッサが過負荷状態にならないようにする必要があります。

不一致に関して注意が必要な機能は、次のとおりです。

- CBAC は full フロー マスクを必要とし、他のフローベースの機能よりも優先されます。フロー マスクに不一致が生じた場合、他のフローベースの機能は MSFC で処理されます。
- 一般的に、NDE は設定されるフロー マスクが最小限であるため柔軟性があります。他のフローベースの機能を設定した場合、Feature Manager ソフトウェアは、すべての機能の要件を満たすために、より固有性の高いフロー マスクを設定することがあります。
- サンプリングされた NetFlow には、dest-source-interface フロー マスク（PFC2）または full-interface フロー マスク（PFC2 および PFC3）が必要です。同じインターフェイス上で、他のフローベースの機能との不一致が生じることがあります。
- NDE と QoS の間では不一致が生じます。NDE と QoS のマイクロフロー ポリシングは、同じインターフェイス上に設定できません。
- NAT に加え、ダイナミック ACE を使用する機能（Web プロシキ認証または Network Admission Control（NAC）レイヤ 3 IP 検証など）がレイヤ 3 インターフェイス上に設定されていると、NAT がオーバーロード用に設定されている場合、後続フラグメントが正しく NAT 変換されないことがあります。この場合、PFC3B または PFC3BXL を搭載したシステムでは、**mls ip nat netflow-frag-l4-zero** コマンドを使用すると、NAT 機能を正常に機能させることができます。

NetFlow のデフォルト設定

表 50-2 に、NetFlow のデフォルト設定を示します。

表 50-2　NetFlow のデフォルト設定

機能	デフォルト値
ルーティングされた IP トラフィックの NetFlow	ディセーブル
入力ブリッジド IP トラフィックの NetFlow	ディセーブル
サンプリングされた NetFlow	ディセーブル
NetFlow アグリゲーション	ディセーブル

NetFlow 設定時の注意事項および制約事項

NetFlow を設定する際は、以下の注意事項と制約事項に従ってください。

- PFC2 以上の場合、CEF テーブル（NetFlow テーブルではない）はハードウェアでのレイヤ 3 スイッチングを実現します。
- Release 12.2(18)SXE 以降のリリースでの PFC3B または PFC3BXL モードでは、NetFlow はブリッジド IP トラフィックをサポートします。PFC3A モードでは、ブリッジド IP トラフィックに対する NetFlow はサポートされません。
- Release 12.2(18)SXF 以降のリリースでは、NetFlow はマルチキャスト IP トラフィックをサポートします。
- 統計情報は、NetFlow テーブルがいっぱいになるとスイッチングされるフローには使用できません。
- NetFlow テーブルの利用率が、推奨レベルの利用率を超過すると、統計情報を保存するための十分な領域が不足する確率が高くなります。表 50-3 に、最大推奨利用率を示します。

表 50-3　NetFlow テーブルの利用率

PFC	推奨される NetFlow テーブルの利用率	NetFlow テーブルの合計容量
PFC3BXL	235,520（230 K）エントリ	262,144（256 K）エントリ
PFC3B	117,760（115 K）エントリ	131,072（128 K）エントリ
PFC3A	65,536（64 K）エントリ	131,072（128 K）エントリ
PFC2	32,768（32 K）エントリ	131,072（128 K）エントリ

NetFlow の設定

ここでは、NetFlow の設定手順について説明します。

- 「PFC での NetFlow の設定」（P.50-7）
- 「MSFC での NetFlow の設定」（P.50-11）

（注）　インターフェイスで NAT を設定する場合、PFC はフラグメント化されたパケットをすべて MSFC に送信して、ソフトウェアで処理させます （CSCdz51590）。

PFC での NetFlow の設定

ここでは、NetFlow による統計情報収集を PFC で設定する手順について説明します。

NetFlow PFC コマンドの概要

表 50-4 に、PFC で使用できる NetFlow コマンドの概要を示します。

表 50-4　PFC NetFlow コマンドの概要

コマンド	目的
mls netflow	PFC で NetFlow をイネーブルにします。
mls flow ip	最小のフロー マスクを設定します。
mls aging	設定可能なエージング パラメータを設定します。
show mls netflow {...}	NetFlow PFC のユニキャストおよびマルチキャスト トラフィックに関する情報を表示します。
show mls netflow aggregation flowmask	NetFlow アグリゲーション フロー マスクを表示します。

（注）

- MSFC で NetFlow アグリゲーションを設定すると、PFC でも自動的にイネーブルになります。
- MSFC でレイヤ 2 トラフィックの NetFlow を設定すると、PFC でも自動的にイネーブルになります。
- MSFC でマルチキャスト NetFlow を設定すると、PFC でも自動的にイネーブルになります。マルチキャスト NetFLow は、Release 12.2(18)SXF 以降のリリースでサポートされます。

PFC での NetFlow のイネーブル化

PFC で NetFlow 統計情報収集をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mls netflow`	PFC で NetFlow をイネーブルにします。
`Router(config)# no mls netflow`	PFC で NetFlow をディセーブルにします。

PFC で NetFlow 統計情報の収集をディセーブルにする例を示します（デフォルト設定はイネーブル）。

```
Router(config)# no mls netflow
```

最小 IP マルチレイヤ スイッチング（MLS）フロー マスクの設定

PFC で NetFlow テーブルに対するフロー マスクの最小特性を設定できます。他の設定済み機能に固有性の高いフロー マスクが必要な場合、実際のフロー マスクは、**mls flow ip** コマンドで設定されたレベルよりも固有性が高くなることがあります（「フロー マスクの不一致」（P.50-4）を参照）。

最小 IP Multilayer Switching（MLS; マルチレイヤ スイッチング）フロー マスクを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls flow ip {source | destination | destination-source | interface-destination-source | full | interface-full}`	プロトコルに最小 IP MLS フロー マスクを設定します。
`Router(config)# no mls flow ip`	デフォルトの IP MLS フロー マスクに戻します（ヌル）。

次に、最小 IP MLS フロー マスクを設定する例を示します。

```
Router(config)# mls flow ip destination
```

IP MLS フロー マスクの設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show mls netflow flowmask`	フロー マスクの設定を表示します。

次に、MLS フロー マスクの設定を表示する例を示します。

```
Router# show mls netflow flowmask
current ip flowmask for unicast: destination address
Router#
```

MLS エージング タイムの設定

MLS エージング タイム（デフォルトは 300 秒）は、すべての NetFlow テーブル エントリに適用されます。normal エージング タイムは、32 ～ 4,092 秒の範囲で設定できます。フローは、設定されたインターバルより 4 秒早く、または 4 秒遅く経過する場合があります。フローは、平均して設定値の 2 秒以内に経過します。

ルーティングの変更またはリンク ステートの変化など、エージング以外のイベントによって MLS エントリが削除される場合があります。

（注）　MLS エントリの数が推奨利用率（「NetFlow 設定時の注意事項および制約事項」（P.50-6）を参照）を超えると、一部のフローで隣接統計情報しか使用できなくなる場合があります。

NetFlow テーブル サイズが推奨利用率を超えないように維持するには、**mls aging** コマンドを使用する際、次のパラメータをイネーブルにします。

- **normal** - 非アクティブのタイマーを設定します。このタイマーの時間内にパケットを受信しなかった場合、そのフロー エントリがテーブルから削除されます。
- **fast aging** - わずかな数のパケットしかスイッチングせず、そのあと再び使用されることのないフローに対して作成されるエントリを、効率的に期限切れにするためのプロセスを設定します。**fast aging** パラメータは、**time** キーワード値を使用して、各フローについて最低でも **threshold** キーワード値で指定される数のパケットがスイッチングされているかどうかを調べます。time で指定される時間内に threshold で指定される数のパケットをスイッチングしていないフローについては、このエントリが期限切れになります。
- **long** - 指定した時間にわたってアクティブであったエントリは、使用中であっても削除するように設定します。long エージングは、不正確な統計情報の原因となるカウンタ ラップアラウンドを防止するために使用します。

削除される一般的なテーブル エントリは、Domain Name Server（DNS; ドメイン ネーム サーバ）または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバとやりとりするフローに対するエントリです。

MLS fast エージング タイムをイネーブルにすることが必要な場合は、最初は 128 秒に設定してください。NetFlow テーブル サイズが増え続け、推奨利用率を超えた場合は、テーブル サイズが推奨利用率未満になるまで設定値を下げます。テーブル サイズが増大し続けて、推奨利用率を超えた場合は、normal MLS エージング タイムを短くします。

MLS エージング タイムを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls aging {fast [threshold {1-128} | time {1-128}] | long 64-1920 | normal 32-4092}`	NetFlow テーブル エントリの MLS エージング タイムを設定します。
`Router(config)# no mls aging fast`	fast aging をディセーブルにします。
`Router(config)# no mls aging {long | normal}`	デフォルトの MLS エージング タイムに戻します。

次に、MLS エージング タイムを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls aging fast threshold 64 time 30
```

MLS エージング タイムの設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show mls netflow aging**	MLS エージング タイムの設定を表示します。

次に、MLS エージング タイムの設定を表示する例を示します。

```
Router# show mls netflow aging
enable timeout packet threshold
------ ------- ----------------
normal aging true 300 N/A
fast aging true 32 100
long aging true 900 N/A
```

PFC での NetFlow アグリゲーションの設定

MSFC で NetFlow アグリゲーションを設定すると、NetFlow アグリゲーションは PFC および DFC で自動的に設定されます（「MSFC での NetFlow アグリゲーションの設定」（P.50-13）を参照）。

PFC または DFC の NetFlow アグリゲーション情報を表示するには、次の作業を行います。

コマンド	目的
Router # **show ip cache flow aggregation** {**as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**) **module** *slot_num*	NetFlow アグリゲーション キャッシュ情報とフローを表示します。
Router # **show mls netflow aggregation flowmask**	NetFlow アグリゲーション フロー マスク情報を表示します。

（注） PFC および DFC では、NetFlow ToS ベースのルータ アグリゲーションをサポートしません。

次に、NetFlow アグリゲーション キャッシュ情報を表示する例を示します。

```
Router# show ip cache flow aggregation destination-prefix module 1
IPFLOW_DST_PREFIX_AGGREGATION records and statistics for module :1
IP Flow Switching Cache, 278544 bytes
2 active, 4094 inactive, 6 added
236 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
Dst If Dst Prefix Msk AS Flows Pkts B/Pk Active
Gi7/9 9.1.0.0 /16 0 3003 12M 64 1699.8
Gi7/10 11.1.0.0 /16 0 3000 9873K 64 1699.8
Router#
```

次に、NetFlow アグリゲーション フロー マスク情報を表示する例を示します。

```
Router# show mls netflow aggregation flowmask
 Current flowmask set for netflow aggregation : Vlan Full Flow
 Netflow aggregations configured/enabled :
        AS Aggregation
        PROTOCOL-PORT Aggregation
        SOURCE-PREFIX Aggregation
        DESTINATION-PREFIX Aggregation
Router#
```

入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化

MSFC で入力ブリッジド IP トラフィックの NetFlow を設定すると、PFC での入力ブリッジド IP トラフィックの NetFlow がイネーブルになります。「入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化」（P.50-13）を参照してください。

マルチキャスト IP トラフィックに対する NetFlow のイネーブル化

MSFC でマルチキャスト IP トラフィックの NetFlow を設定すると、PFC でのマルチキャスト IP トラフィックの NetFlow がイネーブルになります。マルチキャスト IP トラフィックの NetFLow は、Release 12.2(18)SXF 以降のリリースでサポートされます。

詳細については、「マルチキャスト IP トラフィックに対する NetFlow のイネーブル化」（P.50-14）を参照してください。

PFC Netflow 情報の表示

PFC での NetFlow に関する情報を表示するには、次のコマンドを使用します。

コマンド	目的
`Router(config)# show mls netflow {aggregation | aging | creation | flowmask | ip | ipv6 | mpls | table-contention | usage}`	PFC での NetFlow に関する情報を表示します。

MSFC での NetFlow の設定

ここでは、MSFC 上で NetFlow を設定する手順について説明します。

- 「MSFC の NetFlow コマンドの概要」（P.50-12）
- 「MSFC での NetFlow のイネーブル化」（P.50-12）
- 「MSFC での NetFlow アグリゲーションの設定」（P.50-13）
- 「入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化」（P.50-13）
- 「マルチキャスト IP トラフィックに対する NetFlow のイネーブル化」（P.50-14）

MSFC の NetFlow コマンドの概要

表 50-5 に、MSFC で使用できる NetFlow コマンドを示します。

表 50-5　MSFC NetFlow コマンドの概要

コマンド	目的
interface x **ip flow ingress**	特定のインターフェイスに対して、MSFC と PFC で NetFlow をイネーブルにします。
ip flow-aggregation cache	NetFlow アグリゲーションを設定します。MSFC でアグリゲーションを設定すると、PFC のアグリゲーションもイネーブルになります。
export version {8|9}	アグリゲーション データのエクスポート形式 8 または 9 を指定します。
mask source minimum x	アグリゲーションの最小マスクを指定します。
ip flow ingress layer2-switched vlan x	レイヤ 2 スイッチド トラフィックの NetFlow をイネーブルにします。
interface x **ip multicast netflow {ingress|egress}**	特定のインターフェイスでの（MSFC および PFC の）NetFlow マルチキャスト トラフィックをイネーブルにします。
show ip cache flow aggregation	NetFlow アグリゲーション キャッシュ情報とフローを表示します。
show ip cache verbose flow	主要な NetFlow キャッシュ情報とフローを表示します。

MSFC での NetFlow のイネーブル化

MSFC で NetFlow をイネーブルにするには、NetFlow を使用する各レイヤ 3 インターフェイスに対し、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number}`	設定するレイヤ 3 インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip flow ingress`[1] `Router(config-if)# ip route-cache flow`[2]	ハードウェアまたはソフトウェアでルーティングされたフローに関して、選択したインターフェイスの NetFlow をイネーブルにします。ハードウェアでルーティングされたフローの NetFlow をイネーブルにするには、PFC の Netflow もイネーブルにする必要があります。

1. Release 12.2(18)SXD 以降のリリースでサポートされます。
2. Release 12.2(18)SXD では非推奨です。

Release 12.2(18)SXF 以降のリリースでは、**ip flow ingress** コマンドを入力して、インターフェイスの NetFlow をイネーブルにする必要があります。Release 12.2(18)SXF 以前のリリースでは、NetFlow はデフォルトでイネーブルに設定されています。

MSFC での NetFlow アグリゲーションの設定

MSFC での NetFlow アグリゲーションの設定の詳細については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

MSFC での NetFlow ToS ベースのルータ アグリゲーションの設定の詳細については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

（注）

- MSFC で NetFlow アグリゲーションを設定すると、NetFlow アグリゲーションは PFC および DFC で自動的に設定されます（「PFC での NetFlow アグリゲーションの設定」（P.50-10）を参照）。
- PFC および DFC では、NetFlow ToS ベースのルータ アグリゲーションをサポートしません。

入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化

Release 12.2(18)SXE 以降のリリースでの PFC3B または PFC3BXL モードでは、NetFlow は 入力ブリッジド IP トラフィックをサポートします。PFC3A モードでは、ブリッジド IP トラフィックに対する NetFlow はサポートされません。

（注）

- 入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにすると、サンプリングされた NefFlow 機能によってこの統計情報を使用できます（「NetFlow サンプリング」（P.51-7）を参照）。
- VLAN 上でブリッジド IP トラフィックの NetFlow をイネーブルにするには、対応する VLAN インターフェイスを作成し、そのインターフェイスに IP アドレスを割り当て、**no shutdown** コマンドを入力してインターフェイスを立ち上げる必要があります。

VLAN 上の入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow ingress layer2-switched vlan vlan_ID[-vlan_ID] [, vlan_ID[-vlan_ID]]`	指定の VLAN 上での入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにします。 （注）　VLAN 上での入力ブリッジド IP トラフィックに対して NetFlow を使用するには、**mls netflow** コマンドを使用して、PFC 上で NetFlow をイネーブルにする必要があります。
`Router(config)# no ip flow ingress layer2-switched vlan vlan_ID[-vlan_ID] [, vlan_ID[-vlan_ID]]`	指定の VLAN 上での入力ブリッジド IP トラフィックに対して NetFlow をディセーブルにします。

次に、VLAN 200 上の入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip flow ingress layer2-switched vlan 200
```

マルチキャスト IP トラフィックに対する NetFlow のイネーブル化

Release 12.2(18)SXF 以降のリリースでは、マルチキャスト IP に対する NetFlow をサポートします。マルチキャスト IP の NetFlow をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {vlan vlan_ID}	{type slot/port}	{port-channel port_channel_number}`	設定するレイヤ 3 インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip flow ingress`	インターフェイスで NetFlow をイネーブルにします。
ステップ 3	`Router(config-if)# ip multicast netflow {ingress	egress}`	特定のインターフェイスでの（MSFC および PFC の）NetFlow マルチキャスト トラフィックをイネーブルにします。 • NetFlow マルチキャスト入力アカウンティングをイネーブルにするには、**ingress** を指定します。 • Netflow マルチキャスト出力アカウンティングをイネーブルにするには、**egress** を指定します。

マルチキャスト IP に対する NetFlow の詳細については、次のドキュメントにある NetFlow マルチキャスト サポートのマニュアルを参照してください。

Cisco IOS NetFlow Configuration Guide

NetFlow マルチキャスト サポートのマニュアルでは、マルチキャスト ファスト スイッチング、またはマルチキャスト ディストリビューティッド ファスト スイッチング（MDFS）を設定する必要がないことが前提条件で指定されています。ただし、この前提条件は、Release12.2(18)SXF 以降の 12.2SX リリースで NetFlow マルチキャスト サポートを設定する場合には適用されません。

CHAPTER 51

NetFlow データ エクスポート（NDE）の設定

この章では、NetFlow Data Export（NDE; NetFlow データ エクスポート）を設定する手順について説明します。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、以下のマニュアルを参照してください。

- 次の URL にある『*Cisco IOS NetFlow Command Reference*』
  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/tsd_products_support_series_home.html
- NetFlow バージョン 9 がサポートされます。次のマニュアルを参照してください。
  『*Cisco IOS NetFlow Configuration Guide*』

この章で説明する内容は、次のとおりです。

NDE の概要

ここでは、NetFlow データ エクスポート（NDE）の機能について説明します。

NDE の概要

NetFlow は、スイッチを通過するパケットを監視し、NetFlow テーブルに統計情報を保存することにより、トラフィック統計情報を収集します。NetFlow の詳細については、第 50 章「NetFlow の設定」を参照してください。

NetFlow データ エクスポート（NDE）は、NetFlow テーブル統計情報をレコードに変換し、そのレコードを NetFlow コレクタと呼ばれる外部デバイスにエクスポートします。

Policy Feature Card（PFC; ポリシー フィーチャ カード）3A モードでは、NDE はルーテッド トラフィックのみの統計情報をエクスポートします。PFC3B または PFC3BXL では、ルーテッド トラフィックとブリッジド トラフィックの両方の統計情報をエクスポートするように NDE を設定できます。ブリッジド トラフィックの Netflow を使用するには、Release 12.2(18)SXE 以降が必要です。

IP ユニキャスト統計情報は、NDE レコード形式バージョン 5、7、または 9 を使用してエクスポートできます。NetFlow アグリゲーションには NDE バージョン 8 レコード形式、IP ユニキャストにはバージョン 9 レコード形式を使用します。NetFlow バージョン 9 エクスポート形式は、Release 12.2(18)SXF 以降でサポートされます。

大量の統計情報をエクスポートすると、Switch Processor（SP; スイッチ プロセッサ）と Route Processor（RP; ルート プロセッサ）の CPU 使用率に大きな影響を与える場合があります。エクスポートするレコードの量を制御するには、NDE エクスポートからのフローを含めるか、除外するように NDE フロー フィルタを設定します。フィルタを設定すると、NDE は、フィルタ基準に合致するフローだけをエクスポートします。

外部データ コレクタ アドレスは 2 つまで設定できます。2 つめの外部データ コレクタで冗長データ ストリームを提供することにより、完全な NetFlow データを受信する確率が高くなります。この機能は、次のリリースおよびハードウェアで提供されます。

- PFC2 および Release12.2(18)SXD 以降のリリース
- PFC3 および Release12.2(18)SXE 以降のリリース

マルチレイヤ スイッチ フィーチャ カード（MSFC）上での NDE

Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上では、NDE はソフトウェアでルーティングされたフローの統計情報をエクスポートします。MSFC では、NetFlow アグリゲーションがサポートされます。次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

MSFC では、NetFlow Type of Service（ToS; サービス タイプ）ベースのルータ アグリゲーションもサポートされます。次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

Release 12.2(18)SXF 以降のリリースでは、MSFC 上での NetFlow サンプリングがサポートされます。次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

Release 12.2(18)SXF 以降のリリースでは、NetFlow バージョン 9 がサポートされます。次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

NetFlow バージョン 9 レコード形式については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

PFC 上での NDE

PFC 上では、NDE はハードウェアでルーティングまたはブリッジされたフローの統計情報をエクスポートします。ここでは、PFC 上での NDE について説明します。

NDE フロー マスク

NDE の最小 NetFlow フロー マスクを設定できます。NetFlow フロー マスクは、収集された統計情報の粒度を決定することにより、NDE がエクスポートする統計情報の量を制御します。

フロー マスクの詳細については、第 50 章「NetFlow の設定」を参照してください。

追加の NDE フィールド

NDE パケットの次の追加フィールドにデータを読み込むように NDE を設定できます。

- ネクストホップ ルータの IP アドレス
- 出力インターフェイス Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ifIndex
- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）Autonomous System（AS; 自律システム）

FIB テーブルのエントリを検索するソフトウェアは、NDE レコードをコレクタに送信する前に、これらのフィールドにデータを読み込みます。したがって、**show** コマンドを使用してハードウェア NetFlow テーブルを表示すると、これらのフィールドはブランクになります。

NDE のバージョン

Release 12.2(18)SXF 以降のリリースでは、NetFlow バージョン 9 がサポートされます。次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/nfv9expf.htm

NDE は、NDE バージョン 8 を使用する NetFlow アグリゲーション フローの統計情報をエクスポートします。バージョン 8 ヘッダー形式については、次のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt2/xcfnfov.htm#wp1001212

NDE は、NDE バージョン 5、7、および 9 を使用する IP ユニキャスト トラフィックをエクスポートします。

現行のフロー マスクによっては、フロー レコードの一部のフィールドに値が入らない場合があります。サポートされないフィールドには、ゼロ（0）が充填されます。

（注）　Web Cache Communications Protocol（WCCP）レイヤ 2 リダイレクトでは、nexthop フィールドおよび output フィールドが、すべて NetFlow に対する正確な情報を含んでいない場合があります。このため、Web サーバから返されたトラフィックの宛先インターフェイスは、キャッシュ インターフェイスや ANCS インターフェイスではなく、クライアント インターフェイスを持ちます。

次の表に、NDE バージョン 5 および 7 でサポートされているフィールドを示します。

- 表 51-1 - バージョン 5 ヘッダー形式
- 表 51-2 - バージョン 7 ヘッダー形式
- 表 51-3 - バージョン 5 フロー レコード形式
- 表 51-4 - バージョン 7 フロー レコード形式

NetFlow バージョン 9 レコード形式については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e395a.html#wp1180857

表 51-1　NDE バージョン 5 ヘッダー形式

バイト	内容	説明
0 ～ 1	version	NetFlow がエクスポートする形式のバージョン番号
2 ～ 3	count	このパケットにエクスポートされたフロー数（1 ～ 30）
4 ～ 7	SysUptime	ルータが起動してから現在までの時間（ミリ秒）
8 ～ 11	unix_secs	0000 UTC 1970 から現在までの秒数
12 ～ 15	unix_nsecs	0000 UTC 1970 からの残り時間（ナノ秒）
16 ～ 19	flow_sequence	観測したフロー全体のシーケンス カウンタ
20 ～ 21	engine_type	フロー スイッチング エンジンのタイプ
21 ～ 23	engine_id	フロー スイッチング エンジンのスロット番号

表 51-2　NDE バージョン 7 ヘッダー形式

バイト	内容	説明
0 ～ 1	version	NetFlow がエクスポートする形式のバージョン番号
2 ～ 3	count	このパケットにエクスポートされたフロー数（1 ～ 30）
4 ～ 7	SysUptime	ルータが起動してから現在までの時間（ミリ秒）
8 ～ 11	unix_secs	0000 UTC 1970 から現在までの秒数
12 ～ 15	unix_nsecs	0000 UTC 1970 からの残り時間（ナノ秒）
16 ～ 19	flow_sequence	観測したフロー全体のシーケンス カウンタ
20 ～ 23	reserved	未使用（ゼロ）バイト

表 51-3　NDE バージョン 5 フロー レコード形式

バイト	内容	説明	フロー マスク ・X= 読み込まれる ・A= 追加のフィールド（「追加の NDE フィールドへのデータの読み込み」（P.51-13）を参照） 送信元	宛先	宛先送信元	宛先送信元インターフェイス	フル	フル インターフェイス
0 ～ 3	srcaddr	送信元 IP アドレス	X	0	X	X	X	X
4 ～ 7	dstaddr	宛先 IP アドレス	0	X	X	X	X	X
8 ～ 11	nexthop	ネクストホップ ルータの IP アドレス。[1]	0	A[2]	A	A	A	A
12 ～ 13	input	入力インターフェイス SNMP ifIndex	0	0	0	X	0	X
14 ～ 15	output	出力インターフェイス SNMP ifIndex[3]	0	A[2]	A	A	A	A
16 ～ 19	dPkts	フロー中のパケット数	X	X	X	X	X	X
20 ～ 23	dOctets	フロー中のオクテット数（バイト）	X	X	X	X	X	X
24 ～ 27	first	フロー開始時の SysUptime（ミリ秒）	X	X	X	X	X	X
28 ～ 31	last	フローの最後のパケット受信時刻の SysUptime（ミリ秒）	X	X	X	X	X	X
32 ～ 33	srcport	レイヤ 4 送信元ポート番号またはそれと同等のもの	0	0	0	0	X[4]	X[4]
34 ～ 35	dstport	レイヤ 4 宛先ポート番号またはそれと同等のもの	0	0	0	0	X	X
36	pad1	未使用（ゼロ）バイト	0	0	0	0	0	0
37	tcp_flags	TCP フラグの累積 OR[5]	0	0	0	0	0	0
38	prot	レイヤ 4 プロトコル（例、6=TCP、17=UDP）	0	0	0	0	X	X
39	tos	IP サービス タイプ バイト	X[6]	X[6]	X[6]	X[6]	X[6]	X[6]
40 ～ 41	src_as	送信元の自律システム番号、起点またはピア	X	0	X	X	X	X
42 ～ 43	dst_as	宛先の自律システム番号、起点またはピア	0	X	X	X	X	X
44 ～ 45	src_mask	送信元アドレス プレフィクス マスク ビット	X	0	X	X	X	X
46 ～ 47	dst_mask	宛先アドレス プレフィクス マスク ビット	0	X	X	X	X	X
48	pad2	Pad 2	0	0	0	0	0	0

1. Policy-Based Routing（PBR; ポリシーベース ルーティング）、WCCP、または Server Load Balancing（SLB; サーバ ロード バランシング）を設定している場合は常に 0 です。
2. 宛先フロー マスクでは、「ネクスト ホップ ルータの IP アドレス」フィールドおよび「出力インターフェイス SNMP ifIndex」フィールドは、すべてのフローに対して正確な情報を含んでいない場合があります。
3. ポリシーベース ルーティングを設定している場合は常に 0 です。
4. PFC3BXL または PFC3B モードでは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）トラフィックのために、ICMP コードおよびタイプ値があります。
5. ハードウェア スイッチド フローでは常に 0 です。
6. PFC3BXL または PFC3B モードで読み込まれます。

表 51-4　NDE バージョン 7 フロー レコード形式

バイト	内容	説明	フロー マスク ・X= 読み込まれる ・A= 追加のフィールド（「追加の NDE フィールドへのデータの読み込み」（P.51-13）を参照）					
			送信元	宛先	宛先送信元	宛先送信元インターフェイス	フル	フルインターフェイス
0 ～ 3	srcaddr	送信元 IP アドレス	X	0	X	X	X	X
4 ～ 7	dstaddr	宛先 IP アドレス	0	X	X	X	X	X
8 ～ 11	nexthop	ネクストホップ ルータの IP アドレス。[1]	0	A[2]	A	A	A	A
12 ～ 13	input	入力インターフェイス SNMP ifIndex	0	0	0	X	0	X
14 ～ 15	output	出力インターフェイス SNMP ifIndex[3]	0	A[2]	A	A	A	A
16 ～ 19	dPkts	フロー中のパケット数	X	X	X	X	X	X
20 ～ 23	dOctets	フロー中のオクテット数（バイト）	X	X	X	X	X	X
24 ～ 27	First	フロー開始時の SysUptime（ミリ秒）	X	X	X	X	X	X
28 ～ 31	Last	フローの最後のパケット受信時刻の SysUptime（ミリ秒）	X	X	X	X	X	X
32 ～ 33	srcport	レイヤ 4 送信元ポート番号またはそれと同等のもの	0	0	0	0	X[4]	X[4]
34 ～ 35	dstport	レイヤ 4 宛先ポート番号またはそれと同等のもの	0	0	0	0	X	X
36	flags	使用中のフロー マスク	X	X	X	X	X	X
37	tcp_flags	TCP フラグの累積 OR[5]	0	0	0	0	0	0
38	prot	レイヤ 4 プロトコル（例、6=TCP、17=UDP）	0	0	0	0	X	X
39	tos	IP サービス タイプ バイト	X[6]	X[6]	X[6]	X[6]	X[6]	X[6]
40 ～ 41	src_as	送信元の自律システム番号、起点またはピア	X	0	X	X	X	X
42 ～ 43	dst_as	宛先の自律システム番号、起点またはピア	0	X	X	X	X	X
44	src_mask	送信元アドレス プレフィクス マスク ビット	X	0	X	X	X	X
45	dst_mask	宛先アドレス プレフィクス マスク ビット	0	X	X	X	X	X
46 ～ 47	pad2	Pad 2	0	0	0	0	0	0
48 ～ 51	Multilayer Switching（MLS; マルチレイヤ スイッチング）RP	MLS ルータの IP アドレス	0	X	X	X	X	X

1. PBR、WCCP、または SLB を設定している場合は常に 0 です。
2. 宛先フロー マスクでは、「ネクスト ホップ ルータの IP アドレス」フィールドおよび「出力インターフェイス SNMP ifIndex」フィールドは、すべてのフローに対して正確な情報を含んでいない場合があります。
3. ポリシーベース ルーティングを設定している場合は常に 0 です。

4. PFC3BXL または PFC3B モードでは、ICMP トラフィックのために、ICMP コードおよびタイプ値があります。
5. ハードウェア スイッチド フローでは常に 0 です。
6. Release 12.2(17b)SXA 以降のリリースで、PFC3BXL または PFC3B モードで読み込まれます。

NetFlow データのエクスポート

NetFlow は、NetFlow テーブル内のアクティブ フローごとにトラフィック統計情報を維持し、各フロー内のパケットがスイッチングされると統計情報を更新します。

NDE はすべての期限切れフローに関するサマリー トラフィック統計情報を定期的にエクスポートします。これを外部データ コレクタで受信して処理することができます。

エクスポートされた NetFlow データには、最後のエクスポート以降に期限切れになった NetFlow テーブル内のフロー エントリの統計情報が含まれます。NetFlow テーブル内のフロー エントリが期限切れになり、次のいずれかの状況が発生した時点で NetFlow テーブルから消去されます。

- エントリは期限切れになります。
- エントリはユーザにより消去されます。
- インターフェイスが停止します。
- ルート フラップが発生します。

継続的なアクティブ フローを定期的にレポートするには、**mls aging long** コマンドで設定されたインターバルの終了時に、継続的なアクティブ フローのエントリを期限切れにします（デフォルトは 32 分）。

期限切れして間もないフロー数が所定の最大数に到達したときに、または所定時間の経過後に NDE パケットは外部データ コレクタに到達します。

- 30 秒（バージョン 5 エクスポートの場合）
- 10 秒（バージョン 9 エクスポートの場合）

デフォルトでは、フィルタリングされない限り、すべての期限切れフローはエクスポートされます。フィルタが設定されていれば、NDE は、フィルタ基準に合致する期限切れで消去されたフローのみをエクスポートします。NDE フロー フィルタは Nonvolatile RAM（NVRAM; 不揮発性 RAM）に保存され、NDE をディセーブルにしても削除されません。NDE フィルタの設定手順については、「NDE フロー フィルタの設定」（P.51-17）を参照してください。

NetFlow サンプリング

NetFlow サンプリングは、ネットワークを通過しているトラフィック フローのサブセットに対する統計情報をレポートする場合に使用します。詳細な分析を行う場合は、NetFlow 統計情報を外部コレクタにエクスポートできます。

NetFlow サンプリングには、NetFlow トラフィック サンプリングと NetFlow フロー サンプリングの 2 種類があります。ソフトウェア パス内でスイッチングされるトラフィックに対する MSFC ベースの NetFlow トラフィック サンプリングと Cisco 6500 シリーズ スイッチのハードウェア パス内でスイッチングされるトラフィックに対する PFC ベースまたは Distributed Forwarding Card（DFC）ベースの NetFlow フロー サンプリングは相互に独立した機能であるため、それぞれの設定手順で使用するコマンドは異なります。

ここでは、Cisco 6500 シリーズ スイッチでサポートされている、この 2 種類の NetFlow サンプリングについて詳しく説明します。

- 「NetFlow トラフィック サンプリング」（P.51-8）
- 「NetFlow フロー サンプリング」（P.51-8）

NetFlow トラフィック サンプリング

NetFlow トラフィック サンプリングでは、ルータまたはスイッチによって処理されるトラフィック中の連続する n 個のパケット（n はユーザが設定可能なパラメータ）からランダムに選択された 1 つのパケットだけを分析することにより、Cisco ルータまたはスイッチによって転送されるトラフィックのサブセットに対する NetFlow データが提供されます。NetFlow トラフィック サンプリングは、ソフトウェア ベースの NetFlow アカウンティングを実行する Cisco 7200 シリーズ ルータや Cisco 6500 シリーズ MSFC などのプラットフォーム上で NetFlow の実行による CPU のオーバーヘッドを低減するために使用されますが、これは NetFlow で分析（サンプリング）されるパケットの数を減らすことによって行われます。ソフトウェア ベースの NetFlow アカウンティングを実行するプラットフォーム上で NetFLow によってサンプリングされるパケットの数を減らすと、外部コレクタにエクスポートする必要があるパケットの数も減ります。分析するパケットの数を減らすことによって外部コレクタにエクスポートする必要があるパケットの数を減らす方法は、すべてのパケットを分析することで発生するエクスポート トラフィックによってコレクタの容量が圧迫されたり、アウトバウンド インターフェイスがオーバーサブスクリプション状態になったりする場合に有効です。

ソフトウェアベースの NetFlow アカウンティングでの NetFlow トラフィック サンプリングおよびエクスポートは、次のように動作します。

- ルータによって認識されているトラフィックのサブセットからの統計情報がフローに読み込まれます。
- フローが期限切れになります。
- 統計情報がエクスポートされます

Cisco 6500 シリーズ スイッチでは、NetFlow トラフィック サンプリングは、ソフトウェアでスイッチングされたパケットに対して MSFC 上でのみサポートされます。NetFlow トラフィック サンプリングの設定の詳細については、『*Cisco IOS NetFlow Configuration Guide*』を参照してください。

NetFlow フロー サンプリング

NetFlow フロー サンプリングでは、NetFlow で分析するパケットの数に制限はありません。NetFlow フロー サンプリングは、エクスポートのためにルータで処理されるフローのサブセットを選択するために使用します。NetFlow フロー サンプリングは、オーバーサブスクライブ状態の CPU の数を減らしたり、オーバーサブスクライブ状態のハードウェア NetFlow テーブルの使用率を低減したりするための解決策ではありません。NetFlow フロー サンプリングは、エクスポートされるデータの量を減らすことによって CPU の使用率を低減します。NetFlow フロー サンプリングを使用してフローのサブセットのみに対する統計情報をレポートすることによって外部コレクタにエクスポートする必要があるパケットの数を減らす方法は、すべてのフローに対する統計情報をレポートすることで発生するエクスポート トラフィックによってコレクタの容量が圧迫されたり、アウトバウンド インターフェイスがオーバーサブスクリプション状態になったりする場合に有効です。

NetFlow フロー サンプリングは、ルータに取り付けられた PFC および DFC 上でハードウェアベースの NetFlow アカウンティングを実行する場合に Cisco Catalyst 6500 シリーズ スイッチ上で使用できます。

ハードウェアベースの NetFlow アカウンティングでの NetFlow フロー サンプリングおよびエクスポートは、次のように動作します。

- パケットがスイッチに着信し、認識されたトラフィックを反映するフローが作成または更新されます。
- フローが期限切れになります。
- エクスポートするフローのサブセットを選択するために、フローがサンプリングされます。
- NetFlow フロー サンプラによって選択されたフローのサブセットに対する統計情報がエクスポートされます。

（注）　NetFlow フロー サンプリングをイネーブルにすると、fast、normal、long などのエージング方式はディセーブルになります。

NetFlow フロー サンプリングを設定して、時間ベースのサンプリングやパケットベースのサンプリングを使用できます。full-interface または destination-source-interface フロー マスクでは、各レイヤ 3 インターフェイスで NetFlow フロー サンプリングをイネーブルまたはディセーブルにできます。

パケットベースの NetFlow フロー サンプリング

パケットベースの NetFlow フロー サンプリングでは、パケット単位のサンプリング レートとミリ秒単位のインターバルに基づいて、ルータで処理されたフローの総数から一定数のフローのサブセット（サンプル）が選択されます。サンプリング レートの値は、64、128、256、512、1024、2048、4096、および 8192 です。インターバルの値は 8000 ～ 16000 ミリ秒の範囲内でユーザが設定できます。インターバルのデフォルトは 16000 ミリ秒です。設定したインターバルの値は、キャッシュからの期限切れのフローに対するエージング方式（fast、normal、long など）を上書きします。パケットベースの NetFlow フロー サンプリングを設定するためのコマンド構文は、
mls sampling packet-based *rate* [*interval*] です。

パケットベースの NetFlow フロー サンプリングでは、次のいずれかの方法により、サンプリングおよびエクスポートのフローが選択されます。

- **期限切れフローのパケット数がサンプリング レートを超える場合**：インターバル X（X は 8000 ～ 16000 の範囲の値）において、フローのパケット数がサンプリング レートに設定した値を超える場合は、フローがサンプリング（選択）され、エクスポートされます。
- **期限切れフローのパケット数がサンプリング レートに満たない場合**：インターバル X（X は 8000 ～ 16000 の範囲の値）において、フローのパケット数がサンプリング レートに設定した値に満たない場合は、フローのパケット数に基づいて、フローのパケット カウントが 8 つのバケットのいずれかに加算されます。この 8 つのバケットのサイズは、サンプリング レートの 1/8 単位の増分です。フローに含まれるパケットの量がサンプリング レートの 0 ～ 1/8 である場合、パケット カウントは最初のバケットに割り当てられます。フローに含まれるパケットの量がサンプリング レートの 1/8 ～ 2/8 である場合、パケット カウントは 2 つめのバケットに割り当てられます。同様に、パケットの量に応じてパケット カウントが割り当てられます。フローのパケット カウントをバケットに追加した結果、バケットのカウンタがサンプリング レートを超えた場合は、バケットにカウンタが追加された最後のフローがサンプリングされ、エクスポートされます。バケット カウンタが 0 に変更され、積算処理が再び開始されます。この方法により、パケット カウントがサンプリング レートを超えることのないフローをサンプリングおよびエクスポート用に選択できます。

時間ベースの NetFlow フロー サンプリング

時間ベースの NetFlow フロー サンプリングでは、エクスポート インターバル（ミリ秒単位）の最初のサンプリング時間（ミリ秒単位）内に作成されたフローがサンプリングされます。
mls sampling time-based *rate* コマンドで設定できる各サンプリング レートは、時間ベースの NetFlow フロー サンプリングで使用されるサンプル時間とエクスポート インターバルの固定値を持ちます。次に、例を示します。

- サンプリング レートとして 64 を設定した場合は、4096 ミリ秒のエクスポート インターバルごとの最初の 64 ミリ秒（サンプリング時間）以内に作成されたフローが選択されます。
- サンプリング レートとして 2048 を設定した場合は、8192 ミリ秒のエクスポート インターバルごとの最初の 4 ミリ秒（サンプリング時間）以内に作成されたフローが選択されます。

表 51-5 に、時間ベースの NetFlow フロー サンプリングのサンプリング レートとエクスポート インターバルを示します。

表 51-5　時間ベースのサンプリングレート、サンプリング時間、およびエクスポート インターバル

サンプリング レート（設定可能）	サンプリング時間（ミリ秒）（設定不可）	エクスポート インターバル（ミリ秒）（設定不可）
1/64	64	4096
1/128	32	4096
1/256	16	4096
1/512	8	4096
1/1024	4	4096
1/2048	4	8192
1/4096	4	16384
1/8192	4	32768

NDE のデフォルト設定

表 51-4 に、NDE のデフォルト設定を示します。

表 51-6　NDE のデフォルト設定

機能	デフォルト値
NDE	ディセーブル
入力ブリッジド IP トラフィックの NDE	ディセーブル
NDE 送信元アドレス	なし
NDE データ コレクタのアドレスおよび UDP ポート	なし
NDE フィルタ	なし
追加の NDE フィールドへのデータの読み込み	イネーブル

NDE 設定時の注意事項および制約事項

NDE を設定する際に、以下の注意事項と制約事項に従ってください。

- NDE は、NetFlow バージョン 9 を使用する場合のみ IP マルチキャスト トラフィックをサポートします。
- NetFlow アグリゲーションでは、NDE バージョン 8 またはバージョン 9 を使用する必要があります。
- Release12.2(18)SXE 以降のリリースでの PFC3B または PFC3BXL モードでは、NDE はブリッジド IP トラフィックをサポートします。PFC3A モードでは、ブリッジド IP トラフィックに対する NDE はサポートされません。
- NDE は、Internetwork Packet Exchange（IPX）トラフィックやその他の非 IP プロトコルをサポートしません。

NDE の設定

ここでは、NDE の設定手順について説明します。

（注）

- PFC 上で NDE をサポートし、MSFC 上で NDE をサポートするには、MSFC レイヤ 3 インターフェイス上で NetFlow をイネーブルにする必要があります。
- PFC で NDE をサポートするには、MSFC 上で NDE をイネーブルにする必要があります。
- インターフェイスで Network Address Translation（NAT; ネットワーク アドレス変換）および NDE を設定する場合、PFC はフラグメント化されたパケット内のトラフィックをすべて MSFC に送信して、ソフトウェアで処理させます （CSCdz51590）。

PFC 上での NDE の設定

ここでは、PFC 上で NDE を設定する手順について説明します。

PFC からの NDE のイネーブル化

PFC からの NDE をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mls nde sender [version {5 | 7}]`	バージョン 7 レコードまたはバージョン 5 レコードを使用して、PFC からの NDE をイネーブルにします。 **version {5 | 7}** キーワードを使用せずに **mls nde sender** コマンドを入力すると、バージョン 7 レコードがデフォルトでイネーブルになります。 **（注）** NDE を使用して WS-X6708-10GE ポートで直接エクスポートする場合は、mls nde sender version 5 コマンドを入力します。
`Router(config)# ip flow-export version 9`	（任意）バージョン 9 レコードの使用をイネーブルにします[1]。 NDE でのバージョン 9 レコードの使用をイネーブルにする場合は、まず **mls nde sender** コマンドを入力する必要があります。 **（注）** バージョン 9 レコードの使用をイネーブルにすると、バージョン 5 レコードまたはバージョン 7 レコードの使用が上書きされます。
`Router(config)# no ip flow-export version 9`	バージョン 9 レコードの使用をディセーブルにします。
`Router(config)# no mls nde sender`	PFC からの NDE をディセーブルにします。

1. **ip flow-export version 9** コマンドが 12.2(18)SXF に統合されました。

（注）

- PFC からの NDE では、MSFC 用に設定された送信元インターフェイスを使用します（「MSFC NDE 送信元レイヤ 3 インターフェイスの設定」（P.51-14）を参照）。
- Release 12.2(18)SXF 以降のリリースでは、NetFlow バージョン 9 がサポートされます。次の URL を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/nfv9expf.htm

次に、PFC からの NDE をイネーブルにする例を示します。

```
Router(config)# mls nde sender
```

次に、PFC からの NDE をイネーブルにし、NDE バージョン 5 を設定する例を示します。

```
Router(config)# mls nde sender version 5
```

追加の NDE フィールドへのデータの読み込み

NDE パケットの次の追加フィールドにデータを読み込むように NDE を設定できます。

- ネクストホップ ルータの IP アドレス
- 出力インターフェイス SNMP ifIndex
- BGP AS

すべての追加フィールドで、すべてのフロー マスクを使用してデータが読み込まれるわけではありません。詳細については、「NDE のバージョン」（P.51-3）を参照してください。

NDE パケットの追加フィールドにデータを読み込むには、次の作業を行います。

コマンド	目的
`Router(config)# mls nde interface`	NDE パケットの追加フィールドにデータを読み込みます。
`Router(config)# no mls nde interface`	追加フィールドへのデータの読み込みをディセーブルにします。

次に、NDE パケットの追加フィールドにデータを読み込む例を示します。

```
Router(config)# mls nde interface
```

NetFlow フロー サンプリングの設定

ここでは、PFC での NetFlow フロー サンプリングを設定する手順について説明します。

- 「グローバルな NetFlow フロー サンプリングの設定」（P.51-13）
- 「レイヤ 3 インターフェイス上での NetFlow フロー サンプリングの設定」（P.51-14）

グローバルな NetFlow フロー サンプリングの設定

NetFlow フロー サンプリングをグローバルに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls sampling {time-based` *rate* `| packet-based` *rate* `[interval]}`	サンプリングされた NetFlow をイネーブルにし、レートを設定します。パケットベースのサンプリングについては、任意でエクスポート インターバルを設定します。
	`Router(config)# no mls sampling`	サンプリングされた NetFlow の設定を消去します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。

NetFlow フロー サンプリングをグローバルに設定する場合は、次の点に注意してください。

- *レート*に対する有効な値は、64、128、256、512、1024、2048、4096、および 8192 です。
- パケットベースのエクスポート*インターバル*の有効な値は 8,000 ～ 16,000 です。
- PFC3 では、データをエクスポートする場合、サンプリングされた NetFlow をレイヤ 3 インターフェイス上で設定する必要もあります。

レイヤ 3 インターフェイス上での NetFlow フロー サンプリングの設定

（注）
- full-interface または destination-source-interface フロー マスクを使用すると、NetFlow フロー サンプリングを個々のレイヤ 3 インターフェイスでイネーブルまたはディセーブルにできます。その他すべてのフロー マスクでは、NetFlow フロー サンプリングはグローバルにイネーブルまたはディセーブルになります。
- レイヤ 3 インターフェイスは IP アドレスで設定する必要があります。

レイヤ 3 インターフェイス上で NetFlow フロー サンプリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {vlan vlan_ID | type slot/port}`	設定するレイヤ 3 インターフェイスを選択します。
ステップ 2	`Router(config-if)# mls netflow sampling`	レイヤ 3 インターフェイス上で NetFlow フロー サンプリングをイネーブルにします。
	`Router(config-if)# no mls netflow sampling`	レイヤ 3 インターフェイス上で NetFlow フロー サンプリングをディセーブルにします。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。

次に、ファスト イーサネット ポート 5/12 上で NetFlow フロー サンプリングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/12
Router(config-if)# mls netflow sampling
Router(config)# end
Router#
```

MSFC 上での NDE の設定

ここでは、MSFC 上で NDE を設定する手順について説明します。

- 「MSFC NDE 送信元レイヤ 3 インターフェイスの設定」（P.51-14）
- 「NDE の宛先の設定」（P.51-15）
- 「NetFlow フロー サンプリングの設定」（P.51-15）

MSFC NDE 送信元レイヤ 3 インターフェイスの設定

MSFC からの統計情報を含む NDE パケットの送信元として使用されるレイヤ 3 インターフェイスを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow-export source {{vlan vlan_ID} | {type slot/port} | {port-channel number} | {loopback number}}`	MSFC からの統計情報を含む NDE パケットの送信元として使用されるインターフェイスを設定します。
`Router(config)# no ip flow-export source`	NDE 送信元インターフェイスの設定を消去します。

MSFC NDE 送信元レイヤ 3 インターフェイスを設定する際は、次の点に注意してください。

- IP アドレスが設定されているインターフェイスを選択する必要があります。
- ループバック インターフェイスを使用できます。

次に、ループバック インターフェイスを NDE フロー送信元として設定する例を示します。

```
Router(config)# ip flow-export source loopback 0
Router(config)#
```

NDE の宛先の設定

NDE 統計を受信するように宛先 IP アドレスおよび UDP ポートを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow-export destination` *ip_address udp_port_number*	NDE の宛先 IP アドレスおよび UDP ポートを設定します。
`Router(config)# no ip flow-export destination` *ip_address udp_port_number*	NDE の宛先の設定を消去します。

（注）　NetFlow の複数のエクスポート先 - 冗長 NDE データ ストリームを設定し、完全な Netflow データが受信される確率を高めるには、**ip flow-export destination** コマンドを 2 度入力し、それぞれのコマンドで別の宛先 IP アドレスを設定します。NetFlow のエクスポート先を複数指定する機能は、次のハードウェアおよびリリースでサポートされます。

- PFC3 および Release12.2(18)SXE 以降のリリース
- PFC2 および Release12.2(18)SXD 以降のリリース

2 つの宛先を設定するとデータ レコードが 2 度エクスポートされるため、RP の CPU 利用率が増加することに注意してください。

次に、NDE フローの宛先 IP アドレスおよび UDP ポートを設定する例を示します。

```
Router(config)# ip flow-export destination 172.20.52.37 200
```

（注）　宛先アドレスおよび UDP ポート番号は NVRAM に保持され、NDE をディセーブルにして再びイネーブルにした場合、またはスイッチの電源をオフ / オンした場合にも、削除されずに残ります。NetFlow FlowCollector アプリケーションを使用してデータ収集を行う場合は、設定した UDP ポート番号が、FlowCollector の /opt/csconfc/config/nfconfig.file ファイルに示されているポート番号と同じであることを確認してください。

NetFlow フロー サンプリングの設定

12.2(18)SXF 以降のリリースでは、MSFC はソフトウェアでルーティングされたトラフィックの NetFlow サンプリングをサポートします。次のマニュアルを参照してください。

詳細については、次のマニュアルを参照してください。

『*Cisco IOS NetFlow Configuration Guide*』

入力ブリッジド IP トラフィックに対する NDE のイネーブル化

Release12.2(18)SXE 以降のリリースでの PFC3B または PFC3BXL モードでは、NDE は入力ブリッジド IP トラフィックをサポートします。PFC3A モードでは、ブリッジド IP トラフィックに対する NDE はサポートされません。

（注）　VLAN 上でブリッジド IP トラフィックの NetFlow をイネーブルにするには、対応する VLAN インターフェイスを作成し、そのインターフェイスに IP アドレスを割り当て、**no shutdown** コマンドを入力してインターフェイスを立ち上げる必要があります。ブリッジされたエクスポート フローは、入出力 VLAN 情報を持ちますが、物理ポート情報は持ちません。

VLAN 上で NetFlow をイネーブルにすると、NDE はデフォルトでイネーブルになります。VLAN 上の入力ブリッジド IP トラフィックに対して NDE をディセーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow export layer2-switched vlan` *vlan_ID*`[-`*vlan_ID*`] [, `*vlan_ID*`[-`*vlan_ID*`]]`	指定の VLAN 上の入力ブリッジド IP トラフィックに対して NDE をイネーブルにします（**ip flow ingress layer2-switched vlan** コマンドを入力すると、デフォルトでイネーブルになります）。 （注）　VLAN 上での入力ブリッジド IP トラフィックに対して NDE を使用するには、**mls nde sender** コマンドを使用して、PFC 上で NDE をイネーブルにする必要があります。
`Router(config)# no ip flow export layer2-switched vlan` *vlan_ID*`[-`*vlan_ID*`] [, `*vlan_ID*`[-`*vlan_ID*`]]`	指定の VLAN 上での入力ブリッジド IP トラフィックに対して NDE をディセーブルにします。

次に、VLAN 200 上の入力ブリッジド IP トラフィックに対して、NDE をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip flow export layer2-switched vlan 200
```

NDE アドレスおよびポートの設定の表示

NDE アドレスおよびポートの設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show mls nde`	NDE エクスポート フローの IP アドレスおよび UDP ポートの設定を表示します。
`Router# show ip flow export`	NDE エクスポート フローの IP アドレス、UDP ポート、および NDE 送信元インターフェイスの設定を表示します。

次に、NDE エクスポート フローの送信元 IP アドレス、および UDP ポートの設定を表示する例を示します。

```
Router# show mls nde
Netflow Data Export enabled
 Exporting flows to  10.34.12.245 (9999)
 Exporting flows from 10.6.58.7 (55425)
 Version: 7
 Include Filter not configured
 Exclude Filter is:
   source:  ip address 11.1.1.0, mask 255.255.255.0
 Total Netflow Data Export Packets are:
    49 packets, 0 no packets, 247 records
 Total Netflow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_OUTPUT_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0
 Netflow Aggregation Enabled
   source-prefix aggregation export is disabled
   destination-prefix aggregation exporting flows to 10.34.12.245 (9999)
10.34.12.246 (9909)
      exported 84 packets, 94 records
   prefix aggregation export is disabled
Router#
```

次に、NDE エクスポート フローの IP アドレス、UDP ポート、および NDE 送信元インターフェイスの設定を表示する例を示します。

```
Router# show ip flow export
Flow export is enabled
  Exporting flows to 172.20.52.37 (200)
  Exporting using source interface FastEthernet5/8
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
Router#
```

NDE フロー フィルタの設定

ここでは、NDE フロー フィルタについて説明します。

NDE フロー フィルタの概要

デフォルトでは、フィルタを設定しない限り、すべての期限切れフローがエクスポートされます。フィルタを設定すると、期限切れになって消去されたフローのうち、指定されたフィルタ基準に合うフローだけがエクスポートされます。フィルタ値は NVRAM に保存され、NDE をディセーブルにしても消去されません。

NDE フロー フィルタの設定を表示するには、**show mls nde** コマンドを使用します（「NDE の設定の表示」（P.51-20）を参照）。

ポート フロー フィルタの設定

宛先または送信元のポート フロー フィルタを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls nde flow** {**exclude** | **include**} {**dest-port** *number* | **src-port** *number*}	NDE フローのポート フロー フィルタを設定します。
Router(config)# **no mls nde flow** {**exclude** | **include**}	ポート フロー フィルタの設定を消去します。

次に、宛先ポート 23 への期限切れフローだけがエクスポートされるように、ポート フロー フィルタを設定する例を示します（フロー マスクは full に設定されているものと想定します）。

```
Router(config)# mls nde flow include dest-port 23
Router(config)#
```

ホストおよびポート フロー フィルタの設定

ホストおよび TCP/UDP ポート フロー フィルタを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls nde flow** {**exclude** | **include**} {**destination** *ip_address mask* | **source** *ip_address mask* {**dest-port** *number* | **src-port** *number*}}	NDE フローのホストおよびポート フロー フィルタを設定します。
Router(config)# **no mls nde flow** {**exclude** | **include**}	ポート フロー フィルタの設定を消去します。

次に、ホスト 171.69.194.140 から宛先ポート 23 への期限切れフローだけがエクスポートされるように、送信元ホストおよび宛先 TCP/UDP ポート フロー フィルタを設定する例を示します（フロー マスクは ip-flow に設定されているものと想定します）。

```
Router(config)# mls nde flow include source 171.69.194.140 255.255.255.255 dest-port 23
```

ホスト フロー フィルタの設定

宛先または送信元のホスト フロー フィルタを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls nde flow** {**exclude** | **include**} {**destination** *ip_address mask* | **source** *ip_address mask* | **protocol** {**tcp** {**dest-port** *number* | **src-port** *number*} | **udp** {**dest-port** *number* | **src-port** *number*}}	NDE フローのホスト フロー フィルタを設定します。
Router(config)# **no mls nde flow** {**exclude** | **include**}	ポート フィルタの設定を消去します。

次に、ホスト 172.20.52.37 へのフローだけがエクスポートされるように、ホスト フロー フィルタを設定する例を示します。

```
Router(config)# mls nde flow include destination 172.20.52.37 255.255.255.225
Router(config)#
```

プロトコル フロー フィルタの設定

プロトコル フロー フィルタを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls nde flow** {**exclude** | **include**} **protocol** {**tcp** {**dest-port** *number* | **src-port** *number*} | **udp** {**dest-port** *number* | **src-port** *number*}}	NDE フローのプロトコル フロー フィルタを設定します。
Router(config)# **no mls nde flow** {**exclude** | **include**}	ポート フィルタの設定を消去します。

次に、宛先ポート 35 からの期限切れフローだけがエクスポートされるように、TCP プロトコル フロー フィルタを設定する例を示します。

```
Router(config)# mls nde flow include protocol tcp dest-port 35
Router(config)#
```

NDE フロー フィルタのステータスを表示するには、**show mls nde** コマンドを使用します（「NDE の設定の表示」（P.51-20）を参照）。

NDE の設定の表示

NDE の設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show mls nde**	NDE の設定を表示します。

次に、NDE の設定を表示する例を示します。

```
Router# show mls nde
 Netflow Data Export enabled
 Exporting flows to  10.34.12.245 (9988)  10.34.12.245 (9999)
 Exporting flows from 10.6.58.7 (57673)
 Version: 7
 Include Filter not configured
 Exclude Filter not configured
 Total Netflow Data Export Packets are:
    508 packets, 0 no packets, 3985 records
 Total Netflow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_OUTPUT_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0
 Netflow Aggregation Enabled
Router#
```

CHAPTER 52

ローカル スイッチド ポート アナライザ（SPAN）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）の設定

この章では、Catalyst 6500 シリーズ スイッチ上でローカル Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）、Remote SPAN（RSPAN）、および Encapsulated RSPAN（ERSPAN）を設定する手順について説明します。Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）を使用する場合は、ERSPAN は Release 12.2(18)SXE 以降のリリースでサポートされます（「ERSPAN に関する注意事項および制約事項」（P.52-13）を参照）。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Optical Services Module（OSM; オプティカル サービス モジュール）WAN ポートおよび FlexWAN ポートは、SPAN、RSPAN、または ERSPAN をサポートしません。
- PFC2 は ERSPAN をサポートしません。

この章で説明する内容は、次のとおりです。

ローカル SPAN、RSPAN、および ERSPAN の機能概要

ここでは、ローカル SPAN、RSPAN、および ERSPAN の機能について説明します。

ローカル SPAN、RSPAN、および ERSPAN の概要

ローカル SPAN、RSPAN、および ERSPAN セッションを使用すると、1 つまたは複数のポート、あるいは 1 つまたは複数の Virtual LAN（VLAN; 仮想 LAN）を対象にトラフィックをモニタし、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することができます。Release 12.2(18)SXD 以降のリリースでは、宛先トランク ポートに VLAN 単位のフィルタリングを設定できます。

ローカル SPAN、RSPAN、および ERSPAN は、SwitchProbe 装置、その他の Remote Monitoring（RMON）プローブなどのネットワーク アナライザにトラフィックを送信します。SPAN は、送信元ポートまたは VLAN 上のトラフィックのスイッチングには影響しません。SPAN は、送信元ポートと VLAN によって送受信されるパケットのコピーを宛先ポートに送信します。その宛先ポートは、SPAN 専用に設定しなければなりません。

ここでは、ローカル SPAN、RSPAN、および ERSPAN の概要を説明します。

ローカル SPAN の概要

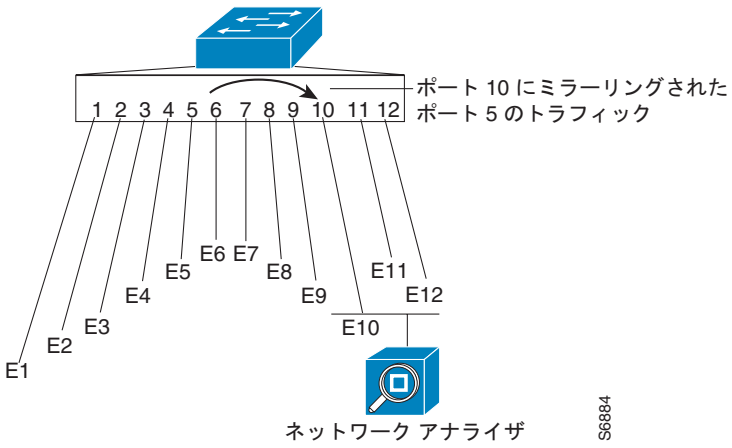
ローカル SPAN セッションは、送信元ポートおよび送信元 VLAN と、1 つまたは複数の宛先ポートを関連付けます。ローカル SPAN セッションを単一のスイッチに設定します。ローカル SPAN には、個別の送信元および宛先のセッションはありません。

ローカル SPAN セッションは、RSPAN VLAN を伝送する送信元トランク ポートからローカルに送信された RSPAN VLAN トラフィックをコピーしません。ローカル SPAN セッションは、送信元ポートからローカルに送信された RSPAN VLAN GRE（総称ルーティング カプセル化）カプセル化トラフィックをコピーしません。

各ローカル SPAN セッションは、ポートまたは VLAN のいずれかを送信元とすることができますが、両方を送信元にすることはできません。

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分析するために宛先ポートへコピーします（図 52-1 を参照）。たとえば、図 52-1 に示すように、イーサネット ポート 5（送信元ポート）上の全トラフィックが、イーサネット ポート 10 にコピーされます。イーサネット ポート 10 のネットワーク アナライザは、イーサネット ポート 5 に物理的に接続していなくても、このポートからのあらゆるトラフィックを受信することができます。

図 52-1　SPAN の設定例



RSPAN の概要

RSPAN は、さまざまなスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク全体に存在する複数のスイッチをリモート モニタします（図 52-2 を参照）。

RSPAN は、RSPAN 送信元セッション、RSPAN VLAN、および RSPAN 宛先セッションで構成されています。RSPAN の送信元セッションと宛先セッションを、さまざまなスイッチ上で個別に設定します。RSPAN 送信元セッションを 1 つのスイッチ上で設定するには、送信元ポートまたは VLAN のセットを RSPAN VLAN に関連付けます。RSPAN 宛先セッションを別のスイッチ上で設定するには、宛先ポートを RSPAN VLAN に関連付けます。

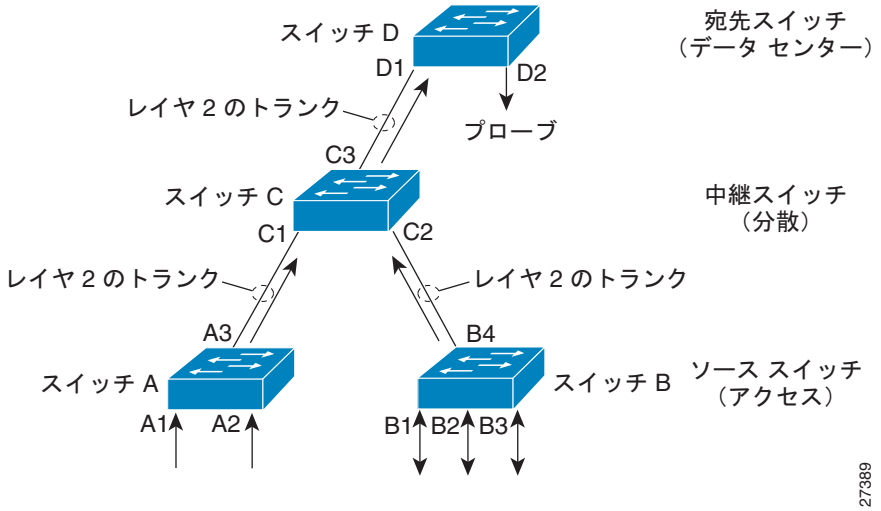
各 RSPAN セッション用のトラフィックは、ユーザ固有の RSPAN VLAN（すべての参加スイッチでその RSPAN セッション専用となっている）経由で、レイヤ 2 の非ルーティング トラフィックとして伝送されます。すべての参加スイッチはレイヤ 2 にトランク接続される必要があります。

RSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートからローカルに送信された RSPAN VLAN トラフィックをコピーしません。RSPAN 送信元セッションは、送信元ポートからローカルに送信された RSPAN GRE カプセル化トラフィックをコピーしません。

各 RSPAN 送信元セッションは、ポートまたは VLAN のいずれかを送信元とすることができますが、両方を送信元にすることはできません。

RSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からのトラフィックをコピーして、RSPAN VLAN のトラフィックを RSPAN 宛先セッションにスイッチングします。RSPAN 宛先セッションでは、トラフィックを宛先ポートにスイッチングします。

図 52-2　RSPAN の設定



ERSPAN の概要

ERSPAN は、さまざまなスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク全体に存在する複数のスイッチをリモート モニタします（図 52-3 を参照）。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。ERSPAN の送信元セッションと宛先セッションを、さまざまなスイッチ上で個別に設定します。

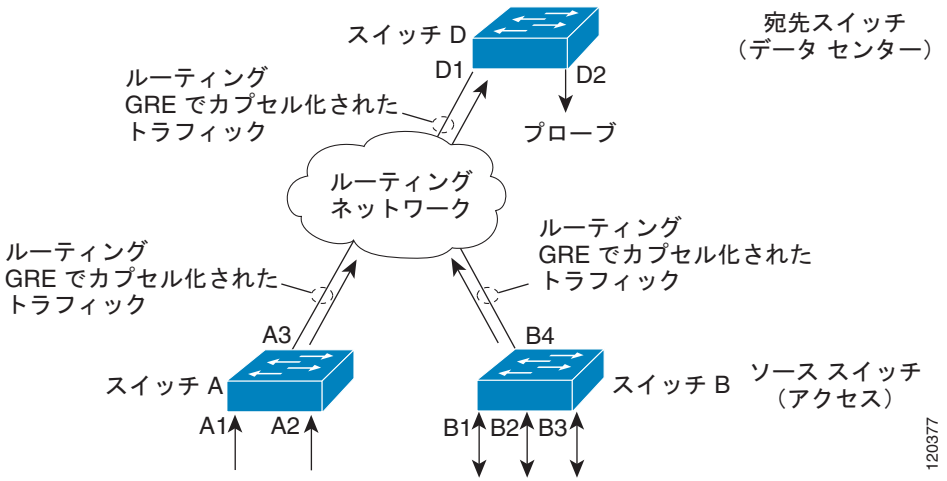
ERSPAN 送信元セッションを 1 つのスイッチ上で設定するには、送信元ポートまたは VLAN のセットを、宛先 IP アドレス、ERSPAN ID 番号、およびオプションとして VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）名に関連付けます。ERSPAN 宛先セッションを別のスイッチ上で設定するには、宛先ポートを、送信元 IP アドレス、ERSPAN ID 番号、およびオプションとして VRF 名に関連付けます。

ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートからローカルに送信された RSPAN VLAN トラフィックをコピーしません。ERSPAN 送信元セッションは、送信元ポートからローカルに送信された ERSPAN GRE カプセル化トラフィックをコピーしません。

各 ERSPAN 送信元セッションは、ポートまたは VLAN のいずれかを送信元とすることができますが、両方を送信元にすることはできません。

ERSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からのトラフィックをコピーして、このトラフィックを、ルーティング可能な GRE カプセル化パケットを使用して ERSPAN 宛先セッションに転送します。ERSPAN 宛先セッションでは、トラフィックを宛先ポートにスイッチングします。

図 52-3　ERSPAN の設定



モニタ対象トラフィック

ここでは、ローカル SPAN、RSPAN、および ERSPAN によってモニタが可能なトラフィックについて説明します。

- 「モニタ対象トラフィックの方向」（P.52-5）
- 「モニタ対象トラフィック」（P.52-5）
- 「重複トラフィック」（P.52-6）

モニタ対象トラフィックの方向

ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションを、入力トラフィックのモニタ（入力 SPAN と呼ばれます）、出力トラフィックのモニタ（出力 SPAN と呼ばれます）、または両方向でのトラフィック フローをモニタするように設定できます。

入力 SPAN は、送信元ポートおよび VLAN が受信したトラフィックを、宛先ポートで分析できるようにコピーします。出力 SPAN は、送信元ポートおよび VLAN が送信したトラフィックをコピーします。**both** キーワードを入力すると、SPAN は送信元ポートおよび VLAN によって送受信されたトラフィックを宛先ポートにコピーします。

モニタ対象トラフィック

デフォルトでは、ローカル SPAN および ERSPAN は、マルチキャストおよび Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フレームを含めて、すべてのトラフィックをモニタします。RSPAN は BPDU モニタをサポートしません。

重複トラフィック

設定によっては、SPAN が、同じ送信元のトラフィックの複数のコピーを、宛先ポートに送信します。たとえば、s1 と s2 という 2 つの SPAN 送信元から、d1 という SPAN 宛先ポートに対して両方向の SPAN セッション（入力および出力の両方）が設定されていて、パケットが、s1 経由でスイッチに入り、そのスイッチから s2 へ出力されるように送信される場合、s1 における入力 SPAN はパケットのコピーを SPAN 宛先ポートの d1 に送信し、s2 における出力 SPAN も、パケットのコピーを SPAN 宛先ポートの d1 に送信します。パケットが s1 から s2 へスイッチングされたレイヤ 2 だった場合、両方の SPAN パケットは同一になります。パケットが s1 から s2 へスイッチングされたレイヤ 3 だった場合、レイヤ 3 の書き換えは送信元と宛先のレイヤ 2 アドレスを変更し、この場合、SPAN パケットは異なるものになります。

ローカル SPAN、RSPAN、および ERSPAN の送信元

ここでは、ローカル SPAN、RSPAN、および ERSPAN の送信元について説明します。

- 「送信元ポート」（P.52-6）
- 「送信元 VLAN」（P.52-6）

送信元ポート

送信元ポートは、トラフィック分析のためにモニタ対象になるポートです。スイッチングおよびルーティングされているポートの両方を、SPAN 送信元ポートとして設定できます。SPAN は、1 つまたは複数の送信元ポートを、単一の SPAN セッションでモニタできます。任意の VLAN に送信元ポートを設定できます。トランク ポートを、送信元ポートとして設定したり、非トランク送信元ポートと混在させることができます。SPAN は、送信元トランク ポートからのカプセル化をコピーしません。

送信元 VLAN

送信元 VLAN は、トラフィック分析のためにモニタ対象になる VLAN です。VLAN-based SPAN（VSPAN; VLAN ベースの SPAN）は、VLAN を SPAN 送信元として使用します。送信元 VLAN にあるすべてのポートが、送信元ポートになります。

ローカル SPAN、RSPAN、および ERSPAN の宛先ポート

宛先ポートは、ローカル SPAN、RSPAN、または ERSPAN が分析用のトラフィックを送信するレイヤ 2 LAN ポートまたはレイヤ 3 LAN ポートです。

ポートを宛先ポートとして設定すると、そのポートはトラフィックを受信することができなくなります。ポートを宛先ポートとして設定すると、そのポートは SPAN 機能によってのみ使用される専用のポートになるからです。SPAN 宛先ポートでは、SPAN セッションに必要なトラフィック以外の転送は行われません。

トランク ポートを宛先ポートとして設定することができます。これによって、宛先トランク ポートがカプセル化したトラフィックを転送することができます。Release 12.2(18)SXD 以降のリリースでは、ローカル SPAN の場合、許可される VLAN のリストを使用して宛先トランク ポートに VLAN 単位のフィルタリングを設定できます（「宛先トランク ポートの VLAN フィルタリングの設定」（P.52-26）を参照）。

ローカル SPAN、RSPAN、および ERSPAN 設定時の注意事項および制約事項

ここでは、ローカル SPAN、RSPAN、および ERSPAN の設定に関する注意事項および制約事項について説明します。

（注）　ERSPAN は Release 12.2(18)SXE 以降のリリースでサポートされます。

機能の非互換性

ローカル SPAN、RSPAN、および ERSPAN には、次のような機能の非互換性問題が存在します。

- 出力 SPAN は出力マルチキャスト モードではサポートされません （CSCsa95965）。
- PFC3 では、Ethernet over MPLS（EoMPLS）ポートを SPAN 送信元として使用できません（CSCed51245）。
- ポートチャネル インターフェイス（EtherChannel）は SPAN 送信元として使用できますが、EtherChannel のアクティブなメンバ ポートを SPAN 送信元ポートとして設定できません。EtherChannel の非アクティブ メンバ ポートは SPAN 送信元として設定できますが、これらのポートは中断ステートになり、トラフィックを伝送しません。
- Release 12.2(33)SXH よりも前のリリースでは、ポートチャネル インターフェイス（EtherChannel）は SPAN 宛先として設定できません。
- SPAN 宛先ポートとして、EtherChannel のアクティブなメンバ ポートを設定できません。EtherChannel の非アクティブ メンバ ポートは SPAN 宛先として設定できますが、これらのポートは中断ステートになり、トラフィックを伝送しません。
- SPAN 宛先ポートは入力トラフィックを廃棄するので、次の機能は SPAN 宛先ポートでは互換性がありません。
  - プライベート VLAN
  - IEEE 802.1X ポートベースの認証
  - ポート セキュリティ
  - Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）および関連機能（PortFast、PortFast BPDU フィルタリング、BPDU ガード、UplinkFast、BackboneFast、EtherChannel ガード、ルート ガード、ループ ガード）
  - VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）
  - Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）
  - IEEE 802.1Q トンネリング

（注）　SPAN 宛先ポートは、IEEE 802.3Z フロー制御に関与できます。

（注）　出力パケット レプリケーションを使用する IP マルチキャスト スイッチングは、SPAN と互換性がありません。出力レプリケーションを使用すると、マルチキャスト パケットが SPAN 宛先ポートに送信されない場合があります。SPAN を使用していて、スイッチング モジュールが出力レプリケーションできる場合は、**mls ip multicast replication-mode ingress** コマンドを入力して出力レプリケーションを強制してください。

ローカル SPAN、RSPAN、および ERSPAN セッションの制限

ここでは、ローカル SPAN、RSPAN、および ERSPAN セッションの制限について説明します。

- 「PFC3」（P.52-8）
- 「PFC2」（P.52-9）

PFC3

PFC3 ローカル SPAN、RSPAN、および ERSPAN セッションの制限は、次のとおりです。

総セッション数	ローカル SPAN、RSPAN、または ERSPAN 送信元セッション	RSPAN 宛先セッション	ERSPAN 宛先セッション
66	2（入力か出力、または両方）	64	23

PFC3 でのローカル SPAN、RSPAN、および ERSPAN 送信元および宛先の制限は、次のとおりです。

	各ローカル SPAN セッション	各 RSPAN 送信元セッション	各 ERSPAN 送信元セッション	各 RSPAN 宛先セッション	各 ERSPAN 宛先セッション
出力または「両方」の送信元				—	—
Release 12.2(18)SXE よりも前のリリース	1	1	1		
Release 12.2(18)SXE 以降のリリース	128	128	128		
入力送信元				—	—
Release 12.2(18)SXD よりも前のリリース	64	64	64		
Release 12.2(18)SXD 以降のリリース	128	128	128		
RSPAN および ERSPAN 宛先セッションの送信元	—	—	—	1 RSPAN VLAN	1 IP アドレス
セッションごとの宛先	64	1 RSPAN VLAN	1 IP アドレス	64	64

PFC2

（注）
- ローカル SPAN セッションの出力 SPAN 送信元を設定する場合、PFC2 は RSPAN をサポートしません。
- RSPAN を設定する場合、PFC2 はローカル SPAN の出力 SPAN 送信元をサポートしません。

PFC2 でのローカル SPAN および RSPAN セッションの制限は、次のとおりです。

総セッション数	ローカル SPAN セッション	RSPAN 送信元セッション	RSPAN 宛先セッション
66	2（入力か出力、または両方）	0	64
	1（入力）	1（入力か出力、または両方）	64
	1 または 2（出力）	0	64

PFC2 でのローカル SPAN および RSPAN 送信元および宛先の制限は、次のとおりです。

	各ローカル SPAN セッション	各 RSPAN 送信元セッション	各 RSPAN 宛先セッション
出力または「両方」の送信元			—
Release 12.2(18)SXF2 よりも前のリリース	1（リモート SPAN 送信元セッションが設定されている場合 0）	1（ローカル SPAN 出力送信元セッションが設定されている場合 0）	
Release 12.2(18)SXF2 以降のリリース	128	128	
入力送信元			—
Release 12.2(18)SXD よりも前のリリース	64	64	
Release 12.2(18)SXD 以降のリリース	128	128	
RSPAN 宛先セッションの送信元	—	—	1 RSPAN VLAN
セッションごとの宛先	64	1 RSPAN VLAN	64

ローカル SPAN、RSPAN、および ERSPAN の注意事項および制約事項

ローカル SPAN、RSPAN、および ERSPAN には、次の注意事項および制約事項が適用されます。

- 1 つの出力 SPAN 送信元ポートからトラフィックをコピーした SPAN 宛先ポートは、出力トラフィックのみをネットワーク アナライザに送信します。ただし、Release 12.2(18)SXE 以降のリリースでは、複数の出力 SPAN 送信元ポートを設定している場合は、ネットワーク アナライザに送信されるトラフィックに、出力 SPAN 送信元ポートから受信した特定タイプの入力トラフィックも含まれます。この入力トラフィックのタイプは次のとおりです。
  - VLAN 上でフラッディングしたすべてのユニキャスト トラフィック
  - ブロードキャストおよびマルチキャスト トラフィック

  この状況が発生するのは、出力 SPAN 送信元ポートはこれらのトラフィック タイプを VLAN から受信したあと、自身がトラフィックの送信元であることを認識し、受信したトラフィックの送信元にこのトラフィックを返送せず、廃棄してしまうためです。SPAN は廃棄する前にこのトラフィックをコピーし、SPAN 宛先ポートに送信します （CSCds22021）。
- **monitor session** コマンドを追加して入力しても、前に設定した SPAN パラメータは消去されません。設定済みの SPAN パラメータを削除するには、**no monitor session** コマンドを使用する必要があります。
- ネットワーク アナライザを SPAN 宛先ポートに接続します。
- すべての SPAN 宛先ポートは、すべてのトラフィックをすべての SPAN 送信元から受信します。

（注） Release 12.2(18)SXD 以降のリリースでは、許可される VLAN のリストを使用して、宛先トランク ポート VLAN フィルタリングを設定できます（「宛先トランク ポートの VLAN フィルタリングの設定」（P.52-26）を参照）。

Release 12.2(18)SXE 以降のリリースでは、ローカル SPAN および RSPAN の場合は、送信元 VLAN フィルタリングを設定できます（「ローカル SPAN および RSPAN の送信元 VLAN フィルタリングの設定」（P.52-25）を参照）。

- レイヤ 2 LAN ポート（**switchport** コマンドを使用して設定された LAN ポート）とレイヤ 3 LAN ポート（**switchport** コマンドで設定されていないポート）の両方を送信元または宛先として設定できます。
- 1 つのセッションに、個別の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。
- 複数の入力送信元ポートを指定する場合、各ポートはそれぞれ異なる VLAN に属するものであってもかまいません。
- 1 つのセッション内では、送信元 VLAN とフィルタ VLAN を混在させることはできません。送信元 VLAN またはフィルタ VLAN を使用できますが、両方を同時に使用することはできません。
- ローカル SPAN、RSPAN、および ERSPAN をイネーブルにすると、すでに入力された設定があれば、その設定が使用されます。
- 送信元を指定し、トラフィックの方向（入力、出力、または両方）を指定しない場合、「両方」がデフォルトで使用されます。
- SPAN は、レイヤ 2 イーサネット フレームをコピーしますが、SPAN は送信元トランク ポート Inter Switch Link（ISL; スイッチ間リンク）や 802.1Q タグをコピーしません。宛先ポートをトランクとして設定して、ローカルにタグ付けされたトラフィックをトラフィック アナライザに送信できます。

（注）　トランクとして設定した宛先ポートは、レイヤ 3 LAN 送信元ポートからのトラフィックを、レイヤ 3 LAN ポートによって使用される内部 VLAN としてタグを付けます。

- ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートからローカルに送信された RSPAN VLAN トラフィックをコピーしません。
- ローカル SPAN セッション、RSPAN 送信元セッション、および ERSPAN 送信元セッションは、送信元ポートからローカルに送信された ERSPAN GRE カプセル化トラフィックをコピーしません。
- 1 つの SPAN セッションで宛先ポートとして指定されたポートは、別の SPAN セッションの宛先ポートにすることはできません。
- 宛先ポートとして設定されたポートは、送信元ポートとして設定できません。
- 宛先ポートは、スパニング ツリー インスタンスには関与しません。ローカル SPAN はモニタ対象トラフィックに BPDU を含めます。したがって、宛先ポートで確認される BPDU は、送信元ポートから送られたものです。RSPAN は BPDU モニタをサポートしません。
- 出力送信元として設定されているポートからの伝送用にスイッチを経由して送信されるすべてのパケットは、宛先ポートにコピーされます。このパケットには、STP がポートをブロッキング ステートにするためポート経由でスイッチから送出されないパケットや、STP が VLAN をトランク ポートでブロッキング ステートに移行するので、トランク ポートにあるパケットが含まれます。

VSPAN に関する注意事項および制約事項

（注）　ローカル SPAN、RSPAN、および ERSPAN は、すべて VSPAN をサポートします。

ここでは、VSPAN に関する注意事項および制約事項について説明します。

- 入力および出力の両方が設定されている VSPAN セッションについては、2 つのパケットが同じ VLAN でスイッチングされている場合、それらは宛先ポートから（1 つは入力ポートからの入力トラフィックとして、もう 1 つは出力ポートからの出力トラフィックとして）転送されます。
- VSPAN は、VLAN 中のレイヤ 2 ポートから出入りするトラフィックのみをモニタします。
  - VLAN を入力送信元として設定し、トラフィックが、モニタされている VLAN へとルーティングされると、そのルーティングされたトラフィックは、VLAN 中のレイヤ 2 ポートで受信する入力トラフィックとして見なされないためモニタされません。
  - VLAN を出力送信元として設定し、トラフィックが、モニタされている VLAN からルーティングされると、そのルーティングされたトラフィックは、VLAN 中のレイヤ 2 ポートから送信される出力トラフィックとして見なされないためモニタされません。

RSPAN に関する注意事項および制約事項

ここでは、RSPAN に関する注意事項および制約事項について説明します。

- ローカル SPAN セッションの出力 SPAN 送信元を設定する場合、Supervisor Engine 2 は RSPAN をサポートしません。
- RSPAN を設定する場合、Supervisor Engine 2 はローカル SPAN の出力 SPAN 送信元をサポートしません。
- すべての参加スイッチはレイヤ 2 にトランク接続される必要があります。
- RSPAN VLAN をサポートするネットワーク装置は、RSPAN 中間装置とすることができます。
- ネットワークが伝送する RSPAN VLAN の数に制限はありません。
- 中間ネットワーク装置は、サポートすることができる RSPAN VLAN の数を制限することがあります。
- すべての送信元、中間、宛先ネットワーク装置において、RSPAN VLAN を設定しなければなりません。VTP がイネーブルの場合、1 ～ 1024 の番号が付いた VLAN の設定を RSPAN VLAN として伝播できます。1024 より大きい番号の VLAN は、すべての送信元、中間、および宛先ネットワーク装置で、RSPAN VLAN として手動で設定する必要があります。
- VTP および VTP プルーニングをイネーブルにすると、RSPAN トラフィックはトランクでプルーニングされて、RSPAN トラフィックがネットワーク全体に不必要にフラッディングするのを防ぎます。
- RSPAN VLAN は、RSPAN トラフィックに対してのみ使用できます。
- 管理トラフィックを伝送するのに使用する VLAN を、RSPAN VLAN として設定しないでください。
- アクセス ポートを RSPAN VLAN に割り当てないでください。RSPAN は、RSPAN VLAN 中のアクセス ポートを中断ステートにします。
- RSPAN トラフィックを伝送するために選択されたトランク ポートを除き、RSPAN VLAN にはポートを設定しないでください。
- Media Access Control（MAC; メディア アクセス制御）アドレス学習は、RSPAN VLAN でディセーブルにされます。
- RSPAN 送信元スイッチにある RSPAN VLAN で、出力 Access Control List（ACL; アクセス制御リスト）を使用して、RSPAN 宛先へ送信されるトラフィックをフィルタリングできます。
- RSPAN は BPDU モニタをサポートしません。
- RSPAN VLAN を VSPAN セッション中の送信元として設定しないでください。
- 参加ネットワーク装置のすべてが RSPAN VLAN の設定をサポートし、参加ネットワーク装置のすべてで各 RSPAN セッションに対して同じ RSPAN VLAN を使用する限り、VLAN を RSPAN VLAN として設定できます。

ERSPAN に関する注意事項および制約事項

ここでは、ERSPAN に関する注意事項および制約事項について説明します。

- ERSPAN は Release 12.2(18)SXE 以降のリリースでサポートされます。
- Release 12.2(18)SXE 以降のリリースでは、スイッチがどのスイッチング モードで動作している場合でも、ERSPAN がサポートされます （CSCec70695）。
- Release 12.2(18)SXE およびリビルドでは、スイッチが compact スイッチング モードで動作している場合に限り、ERSPAN がサポートされますが、すべてのモジュールがファブリック対応である必要があります。
- 次のスーパーバイザ エンジンは ERSPAN をサポートします。
  - PFC3B または PFC3BXL を搭載したスーパーバイザ エンジンは ERSPAN をサポートします。
  - WS-SUP720（PFC3A を搭載した Supervisor Engine 720）は、ハードウェア バージョン 3.2 以上の場合に限り、ERSPAN をサポートします。ハードウェア バージョンを確認するには、**show module version | include WS-SUP720-BASE** コマンドを入力してください。次に、例を示します。

    ```
    Router# show module version | include WS-SUP720-BASE
     7    2  WS-SUP720-BASE     SAD075301SZ Hw :3.2
    ```

  - スーパーバイザ エンジンが ERSPAN をサポートしていることを確認するには、該当するスーパーバイザ エンジンに対して **show asic-version slot** *slot_number* **| include ASIC|HYPERION** コマンドを入力します。次に、例を示します。

    ```
    Router# show asic-version slot 1 | include ASIC|HYPERION
    Module in slot 1 has 2 type(s) of ASICs
            ASIC Name      Count      Version
             HYPERION          1      (6.0)
    ```

    Hyperion バージョン 2.0 以上は ERSPAN をサポートしていません。
- Supervisor Engine 2 は、ERSPAN をサポートしていません。
- ERSPAN パケットでは、GRE ヘッダー内の「protocol type」フィールドの値は 0x88BE です。
- レイヤ 3 ERSPAN パケットのペイロードは、コピーされたレイヤ 2 イーサネット フレームからすべての ISL または 802.1Q タグを取り除いたものです。
- ERSPAN は、コピーされた個々のレイヤ 2 イーサネット フレームに 50 バイトのヘッダーを追加し、4 バイトの Cyclic Redundancy Check（CRC; 巡回冗長検査）トレーラと置き換えます。
- ERSPAN は、最大 9,202 バイトのレイヤ 3 パケットを保持するジャンボ フレームをサポートします。コピーされたレイヤ 2 イーサネット フレームの長さが 9,170（9,152 バイトのレイヤ 3 パケット）を超える場合は、ERSPAN はコピーされたレイヤ 2 イーサネット フレームを切り捨て、9,202 バイトの ERSPAN レイヤ 3 パケットを作成します。
- 設定された MTU サイズとは関係なく、ERSPAN は最長 9,202 バイトのレイヤ 3 パケットを作成します。ERSPAN トラフィックは、MTU サイズを 9,202 バイト未満に規定しているネットワーク内のインターフェイスによって廃棄される可能性があります。
- デフォルトの MTU サイズ（1,500 バイト）の場合、コピーされたレイヤ 2 イーサネット フレームの長さが 1,468 バイト（1,450 バイトのレイヤ 3 パケット）を超えると、MTU サイズを 1,500 バイトに規定しているネットワーク内のインターフェイスによって ERSPAN トラフィックは廃棄されます。

（注）　**mtu** インターフェイス コマンド、および **system jumbomtu** コマンド（「ジャンボ フレームのサポートの設定」（P.9-10）を参照）は、レイヤ 3 パケットの最大サイズを設定します（デフォルト値は 1,500 バイト、最大値は 9,216 バイト）。

- すべての参加スイッチはレイヤ 3 に接続されている必要があり、ネットワーク パスが ERSPAN トラフィックのサイズをサポートしている必要があります。
- ERSPAN はパケット分割をサポートしません。「do not fragment」ビットは、ERSPAN パケットの IP ヘッダー内で設定されます。ERSPAN 宛先セッションでは、分割された ERSPAN パケットを再構成できません。
- ERSPAN トラフィックは、ネットワークのトラフィック負荷条件の影響を受けます。ERSPAN パケットの IP precedence または DSCP 値を設定することで、QoS において ERSPAN トラフィックを優先できます。
- ERSPAN トラフィックでサポートされる唯一の宛先は、PFC3 上の ERSPAN 宛先セッションです。
- スイッチ上のすべての ERSPAN 送信元セッションには、同一の起点 IP アドレスを使用する必要があります。これは、**origin ip address** コマンドによって設定します（「ERSPAN 送信元セッションの設定」（P.52-20）を参照）。
- スイッチ上のすべての ERSPAN 宛先セッションは、同じ宛先インターフェイス上の同一の IP アドレスを使用する必要があります。宛先インターフェイスの IP アドレスは、**ip address** コマンドを使用して入力します（「ERSPAN 宛先セッションの設定」（P.52-23）を参照）。
- ERSPAN 送信元セッションの宛先 IP アドレス（宛先スイッチのインターフェイス上で設定する必要がある）は、ERSPAN 宛先セッションが宛先ポートまで送信するトラフィックの送信元です。**ip address** コマンドを使用して、送信元セッションおよび宛先セッションの両方に同一のアドレスを設定します。
- ERSPAN ID は、さまざまな ERSPAN 送信元セッションから送られ、同一の宛先 IP アドレスに到着した ERSPAN トラフィックを区別します。

ローカル SPAN、RSPAN、および ERSPAN の設定

ここでは、ローカル SPAN、RSPAN、および ERSPAN の設定手順について説明します。

宛先ポートの許可リストの設定（任意）

ポートを誤って宛先として設定してしまうことがないように、宛先として有効なポートの一覧を示す許可リストを作成できます。宛先ポートの許可リストを設定すると、許可リスト内のポートだけが宛先として設定できるようになります。

宛先ポートの許可リストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor permit-list`	宛先ポートの許可リストの使用をイネーブルにします。
ステップ 3	`Router(config)# no monitor permit-list`	宛先ポートの許可リストの使用をディセーブルにします。
ステップ 4	`Router(config)# monitor permit-list destination interface` *type*[1] *slot/port*[*-port*] [*,* *type*[1] *slot/port - port*]	宛先ポートの許可リストを設定するか、または既存の宛先ポート許可リストに追加します。
ステップ 5	`Router(config)# no monitor permit-list destination interface` *type*[1] *slot/port*[*-port*] [*,* *type*[1] *slot/port - port*]	既存の宛先ポート許可リストを削除または消去します。
ステップ 6	`Router(config)# do show monitor permit-list`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ギガビット イーサネット ポート 5/1 ～ 5/4、および 6/1 を含む宛先ポート許可リストを設定する例を示します。

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

次に、設定を確認する例を示します。

```
Router(config)# do show monitor permit-list
 SPAN Permit-list      :Admin Enabled
 Permit-list ports     :Gi5/1-4,Gi6/1
```

ローカル SPAN の設定

ローカル SPAN は、個別の送信元および宛先のセッションを使用しません。ローカル SPAN セッションを設定するには、同じセッション番号のローカル SPAN 送信元および宛先を設定します。ローカル SPAN セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor session local_span_session_number source {{single_interface | interface_list | interface_range | mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]}`	ローカル SPAN 送信元セッション番号と送信元ポートまたは VLAN を関連付けて、モニタするトラフィックの方向を選択します。
ステップ 3	`Router(config)# monitor session local_span_session_number destination {single_interface | interface_list | interface_range | mixed_interface_list}` `Router(config)# no monitor session {session_number | all | local | range session_range[[,session_range],...]}`	ローカル SPAN セッション番号と宛先ポートを関連付けます。 モニタ設定を消去します。

ローカル SPAN セッションを設定する際は、次の点に注意してください。

- *local_span_session_number* は 1 ～ 66 の範囲で指定できます。
- *single_interface* は **interface** *type slot*/*port* の形式で、*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注） 各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は **interface** *type slot*/*first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- モニタ対象トラフィックが宛先ポートを出る際、タグ付けを行うには、宛先ポートを無条件にトランクに設定してから、そのポートを宛先として設定します（「無条件トランクとしての宛先ポートの設定」（P.52-25）を参照）。

モニタ セッションを消去する際は、次の点に注意してください。

- 他のパラメータを指定しないで入力された **no monitor session** *number* コマンドは、セッションの *session_number* を消去します。
- *session_range* は *first_session_number-last_session_number* です。

（注）　**no monitor session range** コマンドでは、ダッシュの前後にスペースを入れません。複数の範囲を入力する場合、カンマの前後にスペースを入れないでください。

次に、セッション 1 の双方向送信元として、ファスト イーサネット ポート 5/1 を設定する例を示します。

```
Router(config)# monitor session 1 source interface fastethernet 5/1
```

次に、SPAN セッション 1 の宛先として、ファスト イーサネット ポート 5/48 を設定する例を示します。

```
Router(config)# monitor session 1 destination interface fastethernet 5/48
```

追加の例については、「設定例」（P.52-28）を参照してください。

RSPAN の設定

RSPAN では、1 つのスイッチで送信元セッションを使用し、別のスイッチで宛先セッションを使用します。ここでは、RSPAN セッションの設定手順について説明します。

- 「RSPAN VLAN の設定」（P.52-17）
- 「RSPAN 送信元セッションの設定」（P.52-18）
- 「RSPAN 宛先セッションの設定」（P.52-19）

RSPAN VLAN の設定

VLAN を RSPAN VLAN として設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# vlan` *vlan_ID*{[-*vlan_ID*]|[,*vlan_ID*])	単独のイーサネット VLAN、イーサネット VLAN の範囲、またはカンマで区切った複数のイーサネット VLAN のリストを作成または変更します（スペースは挿入しないでください）。
ステップ 3	`Router(config-vlan)# remote-span` `Router(config-vlan)# no remote-span`	VLAN を RSPAN VLAN として設定します。 RSPAN VLAN の設定を消去します。
ステップ 4	`Router(config-vlan)# end`	VLAN データベースを更新して、イネーブル EXEC モードに戻ります。

RSPAN 送信元セッションの設定

RSPAN 送信元セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor session` *RSPAN_source_session_number* **source** {{*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]}}	RSPAN 送信元セッションの番号と送信元ポートまたは VLAN を関連付けて、モニタするトラフィックの方向を選択します。
ステップ 3	`Router(config)# monitor session` *RSPAN_source_session_number* **destination remote vlan** *rspan_vlan_ID*	RSPAN 送信元セッションの番号と RSPAN VLAN を関連付けます。
ステップ 4	`Router(config)# no monitor session` {*session_number* | **all** | **range** *session_range*[[,*session_range*],...] | **remote**}	モニタ設定を消去します。

モニタ セッションを設定する際は、次の点に注意してください。

- RSPAN VLAN を設定するには、「RSPAN VLAN の設定」（P.52-17）を参照してください。
- *RSPAN_source_span_session_number* は 1 ～ 66 の範囲で指定できます。
- *single_interface* は **interface** *type slot*/*port* の形式で、*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注） 各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は **interface** *type slot*/*first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。

モニタ セッションを消去する際は、次の点に注意してください。

- 他のパラメータを指定しないで入力された **no monitor session** *number* コマンドは、セッションの *session_number* を消去します。
- *session_range* は *first_session_number-last_session_number* です。

（注） **no monitor session range** コマンドでは、ダッシュの前後にスペースを入れません。複数の範囲を入力する場合、カンマの前後にスペースを入れないでください。

次に、セッション 2 の送信元として、ファスト イーサネット ポート 5/2 を設定する例を示します。

```
Router(config)# monitor session 2 source interface fastethernet 5/2
```

次に、RSPAN VLAN 200 をセッション 2 の宛先として設定する例を示します。

```
Router(config)# monitor session 2 destination remote vlan 200
```

追加の例については、「設定例」（P.52-28）を参照してください。

RSPAN 宛先セッションの設定

（注） RSPAN 送信元セッション スイッチ上に RSPAN 宛先セッションを設定して、RSPAN トラフィックをローカルにモニタすることができます。

RSPAN 宛先セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor session` *RSPAN_destination_session_number* **source remote vlan** *rspan_vlan_ID*	RSPAN 宛先セッション番号と RSPAN VLAN を関連付けます。
ステップ 3	`Router(config)# monitor session` *RSPAN_destination_session_number* **destination** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*}}	RSPAN 宛先セッション番号と宛先ポートを関連付けます。
ステップ 4	`Router(config)# no monitor session` {*session_number* | **all** | **range** *session_range*[[,*session_range*],...] | **remote**}	モニタ設定を消去します。

モニタ セッションを設定する際は、次の点に注意してください。

- モニタ対象トラフィックにタグ付けをするには、ポートを無条件にトランクに設定してから、そのポートを宛先として設定する必要があります（「無条件トランクとしての宛先ポートの設定」（P.52-25）を参照）。
- *RSPAN_destination_span_session_number* は 1 ～ 66 の範囲で指定できます。
- *single_interface* は **interface** *type slot*/*port* の形式で、*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

  （注） 各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は **interface** *type slot*/*first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。

モニタ セッションを消去する際は、次の点に注意してください。

- 他のパラメータを指定しないで入力された、**no monitor session** *number* コマンドは、セッションの *session_number* を消去します。
- *session_range* は *first_session_number-last_session_number* です。

（注）　**no monitor session range** コマンドでは、ダッシュの前後にスペースを入れません。複数の範囲を入力する場合、カンマの前後にスペースを入れないでください。

次に、RSPAN VLAN 200 をセッション 3 の送信元として設定する例を示します。

```
Router(config)# monitor session 3 source remote vlan 200
```

次に、セッション 3 の宛先として、ファスト イーサネット ポート 5/47 を設定する例を示します。

```
Router(config)# monitor session 3 destination interface fastethernet 5/47
```

追加の例については、「設定例」（P.52-28）を参照してください。

ERSPAN の設定

ERSPAN では、個別の送信元セッションおよび宛先セッションを使用します。送信元セッションと宛先セッションは、異なるスイッチ上に設定します。ここでは、ERSPAN セッションの設定手順について説明します。

- 「ERSPAN 送信元セッションの設定」（P.52-20）
- 「ERSPAN 宛先セッションの設定」（P.52-23）

（注）　PFC3 を使用する場合は、ERSPAN は Release 12.2(18)SXE 以降のリリースでサポートされます（「ERSPAN に関する注意事項および制約事項」（P.52-13）を参照）。

ERSPAN 送信元セッションの設定

ERSPAN 送信元セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor session` *ERSPAN_source_session_number* `type erspan-source`	ERSPAN 送信元セッション番号を設定し、このセッションに対する ERSPAN 送信元セッション コンフィギュレーション モードを開始します。
	`Router(config)# no monitor session {`*session_number* `|` `all |` `range` *session_range*`[[,`*session_range*`],...]}`	モニタ設定を消去します。
ステップ 3	`Router(config-mon-erspan-src)# description` *session_description*	（任意）ERSPAN 送信元セッションの説明を入力します。
ステップ 4	`Router(config-mon-erspan-src)# shutdown`	（デフォルト）ERSPAN 送信元セッションを非アクティブにします。
	`Router(config-mon-erspan-src)# no shutdown`	ERSPAN 送信元セッションをアクティブにします。

	コマンド	目的
ステップ 5	`Router(config-mon-erspan-src)# source {{single_interface | interface_list | interface_range | mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]}`	ERSPAN 送信元セッションの番号と送信元ポートまたは VLAN を関連付けて、モニタするトラフィックの方向を選択します。
ステップ 6	`Router(config-mon-erspan-src)# filter single_vlan | vlan_list | vlan_range | mixed_vlan_list`	（任意）ERSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。
ステップ 7	`Router(config-mon-erspan-src)# destination`	ERSPAN 送信元セッションの宛先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	`Router(config-mon-erspan-src-dst)# ip address ip_address`	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチのインターフェイス上でも設定する必要があるほか、ERSPAN 宛先セッションの設定でも入力する必要があります（「ERSPAN 宛先セッションの設定」（P.52-23）、ステップ 7 を参照）。
ステップ 9	`Router(config-mon-erspan-src-dst)# erspan-id ERSPAN_flow_id`	ERSPAN トラフィックを識別するため、送信元および宛先セッションで使用される ID 番号を設定します。これは、ERSPAN 宛先セッションの設定でも入力する必要があります（「ERSPAN 宛先セッションの設定」（P.52-23）、ステップ 8 を参照）。
ステップ 10	`Router(config-mon-erspan-src-dst)# origin ip address ip_address [force]`	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
ステップ 11	`Router(config-mon-erspan-src-dst)# ip ttl ttl_value`	（任意）ERSPAN トラフィック内のパケットの IP Time to Live（TTL; 存続可能時間）値を設定します。
ステップ 12	`Router(config-mon-erspan-src-dst)# ip prec ipp_value`	（任意）ERSPAN トラフィック内のパケットの IP precedence 値を設定します。
ステップ 13	`Router(config-mon-erspan-src-dst)# ip dscp dscp_value`	（任意）ERSPAN トラフィック内のパケットの IP DSCP 値を設定します。
ステップ 14	`Router(config-mon-erspan-src-dst)# vrf vrf_name`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 15	`Router(config-mon-erspan-src-dst)# end`	コンフィギュレーション モードを終了します。

モニタ セッションを設定する際は、次の点に注意してください。

- *session_description* には最大 240 文字を使用できます。ただし、特殊文字またはスペースは使用できません。

（注）　**description** コマンドに続けて、240 文字を入力できます。

- *ERSPAN_source_span_session_number* は 1 ～ 66 の範囲で指定できます。
- *single_interface* は **interface** *type slot/port* の形式で、*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は **interface** *type slot/first_port - last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID - last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。
- *ERSPAN_flow_id* は 1 ～ 1023 の範囲で指定できます。
- 1 つのスイッチのすべての ERSPAN 送信元セッションは、同一の送信元 IP アドレスを使用する必要があります。スイッチ上ですべての ERSPAN 送信元セッションに設定された起点 IP アドレスを変更するには、**origin ip address** *ip_address* **force** コマンドを入力します。
- *ttl_value* は 1 ～ 255 の範囲で指定できます。
- *ipp_value* は 0 ～ 7 の範囲で指定できます。
- *dscp_value* は 0 ～ 63 の範囲で指定できます。

モニタ セッションを消去する際は、次の点に注意してください。

- 他のパラメータを指定しないで入力された **no monitor session** *number* コマンドは、セッションの *session_number* を消去します。
- *session_range* は *first_session_number-last_session_number* です。

（注） **no monitor session range** コマンドでは、ダッシュの前後にスペースを入れません。複数の範囲を入力する場合、カンマの前後にスペースを入れないでください。

次に、ギガビット イーサネット ポート 4/1 からの双方向トラフィックをモニタするようにセッション 3 を設定する例を示します。

```
Router(config)# monitor session 3 type erspan-source
Router(config-mon-erspan-src)# source interface gigabitethernet 4/1
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)# ip address 10.1.1.1
Router(config-mon-erspan-src-dst)# origin ip address 20.1.1.1
Router(config-mon-erspan-src-dst)# erspan-id 101
```

追加の例については、「設定例」（P.52-28）を参照してください。

ERSPAN 宛先セッションの設定

（注）　ERSPAN トラフィックをローカルにモニタできません。

ERSPAN 宛先セッションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# monitor session ERSPAN_destination_session_number type erspan-destination`	ERSPAN 宛先セッション番号を設定し、このセッションに対する ERSPAN 宛先セッション コンフィギュレーション モードを開始します。
	`Router(config)# no monitor session {session_number | all | range session_range[[,session_range],...]}`	モニタ設定を消去します。
ステップ 3	`Router(config-mon-erspan-dst)# description session_description`	（任意）ERSPAN 宛先セッションの説明を入力します。
ステップ 4	`Router(config-mon-erspan-dst)# shutdown`	（デフォルト）ERSPAN 宛先セッションを非アクティブにします。
	`Router(config-mon-erspan-dst)# no shutdown`	ERSPAN 宛先セッションをアクティブにします。
ステップ 5	`Router(config-mon-erspan-dst)# destination {single_interface | interface_list | interface_range | mixed_interface_list}`	ERSPAN 宛先セッション番号と宛先ポートを関連付けます。
ステップ 6	`Router(config-mon-erspan-dst)# source`	ERSPAN 宛先セッションの送信元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	`Router(config-mon-erspan-dst-src)# ip address ip_address [force]`	ERSPAN フローの宛先 IP アドレスを設定します。これは、ローカル インターフェイス上のアドレスであり、「ERSPAN 送信元セッションの設定」（P.52-20）のステップ 8 で入力したアドレスと一致する必要があります。
ステップ 8	`Router(config-mon-erspan-dst-src)# erspan-id ERSPAN_flow_id`	ERSPAN トラフィックを識別するため、宛先および宛先セッションで使用される ID 番号を設定します。これは、「ERSPAN 送信元セッションの設定」（P.52-20）、ステップ 9 で入力した ID と一致する必要があります。
ステップ 9	`Router(config-mon-erspan-dst-src)# vrf vrf_name`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 10	`Router(config-mon-erspan-dst-src)# end`	コンフィギュレーション モードを終了します。

モニタ セッションを設定する際は、次の点に注意してください。

- *ERSPAN_destination_span_session_number* は 1 ～ 66 の範囲で指定できます。
- *single_interface* は **interface** *type slot*/*port* の形式で、*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。

- *interface_list* は *single_interface* , *single_interface* , *single_interface* ... です。

（注）　各リストでは、カンマの前後にスペースを入れる必要があります。各範囲では、ダッシュの前後にスペースを入れる必要があります。

- *interface_range* は **interface** *type slot*/*first_port* - *last_port* です。
- *mixed_interface_list* は、順不同で *single_interface* , *interface_range* , ... です。
- スイッチ上のすべての ERSPAN 宛先セッションは、同じ宛先インターフェイス上の同一の IP アドレスを使用する必要があります。スイッチ上ですべての ERSPAN 宛先セッションに設定された IP アドレスを変更するには、**ip address** *ip_address* **force** コマンドを入力します。

（注）　また、すべての ERSPAN 送信元セッションの宛先 IP アドレスを変更する必要があります（「ERSPAN 送信元セッションの設定」（P.52-20）、ステップ 8 を参照）。

- *ERSPAN_flow_id* は 1 ～ 1023 の範囲で指定できます。

モニタ セッションを消去する際は、次の点に注意してください。

- 他のパラメータを指定しないで入力された **no monitor session** *number* コマンドは、セッションの *session_number* を消去します。
- *session_range* は *first_session_number-last_session_number* です。

（注）　**no monitor session range** コマンドでは、ダッシュの前後にスペースを入れません。複数の範囲を入力する場合、カンマの前後にスペースを入れないでください。

次に、IP アドレス 10.1.1.1 に着信した ERSPAN ID 101 トラフィックを、ギガビット イーサネット ポート 2/1 に送信するように ERSPAN 宛先セッションを設定する例を示します。

```
Router(config)# monitor session 3 type erspan-destination
Router(config-erspan-dst)# destination interface gigabitethernet 2/1
Router(config-erspan-dst)# source
Router(config-erspan-dst-src)# ip address 10.1.1.1
Router(config-erspan-dst-src)# erspan-id 101
```

追加の例については、「設定例」（P.52-28）を参照してください。

ローカル SPAN および RSPAN の送信元 VLAN フィルタリングの設定

送信元 VLAN フィルタリングは、送信元がトランク ポートの場合に特定の VLAN をモニタします。

（注）　ERSPAN の送信元 VLAN フィルタリングを設定する方法については、「ERSPAN の設定」（P.52-20）を参照してください。

ローカル SPAN または RSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	`Router(config)# monitor session session_number filter single_vlan | vlan_list | vlan_range | mixed_vlan_list`
	
	`Router(config)# no monitor session session_number filter single_vlan | vlan_list | vlan_range | mixed_vlan_list`
		ローカル SPAN または RSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。
		送信元 VLAN フィルタリングを消去します。

送信元 VLAN フィルタリングを設定する場合は、次の点に注意してください。

- *single_vlan* は、単一の VLAN の ID 番号です。
- *vlan_list* は *single_vlan* , *single_vlan* , *single_vlan* ... です。
- *vlan_range* は、*first_vlan_ID* - *last_vlan_ID* です。
- *mixed_vlan_list* は、順不同で *single_vlan* , *vlan_range* , ... です。

次に、送信元がトランク ポートである場合に、VLAN 1 ～ 5 および VLAN 9 をモニタする例を示します。

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

無条件トランクとしての宛先ポートの設定

モニタ対象トラフィックが宛先ポートを出る際、タグ付けを行うには、宛先ポートをトランクとして設定します。

宛先ポートをトランクとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 3	`Router(config-if)# switchport`	LAN ポートをレイヤ 2 スイッチング用に設定します（この操作は LAN ポートがレイヤ 2 スイッチング用に設定されていない場合にのみ必要です）。
ステップ 4	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	カプセル化を設定して、レイヤ 2 スイッチング ポートを ISL または 802.1Q トランクとして設定します。

	コマンド	目的
ステップ 5	`Router(config-if)# switchport mode trunk`	無条件にポートをトランクに設定します。
ステップ 6	`Router(config-if)# switchport nonegotiate`	DTP を使用しないようにトランクを設定します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポートを無条件 IEEE 802.1Q トランクとして設定する例を示します。

```
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
```

宛先トランク ポートの VLAN フィルタリングの設定

（注） トランクで VLAN をフィルタリングするだけでなく、許可される VLAN リストをアクセス ポートに適用することもできます。

Release 12.2(18)SXD 以降のリリースでは、宛先ポートがトランクの場合、トランクで許可される VLAN のリストを使用して宛先ポートから送信されるトラフィックをフィルタリングできます（CSCeb01318）。

宛先トランク ポート VLAN フィルタリングを使用すると、すべての宛先ポートがすべての送信元からのすべてのトラフィックを受信するという制約がなくなります。宛先トランク ポート VLAN フィルタリングでは、各宛先トランク ポートからネットワーク アナライザに送信されたトラフィックを、VLAN 単位で選択できます。

宛先トランク ポートに宛先トランク ポート VLAN フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface` *type*[1] *slot/port*	設定する宛先トランク ポートを選択します。
ステップ 3	`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]]`	トランク上で許可される VLAN のリストを設定します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

宛先トランク ポートで許可される VLAN のリストを設定する際は、次の点に注意してください。

- *vlan* パラメータは、1 ～ 4094 の範囲の単一の VLAN 番号、または 2 つの VLAN 番号（小さい番号が先、ダッシュで区切る）で指定する VLAN 範囲です。カンマで区切った *vlan* パラメータの間、またはダッシュ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。
- すべての VLAN を許可されたリストから削除するには、**switchport trunk allowed vlan none** コマンドを入力します。

- VLAN を許可されたリストに追加するには、**switchport trunk allowed vlan add** コマンドを入力します。
- SPAN 設定を削除せずに許可された VLAN リストを変更できます。

次に、複数の VLAN が送信元で複数のトランク ポートが宛先であるローカル SPAN セッションを設定する例を示します。宛先トランク ポート VLAN フィルタリングは SPAN トラフィックをフィルタリングし、各宛先トランク ポートが、1 つの VLAN からトラフィックを伝送します。

```
interface GigabitEthernet1/1
description SPAN destination interface for VLAN 10
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/2
description SPAN destination interface for VLAN 11
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 11
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/3
description SPAN destination interface for VLAN 12
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 12
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/4
description SPAN destination interface for VLAN 13
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 13
switchport mode trunk
switchport nonegotiate
!
monitor session 1 source vlan 10 - 13
monitor session 1 destination interface Gi1/1 - 4
```

設定の確認

設定を確認するには、**show monitor session** コマンドを入力します。

次に、セッション 2 の設定を確認する例を示します。

```
Router# show monitor session 2
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa3/1
Dest RSPAN VLAN:   901
Router#
```

次に、セッション 2 の詳細を完全に表示する例を示します。

```
Router# show monitor session 2 detail
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa1/1-3
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:      None
Dest RSPAN VLAN:   901
```

設定例

次に、RSPAN 送信元セッション 2 を設定する例を示します。

```
Router(config)# monitor session 2 source interface fastethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

次に、セッション 1 とセッション 2 の設定を消去する例を示します。

```
Router(config)# no monitor session range 1-2
```

次に、複数の送信元で RSPAN 送信元セッションを設定する例を示します。

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

次に、セッションの送信元を削除する例を示します。

```
Router(config)# no monitor session 2 source interface fastethernet 5/15 , 7/3
```

次に、セッションの送信元に対するオプションを削除する例を示します。

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

次に、セッションの VLAN フィルタリングを削除する例を示します。

```
Router(config)# no monitor session 2 filter vlan 3
```

次に、RSPAN 宛先セッション 8 の設定例を示します。

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

次に、ERSPAN 送信元セッション 12 の設定例を示します。

```
monitor session 12 type erspan-source
 description SOURCE_SESSION_FOR_VRF_GRAY
 source interface Gi8/48 rx
 destination
  erspan-id 120
  ip address 10.8.1.2
  origin ip address 32.1.1.1
  vrf gray
```

次に、ERSPAN 宛先セッション 12 の設定例を示します。

```
monitor session 12 type erspan-destination
 description DEST_SESSION_FOR_VRF_GRAY
 destination interface Gi4/48
 source
  erspan-id 120
  ip address 10.8.1.2
  vrf gray
```

次に、ERSPAN 送信元セッション 13 の設定例を示します。

```
monitor session 13 type erspan-source
 source interface Gi6/1 tx
 destination
  erspan-id 130
  ip address 10.11.1.1
  origin ip address 32.1.1.1
```

次に、ERSPAN 宛先セッション 13 の設定例を示します。

```
monitor session 13 type erspan-destination
 destination interface Gi6/1
 source
  erspan-id 130
  ip address 10.11.1.1
```

CHAPTER 53

SNMP ifIndex の持続性の設定

この章では、Catalyst 6500 シリーズ スイッチに Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）Interface Index（ifIndex）の持続性を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

SNMP ifIndex の持続性の概要

SNMP ifIndex の持続性の機能は、スイッチが再起動するときに保持され使用されているインターフェイス インデックス（ifIndex）値を提供します。ifIndex 値は、物理または、論理インターフェイスに関連する一意の識別番号です。

関連する RFC では、特定の ifIndex 値とインターフェイス間のやりとりが、スイッチの再起動時に維持されているための要件はありませんが、多くのアプリケーション（たとえば、装置目録、課金情報、障害検出）は、このやりとりの維持を必要とします。

インターフェイスを ifIndex に関連付けるのに、一定のインターバルでスイッチをポーリングすることができますが、定期的にポーリングすることは実用的ではありません。SNMP ifIndex の持続性機能は、持続的な ifIndex 値を提供し、それによってインターフェイスをポーリングする必要がなくなります。

以下の定義は、RFC 2233「The Interfaces Group MIB using SMIv2」に基づいています。以下の用語は、Interfaces MIB（IF-MIB; インターフェイス管理情報ベース）内の値です。

- **ifIndex** - そのインターフェイスの SNMP ID に対する各インターフェイスを識別する一意の番号（0 より大きい）。
- **ifName** - インターフェイスのテキストベースの名前。[ethernet 3/1] など。
- **ifDescr** - インターフェイスの説明。この説明用の推奨情報としては、メーカー名、製品名、インターフェイスのハードウェアとソフトウェアのバージョンがあります。

SNMP ifIndex の持続性の設定

ここでは、SNMP ifIndex の持続性の設定手順について説明します。

- 「SNMP ifIndex の持続性のグローバルなイネーブル化」（P.53-2）（任意）
- 「特定のインターフェイス上における SNMP ifIndex の持続性のイネーブル化およびディセーブル化」（P.53-3）（任意）

（注）　ifIndex コマンドが設定されていることを確認するには、**more system:running-config** コマンドを使用します。

SNMP ifIndex の持続性のグローバルなイネーブル化

SNMP ifIndex の持続性は、デフォルトでディセーブルになります。SNMP ifIndex の持続性をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# snmp-server ifindex persist`	SNMP ifIndex の持続性をグローバルにイネーブルにします。

次の例では、SNMP ifIndex の持続性をすべてのインターフェイスでイネーブルにします。

```
router(config)# snmp-server ifindex persist
```

SNMP ifIndex の持続性のグローバルなディセーブル化

SNMP ifIndex の持続性をイネーブルにしたあとディセーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# no snmp-server ifindex persist`	SNMP ifIndex の持続性をグローバルにディセーブルにします。

次の例では、SNMP ifIndex の持続性がすべてのインターフェイスでディセーブルにされます。

```
router(config)# no snmp-server ifindex persist
```

特定のインターフェイス上における SNMP ifIndex の持続性のイネーブル化およびディセーブル化

特定のインターフェイス上でのみ、SNMP ifIndex の持続性をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {vlan vlan_ID}	{type[1] slot/port}	{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 2	`Router(config-if)# snmp ifindex persist`	特定のインターフェイスで SNMP ifIndex の持続性をイネーブルにします。
	`Router(config-if)# no snmp ifindex persist`	特定のインターフェイスで SNMP ifIndex の持続性をディセーブルにします。
ステップ 3	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

1. *type* = サポートされているインターフェイスのタイプ

（注）　**[no] snmp ifindex persistence** インターフェイス コマンドは、サブインターフェイスで使用することはできません。インターフェイスに適用されるコマンドは、そのインターフェイスに関連するすべてのサブインターフェイスに自動的に適用されます。

次の例では、SNMP ifIndex の持続性が、イーサネット インターフェイス 3/1 でのみイネーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex persist
router(config-if)# exit
```

次の例では、SNMP ifIndex の持続性が、イーサネット インターフェイス 3/1 でのみディセーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# no snmp ifindex persist
router(config-if)# exit
```

特定のインターフェイスにおける SNMP ifIndex の持続性設定の消去

インターフェイス固有の SNMP ifIndex の持続性設定を消去し、インターフェイスがグローバル コンフィギュレーション設定を使用するように設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type slot/port`	特定のインターフェイスのインターフェイス 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 コマンドの構文は使用しているプラットフォームにより異なることに注意してください。
ステップ 2	`Router(config-if)# snmp ifindex clear`	インターフェイス固有の SNMP ifIndex 持続性設定を消去し、グローバル コンフィギュレーション設定に戻します。
ステップ 3	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

次の例では、イーサネット インターフェイス 3/1 における SNMP ifIndex の持続性に対する以前の設定を、コンフィギュレーションから削除します。SNMP ifIndex の持続性がグローバルにイネーブルに設定されている場合、SNMP ifIndex の持続性はイーサネット インターフェイス 3/1 でイネーブルになります。SNMP ifIndex の持続性がグローバルにディセーブルに設定されている場合、SNMP ifIndex の持続性は、イーサネット インターフェイス 3/1 でディセーブルになります。

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex clear
router(config-if)# exit
```

CHAPTER 54

電源管理および環境モニタ

この章では、Catalyst 6500 シリーズ スイッチの電源管理および環境モニタ機能について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

電源管理の機能概要

ここでは、Catalyst 6500 シリーズ スイッチの電源管理について説明します。

（注） システムの電源装置を冗長構成にする場合は、両方の電源装置のワット数が同じでなければなりません。Catalyst 6500 シリーズ スイッチでは、同一シャーシ内で AC 入力および DC 入力電源装置の両方を使用できます。サポートされる電源構成の詳細については、『*Catalyst 6500 Series Switch Installation Guide*』を参照してください。

モジュールは、所要電力がそれぞれ異なります。構成によっては、必要とされる電力が 1 台の電源装置では足りない場合があります。電源管理機能を使用すると、電源装置 2 台で搭載されたモジュールすべてに電力供給できます。ただし、両方の電源装置から供給される合計電力が 1 台の電源装置の電力容量よりも大きくなることはないので、冗長構成はこの構成ではサポートされません。ここでは、冗長および非冗長の電源構成について説明します。

システムの所要電力については、「システムの所要電力の判別」（P.54-5）を参照してください。

電源の冗長構成のイネーブル化またはディセーブル化

冗長構成をディセーブルまたはイネーブルにするには（デフォルトでイネーブル）、グローバル コンフィギュレーション モードで **power redundancy-mode combined** | **redundant** コマンドを入力します。電源装置の構成は、いつでも冗長または非冗長に変更できます。

冗長構成をディセーブルにするには、**combined** キーワードを使用します。非冗長構成では、システムで使用できる電力量は、2 台の電源装置で供給できる合計電力です。システムは合計電力量の許容範囲以内であれば、何個でもモジュールに電力を供給できます。ただし、1 台の電源装置が故障し、それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合、システムは十分な電力を供給できないモジュールの電源を切断します。

冗長構成をイネーブルにするには、**redundant** キーワードを使用します。冗長構成では、両方の電源装置から供給される合計電力が、1 台の電源装置の電力容量よりも大きくなることはありません。1 台の電源装置が故障した場合、もう 1 台がシステムの負荷全体を引き継ぎます。2 台の電源装置を搭載して電源をオンにすると、それぞれの電源装置がシステムに必要な電力の約半分を同時に供給します。負荷分散と冗長構成は自動的にイネーブルになるので、ソフトウェアの設定は必要ありません。

各モジュールの現在のステートおよび使用できる総電力量を表示するには、**show power** コマンドを使用します（「システムの電力ステータスの確認」（P.54-4）を参照）。

表 54-1 に、電源装置の構成を変更した場合のシステムへの影響について説明します。

表 54-1　電源装置の構成を変更した場合の影響

構成の変更内容	影響
冗長から非冗長へ	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、**show power** コマンド出力の [oper state] フィールドで [*power-deny*] と表示されていたモジュールに電源が入ります。
非冗長から冗長へ（両方の電源装置でワット数が同じであるものとします）	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、一方の電源装置の電力量に減少します。 • それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては **show power** コマンド出力の [oper state] フィールドで [*power-deny*] と表示されます。
冗長構成がイネーブルで、同じワット数の電源装置を取り付けた場合	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、一方の電源装置の電力量と等しくなります。 • 供給できる電力量には変化がないので、モジュールのステータスは変化しません。
冗長構成がディセーブルで、同じワット数の電源装置を取り付けた場合	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、**show power** コマンド出力の [oper state] フィールドで [*power-deny*] と表示されていたモジュールに電源が入ります。

表 54-1　電源装置の構成を変更した場合の影響 （続き）

構成の変更内容	影響
冗長構成がイネーブルで、ワット数がより大きいまたは小さい電源装置を取り付けた場合	• システム ログと、Syslog メッセージが生成されます。 • 取り付けた電源装置のワット数がすでに搭載されている電源装置のワット数より大きくても、システムはワット数の異なる電源装置の使用を認めません。新しく取り付けた電源装置はシャットダウンされます。
冗長構成がディセーブルで、ワット数がより大きいまたは小さい電源装置を取り付けた場合	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、両方の電源装置の合計電力量に増加します。 • 十分な電力がある場合、**show power** コマンド出力の [oper state] フィールドで [*power-deny*] と表示されていたモジュールに電源が入ります。
冗長構成がイネーブルの電源装置を取り外した場合	• システム ログと、Syslog メッセージが生成されます。 • 供給できる電力量には変化がないので、モジュールのステータスは変化しません。
冗長構成がディセーブルの電源装置を取り外した場合	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、一方の電源装置の電力量に減少します。 • それまでに電力が供給されていた全モジュールに供給できる十分な電力がない場合は、一部のモジュールの電源が切断され、そのモジュールについては **show power** コマンド出力の [oper state] フィールドで [*power-deny*] と表示されます。
冗長構成がイネーブルで、ワット数が異なる電源装置を取り付けてシステムを起動した場合	• システム ログと、Syslog メッセージが生成されます。 • システムは、冗長構成ではワット数の異なる電源装置の使用を認めません。ワット数の小さい方の電源装置がシャットダウンされます。
冗長構成がディセーブルで、ワット数が等しいかまたは異なる電源装置を取り付けてシステムを起動した場合	• システム ログと、Syslog メッセージが生成されます。 • システムの電力が、両方の電源装置の合計電力と等しくなります。 • システムは合計電力量の許容範囲以内であれば、何個でもモジュールに電力を供給できます。

モジュールの電源切断および電源投入

モジュールの電源を Command-Line Interface（CLI; コマンドライン インターフェイス）から切断および投入するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# power enable module slot_number`	モジュールに電源を投入します。
	`Router(config)# no power enable module slot_number`	モジュールの電源を切断します。

（注） **no power enable module** *slot* コマンドを使用してモジュールの電源を切断した場合、そのモジュールの設定は保存されません。

次に、スロット 3 のモジュールに電源投入する例を示します。

```
Router# configure terminal
Router(config)# power enable module 3
```

システムの電力ステータスの確認

各システム コンポーネントの現在の電力ステータスを表示するには、次のように **show power** コマンドを使用します。

```
Router# show power
system power redundancy mode = redundant
system power total =     1153.32 Watts (27.46 Amps @ 42V)
system power used =       397.74 Watts ( 9.47 Amps @ 42V)
system power available =  755.58 Watts (17.99 Amps @ 42V)
                        Power-Capacity PS-Fan Output Oper
PS   Type               Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
1    WS-CAC-2500W       1153.32 27.46  OK     OK     on
2    none
                        Pwr-Requested  Pwr-Allocated  Admin Oper
Slot Card-Type          Watts   A @42V Watts   A @42V State State
---- ------------------ ------- ------ ------- ------ ----- -----
1    WS-X6K-SUP2-2GE     142.38  3.39   142.38  3.39  on    on
2                          -     -      142.38  3.39  -     -
5    WS-X6248-RJ-45      112.98  2.69   112.98  2.69  on    on
Router#
```

特定の電源の現在の電力ステータスを表示するには、次のように **show power** コマンドを使用します。

```
Router# show power status power-supply 2
                        Power-Capacity PS-Fan Output Oper
PS   Type               Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
1    WS-CAC-6000W       2672.04  63.62 OK     OK     on
2    WS-CAC-9000W-E     2773.68  66.04 OK     OK     on
Router#
```

電源の入力フィールドを表示するには、コマンドに電源番号を指定します。複数の出力モードを持つ電源に対し、新規の電源出力フィールド、および動作モードが表示されます。次のように **show env status power-supply** コマンドを入力します。

```
Router# show env status power-supply 1
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-input 1: AC low
  power-supply 1 power-output-fail: OK
Router# show env status power-supply 2
power-supply 2:
  power-supply 2 fan-fail: OK
  power-supply 2 power-input 1: none<<< new
  power-supply 2 power-input 2: AC low<<< new
  power-supply 2 power-input 3: AC high<<< new
  power-supply 2 power-output: low (mode 1)<<< high for highest mode only
  power-supply 2 power-output-fail: OK
```

モジュールの電源オフ/オン

モジュールの電源をオフ/オン（リセット）するには、グローバル コンフィギュレーション モードで **power cycle module** *slot* コマンドを使用します。モジュールの電源は 5 秒間オフになり、それからオンになります。

システムの所要電力の判別

電源装置のサイズにより、システムの所要電力が異なります。1000 W および 1300 W の電源装置を使用する場合、シャーシのサイズ、および搭載するモジュールのタイプによって、構成が制約される場合があります。電力消費の詳細については、次の URL にある『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm

システムのハードウェア容量の判別

Release 12.2(18)SXF 以降のリリースでは、**show platform hardware capacity** コマンドを入力することで、システムのハードウェア容量を判別できます。このコマンドは、ハードウェア リソースの現在のシステム利用率を表示し、現在使用可能なハードウェア容量を一覧表示します。この内容は次のとおりです。

- ハードウェア転送テーブルの利用率
- スイッチ ファブリックの利用率
- CPU（1 つまたは複数）の利用率
- メモリ装置（フラッシュ、DRAM、NVRAM（不揮発性 RAM））の利用率

次に、Catalyst 6500 シリーズ スイッチのルート プロセッサ、スイッチ プロセッサ、および LAN モジュールに対する CPU 容量とその利用率情報を表示する例を示します。

```
Router# show platform hardware capacity cpu
CPU Resources
  CPU utilization: Module             5 seconds       1 minute       5 minutes
                   1  RP               0% /  0%            1%             1%
                   1  SP               5% /  0%            5%             4%
                   7                  69% /  0%           69%            69%
                   8                  78% /  0%           74%            74%

  Processor memory: Module   Bytes:       Total           Used       %Used
                    1  RP              176730048       51774704       29%
                    1  SP              192825092       51978936       27%
                    7                  195111584       35769704       18%
                    8                  195111584       35798632       18%
  I/O memory: Module         Bytes:       Total           Used       %Used
              1  RP                     35651584       12226672       34%
              1  SP                     35651584        9747952       27%
              7                         35651584        9616816       27%
              8                         35651584        9616816       27%
Router#
```

次に、Catalyst 6500 シリーズ スイッチのルート プロセッサ、スイッチ プロセッサ、および DFC に対する EOBC 関連の統計情報を表示する例を示します。

```
Router# show platform hardware capacity eobc EOBC Resources
  Module                      Packets/sec     Total packets     Dropped packets
  1  RP      Rx:                       61            108982                   0
             Tx:                       37             77298                   0
  1  SP      Rx:                       34            101627                   0
             Tx:                       39            115417                   0
  7          Rx:                        5             10358                   0
             Tx:                        8             18543                   0
  8          Rx:                        5             12130                   0
             Tx:                       10             20317                   0
Router#
```

次に、現在、およびピーク時のスイッチング利用率を表示する例を示します。

```
Router# show platform hardware capacity fabric Switch Fabric Resources
  Bus utilization: current is 100%, peak was 100% at 12:34 12mar45
  Fabric utilization:      ingress                      egress
      Module channel speed current peak                 current peak
       1      0        20G   100%  100% 12:34 12mar45  100%    100% 12:34 12mar45
       1      1        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
       4      0        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
      13      0         8G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
Router#
```

次に、システム内のフラッシュおよび NVRAM リソースに対する合計容量、使用バイト数、および利用率（%）を表示する例を示します。

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
  Usage: Module Device               Bytes:      Total          Used     %Used
         1  RP  bootflash:                    31981568      15688048       49%
         1  SP  disk0:                      128577536     105621504       82%
         1  SP  sup-bootflash:               31981568      29700644       93%
         1  SP  const_nvram:                   129004           856        1%
         1  SP  nvram:                         391160         22065        6%
         7      dfc#7-bootflash:            15204352        616540        4%
         8      dfc#8-bootflash:            15204352             0        0%
Router#
```

次に、システム内の EARL に対する容量および利用率を表示する例を示します。

```
Router# show platform hardware capacity forwarding
L2 Forwarding Resources
           MAC Table usage:   Module  Collisions  Total       Used     %Used
                              6               0  65536         11        1%
             VPN CAM usage:                       Total       Used     %Used
                                                    512          0        0%
L3 Forwarding Resources
              FIB TCAM usage:                     Total       Used     %Used
                   72 bits (IPv4, MPLS, EoM)     196608         36        1%
                  144 bits (IP mcast, IPv6)       32768          7        1%

                      detail:      Protocol                   Used     %Used
                                   IPv4                         36        1%
                                   MPLS                          0        0%
                                   EoM                           0        0%

                                   IPv6                          4        1%
                                   IPv4 mcast                    3        1%
                                   IPv6 mcast                    0        0%

            Adjacency usage:                     Total       Used     %Used
                                                1048576        175        1%

     Forwarding engine load:
                      Module       pps   peak-pps  peak-time
                      6              8       1972  02:02:17 UTC Thu Apr 21 2005

Netflow Resources
          TCAM utilization:       Module       Created      Failed     %Used
                                  6                 1           0        0%
          ICAM utilization:       Module       Created      Failed     %Used
                                  6                 0           0        0%

                 Flowmasks:   Mask#   Type        Features
                        IPv4:     0   reserved    none
                        IPv4:     1   Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
                        IPv4:     2   unused      none
                        IPv4:     3   reserved    none

                        IPv6:     0   reserved    none
                        IPv6:     1   unused      none
                        IPv6:     2   unused      none
                        IPv6:     3   reserved    none

CPU Rate Limiters Resources
             Rate limiters:       Total         Used      Reserved     %Used
                    Layer 3           9            4             1       44%
                    Layer 2           4            2             2       50%

ACL/QoS TCAM Resources
  Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
       QoSent - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
       Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
       LOUdst - LOU destination, ADJ - ACL adjacency

  Module ACLent ACLmsk QoSent QoSmsk Lbl-in Lbl-eg LOUsrc LOUdst  AND OR  ADJ
  6          1%     1%     1%     1%     1%     1%     0%     0%   0% 0%   1%

Router#
```

次に、インターフェイス リソースを表示する例を示します。

```
Router# show platform hardware capacity interface Interface Resources
  Interface drops:
    Module    Total drops:    Tx            Rx      Highest drop port: Tx  Rx
    9                          0             2                          0  48

  Interface buffer sizes:
    Module                              Bytes:     Tx buffer           Rx buffer
         1                                            12345               12345
         5                                            12345               12345
Router#
```

次に、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）情報を表示する例を示します。

```
Router# show platform hardware capacity monitor SPAN Resources
  Source sessions: 2 maximum, 0 used
    Type                                    Used
    Local                                      0
    RSPAN source                               0
    ERSPAN source                              0
    Service module                             0
  Destination sessions: 64 maximum, 0 used
    Type                                    Used
    RSPAN destination                          0
    ERSPAN destination (max  24)               0
Router#
```

次に、レイヤ 3 マルチキャスト機能の各リソースに対する容量および利用率を表示する例を示します。

```
Router# show platform hardware capacity multicast
L3 Multicast Resources
  IPv4 replication mode: ingress
  IPv6 replication mode: ingress
  Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used
  Replication capability: Module                                IPv4     IPv6
                          5                                   egress   egress
                          9                                  ingress  ingress
  MET table Entries: Module                                Total    Used    %Used
                     5                                     65526       6       0%
Router#
```

次に、システム電源の容量および利用率情報を表示する例を示します。

```
Router# show platform hardware capacity power
Power Resources
  Power supply redundancy mode: administratively combined operationally combined
  System power: 1922W, 0W (0%) inline, 1289W (67%) total allocated
  Powered devices: 0 total
Router#
```

次に、Catalyst 6500 シリーズ スイッチ内の各 EARL に対する Quality of Service（QoS; サービス品質）ポリサー リソースの容量および利用率を表示する例を示します。

```
Router# show platform hardware capacity qos
QoS Policer Resources
  Aggregate policers: Module                      Total         Used     %Used
                      1                            1024          102       10%
                      5                            1024            1        1%
  Microflow policer configurations: Module        Total         Used     %Used
                                     1               64           32       50%
                                     5               64            1        1%
Router#
```

次に、重要なシステム リソースについての情報を表示する例を示します。

```
Router# show platform hardware capacity systems System Resources
  PFC operating mode: PFC3BXL
  Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus
  Switching Resources: Module   Part number              Series       CEF mode
                       5        WS-SUP720-BASE        supervisor           CEF
                       9        WS-X6548-RJ-45            CEF256           CEF
Router#
```

次に、Virtual LAN（VLAN; 仮想 LAN）情報を表示する例を示します。

```
Router# show platform hardware capacity vlan VLAN Resources
  VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free Router#
```

センサの温度スレッシュホールドの判別

システム センサは、さまざまな温度スレッシュホールド設定に基づいてアラームを発行します。**show environment alarm threshold** コマンドを使用すると、各センサに対して許可される温度を判別できます。

次に、センサの温度スレッシュホールドを判別する例を示します。

```
Router> show environment alarm threshold
environmental alarm thresholds:

power-supply 1 fan-fail: OK
  threshold #1 for power-supply 1 fan-fail:
    (sensor value != 0) is system minor alarm power-supply 1 power-output-fail: OK
  threshold #1 for power-supply 1 power-output-fail:
    (sensor value != 0) is system minor alarm fantray fan operation sensor: OK
  threshold #1 for fantray fan operation sensor:
    (sensor value != 0) is system minor alarm operating clock count: 2
  threshold #1 for operating clock count:
    (sensor value < 2) is system minor alarm
  threshold #2 for operating clock count:
    (sensor value < 1) is system major alarm operating VTT count: 3
  threshold #1 for operating VTT count:
    (sensor value < 3) is system minor alarm
  threshold #2 for operating VTT count:
    (sensor value < 2) is system major alarm VTT 1 OK: OK
  threshold #1 for VTT 1 OK:
    (sensor value != 0) is system minor alarm VTT 2 OK: OK
  threshold #1 for VTT 2 OK:
    (sensor value != 0) is system minor alarm VTT 3 OK: OK
  threshold #1 for VTT 3 OK:
    (sensor value != 0) is system minor alarm clock 1 OK: OK
```

```
threshold #1 for clock 1 OK:
  (sensor value != 0) is system minor alarm clock 2 OK: OK
threshold #1 for clock 2 OK:
  (sensor value != 0) is system minor alarm module 1 power-output-fail: OK
threshold #1 for module 1 power-output-fail:
  (sensor value != 0) is system major alarm module 1 outlet temperature: 21C
threshold #1 for module 1 outlet temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for module 1 outlet temperature:
  (sensor value > 70) is system major alarm module 1 inlet temperature: 25C
threshold #1 for module 1 inlet temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for module 1 inlet temperature:
  (sensor value > 70) is system major alarm module 1 device-1 temperature: 30C
threshold #1 for module 1 device-1 temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for module 1 device-1 temperature:
  (sensor value > 70) is system major alarm module 1 device-2 temperature: 29C
threshold #1 for module 1 device-2 temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for module 1 device-2 temperature:
  (sensor value > 70) is system major alarm module 5 power-output-fail: OK
threshold #1 for module 5 power-output-fail:
  (sensor value != 0) is system major alarm module 5 outlet temperature: 26C
threshold #1 for module 5 outlet temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for module 5 outlet temperature:
  (sensor value > 75) is system major alarm module 5 inlet temperature: 23C
threshold #1 for module 5 inlet temperature:
  (sensor value > 50) is system minor alarm
threshold #2 for module 5 inlet temperature:
  (sensor value > 65) is system major alarm EARL 1 outlet temperature: N/O
threshold #1 for EARL 1 outlet temperature:
  (sensor value > 60) is system minor alarm
threshold #2 for EARL 1 outlet temperature:
  (sensor value > 75) is system major alarm EARL 1 inlet temperature: N/O
threshold #1 for EARL 1 inlet temperature:
  (sensor value > 50) is system minor alarm
threshold #2 for EARL 1 inlet temperature:
  (sensor value > 65) is system major alarm
```

環境モニタの機能概要

シャーシ コンポーネントの環境をモニタすることにより、コンポーネント障害の兆候を早期に発見し、安全で信頼性の高いシステム運用を実現するとともに、ネットワーク障害を防止できます。ここでは、これらの重要なシステム コンポーネントをモニタし、システム内でハードウェア関連の問題点を特定し、すみやかに修正する方法を説明します。

システム環境ステータスのモニタ

システム ステータス情報を表示するには、**show environment** [**alarm** | **cooling** | **status** | **temperature**] コマンドを入力します。キーワードを指定することで、次の情報が表示されます。

- **alarm** - 環境アラームを表示します。
  - **status** - アラーム ステータスを表示します。
  - **thresholds** - アラーム スレッシュホールドを表示します。
- **cooling** - ファン トレイ ステータス、シャーシの冷却容量、周囲温度、スロット単位の冷却容量を表示します。
- **status** - Field-Replaceable Unit（FRU）の動作ステータスおよび電源と温度情報を表示します。
- **temperature** - FRU の温度情報を表示します。

システム ステータス情報を表示するには、次のように **show environment** コマンドを入力します。

```
Router# show environment
environmental alarms:
  no alarms

Router# show environment alarm
environmental alarms:
  no alarms

Router# show environment cooling
fan-tray 1:
  fan-tray 1 fan-fail: failed
fan-tray 2:
  fan 2 type: FAN-MOD-9
  fan-tray 2 fan-fail: OK
chassis cooling capacity: 690 cfm
ambient temperature: 55C                        ["40C (user-specified)" if temp-controlled]
chassis per slot cooling capacity: 75 cfm

  module 1 cooling requirement: 70 cfm
  module 2 cooling requirement: 70 cfm
  module 5 cooling requirement: 30 cfm
  module 6 cooling requirement: 70 cfm
  module 8 cooling requirement: 70 cfm
  module 9 cooling requirement: 30 cfm

Router# show environment status
backplane:
  operating clock count: 2
  operating VTT count: 3
fan-tray 1:
  fan-tray 1 type: WS-9SLOT-FAN
  fan-tray 1 fan-fail: OK
VTT 1:
  VTT 1 OK: OK
  VTT 1 outlet temperature: 33C
```

```
VTT 2:
  VTT 2 OK: OK
  VTT 2 outlet temperature: 35C
VTT 3:
  VTT 3 OK: OK
  VTT 3 outlet temperature: 33C
clock 1:
  clock 1 OK: OK, clock 1 clock-inuse: in-use
clock 2:
  clock 2 OK: OK, clock 2 clock-inuse: not-in-use
power-supply 1:
  power-supply 1 fan-fail: OK
  power-supply 1 power-output-fail: OK
module 1:
  module 1 power-output-fail: OK
  module 1 outlet temperature: 30C
  module 1 device-2 temperature: 35C
  RP 1 outlet temperature: 35C
  RP 1 inlet temperature: 36C
  EARL 1 outlet temperature: 33C
  EARL 1 inlet temperature: 31C
module 2:
  module 2 power-output-fail: OK
  module 2 outlet temperature: 31C
  module 2 inlet temperature: 29C
module 3:
  module 3 power-output-fail: OK
  module 3 outlet temperature: 36C
  module 3 inlet temperature: 29C
module 4:
  module 4 power-output-fail: OK
  module 4 outlet temperature: 32C
  module 4 inlet temperature: 32C
module 5:
  module 5 power-output-fail: OK
  module 5 outlet temperature: 39C
  module 5 inlet temperature: 34C
module 7:
  module 7 power-output-fail: OK
  module 7 outlet temperature: 42C
  module 7 inlet temperature: 29C
  EARL 7 outlet temperature: 45C
  EARL 7 inlet temperature: 32C
module 9:
  module 9 power-output-fail: OK
  module 9 outlet temperature: 41C
  module 9 inlet temperature: 36C
  EARL 9 outlet temperature: 33C
  EARL 9 inlet temperature: N/O
```

LED 環境表示の概要

LED は 2 種類のアラームを示します。メジャーおよびマイナーです。メジャー アラームは、システムのシャットダウンを引き起こす可能性のある重大な問題を表します。マイナー アラームは、解消されなければ重大な問題に発展する可能性のある問題を表すメッセージです。

過熱状態により、システムが（メジャーまたはマイナー）アラームを表示した場合、5 分間アラームはキャンセルされず、いかなる措置（モジュールのリセットまたはシャットダウンなど）も行われません。この間に温度がアラーム スレッシュホールドより 5℃（41°F）下がると、アラームはキャンセルされます。

表 54-2 に、スーパーバイザ エンジンおよびスイッチング モジュールに関する環境インジケータを示します。

（注）　スーパーバイザ エンジンの SYSTEM LED を含む、LED についての詳細は、『*Catalyst 6500 Series Switch Module Installation Guide*』を参照してください。

表 54-2　スーパーバイザ エンジンおよびスイッチング モジュールの環境モニタ

コンポーネント	アラームの種類	LED 表示	アクション
スーパーバイザ エンジンの温度センサがメジャー スレッシュホールドを超過[1]	メジャー	STATUS[2] LED レッド[3]	Syslog メッセージおよび Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを生成します。 冗長構成の場合、システムは冗長スーパーバイザ エンジンに切り替え、アクティブなスーパーバイザ エンジンはシャットダウンします。 冗長構成ではなく、過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
スーパーバイザ エンジンの温度センサが、マイナー スレッシュホールドを超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップを生成します。 状態をモニタします。
冗長スーパーバイザ エンジンの温度センサがメジャーまたはマイナー スレッシュホールドを超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP トラップを生成します。 メジャー アラームが生成され過熱状態が改善されない場合、システムは 5 分後にシャットダウンします。
	マイナー	STATUS LED オレンジ	マイナー アラームが生成された場合、状態をモニタします。
スイッチング モジュールの温度センサがメジャー スレッシュホールドを超過	メジャー	STATUS LED レッド	Syslog メッセージおよび SNMP を生成します。 モジュールの電源を切断します[4]。
スイッチング モジュールの温度センサがマイナー スレッシュホールドを超過	マイナー	STATUS LED オレンジ	Syslog メッセージおよび SNMP トラップを生成します。 状態をモニタします。

1. 温度センサは、主要なスーパーバイザ エンジン コンポーネント（ドータカードも含む）をモニタします。
2. STATUS LED は、スーパーバイザ エンジンの前面パネルおよびすべてのモジュールの前面パネルにあります。
3. STATUS LED は、スーパーバイザ エンジンが故障するとレッドになります。冗長構成のスーパーバイザがない場合は、SYSTEM LED もレッドになります。
4. 手順については、「電源管理の機能概要」（P.54-1）を参照してください。

CHAPTER 55

総合オンライン診断の設定

この章では、Catalyst 6500 シリーズ スイッチに総合オンライン診断（GOLD）を設定する手順について説明します。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

オンライン診断の機能概要

オンライン診断では、Catalyst 6500 シリーズ スイッチが稼動中のネットワークに接続している間に、スイッチのハードウェア機能をテストし、確認できます。

オンライン診断には、個別のハードウェア コンポーネントを確認して、データ パスおよび制御信号を検証するパケット スイッチング テストが含まれます。これには、中断を伴うオンライン診断テスト（Built In Self Test（BIST）や破壊モードのループバック テストなど）と中断を伴わないオンライン診断テスト（パケット スイッチング、ブートアップ中の実行、ライン カードの Online Insertion and Removal（OIR; ホットスワップ）、システム リセット）があります。中断を伴わないオンライン診断テストは、バックグラウンド ヘルス モニタリングの一部として、またはユーザ要求（オンデマンド オンライン診断）により実行されます。

オンライン診断では、次の分野の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス（Gigabit Interface Converters（GBIC; ギガビット インターフェイス コンバータ）、イーサネット ポートなど）
- コネクタ（コネクタのゆるみ、曲がったピンなど）
- はんだ接合
- メモリ（年数経過による故障）

オンライン診断は、高可用性機能要件の 1 つです。高可用性は、ネットワーク上の装置障害による影響を制限しようとする品質規格です。高可用性の重要な部分は、ハードウェア障害を検出し、スイッチが稼動中のネットワークで動作している間に修正措置を実行することです。高可用性のオンライン診断では、ハードウェア障害を検出して、スイッチオーバーを判断するために高可用性ソフトウェアにフィードバックします。

オンライン診断はブートアップ、オンデマンド、スケジュール、またはヘルス モニタリング診断に分類されます。ブートアップ診断は、ブートアップ中に実行する機能です。オンデマンド診断は Command-Line Interface（CLI; コマンドライン インターフェイス）から実行します。スケジュール診断は、スイッチが稼動中のネットワークに接続している状態で、ユーザが指定した間隔や指定した時間に実行します。ヘルス モニタリング診断はバックグラウンドで実行します。

オンライン診断の設定

ここでは、オンライン診断の設定手順について説明します。

ブートアップ オンライン診断レベルの設定

ブートアップ診断レベルは、最小または完全として設定できます。または、ブートアップ オンライン診断レベルをまったく実行しないことも選択できます。すべてのブートアップ診断テストを実行するには、**complete** キーワードを入力します。スイッチのすべてのポートに対し、EARL テストとループバック テストのみを実行するには、**minimal** キーワードを入力します。すべての診断テストを実行しない場合は、コマンドの **no** 形式を入力します。ブートアップ診断レベルのデフォルトは最小です。

ブートアップ診断レベルを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# diagnostic bootup level {minimal | complete}`	ブートアップ診断レベルを設定します。

次に、ブートアップ オンライン診断レベルを設定する例を示します。

```
Router(config)# diagnostic bootup level complete
Router(config)#
```

次に、ブートアップ オンライン診断レベルを表示する例を示します。

```
Router(config)# show diagnostic bootup level
Router(config)#
```

オンデマンド オンライン診断の設定

CLI からオンデマンド オンライン診断テストを実行できます。障害の検出時にテストを中止する、またはテストを続行するのどちらかに設定できます。また、障害カウントを設定し、障害が設定数に達したあとでテストを中止するように設定できます。反復設定を使用して、複数回テストを実行するように設定できます。

メモリ テストの前にパケット スイッチング テストを実行してください。

（注）　次に示すすべてのステップを完了するまで、**diagnostic start all** コマンドは使用しないでください。

一部のオンデマンド オンライン診断テストは、他のテストの結果に影響を及ぼすことがあります。したがって、各テストは次の順序で実行する必要があります。

1. 中断を伴わないテストを実行します。
2. 関連する機能分野に含まれるすべてのテストを実行します。
3. TestTrafficStress テストを実行します。
4. TestEobcStressPing テストを実行します。
5. 完全メモリ テストを実行します。

オンデマンド オンライン診断テストを実行するには、次の作業を行います。

ステップ 1　中断を伴わないテストを実行します。

使用可能なテストとその属性を表示し、中断を伴わないカテゴリに属するコマンドを判別するには、**show diagnostic content** コマンドを使用します。

ステップ 2　関連する機能分野に含まれるすべてのテストを実行します。

パケット スイッチング テストは、それぞれ特定の機能分野に分類されます。特定の機能分野で問題の発生が疑われる場合は、この機能分野に含まれるすべてのテストを実行します。テストの必要な機能分野を明確に特定できない場合、または使用可能なすべてのテストを実行するには、**complete** キーワードを使用します。

ステップ 3　TestTrafficStress テストを実行します。

これは、中断を伴うパケット スイッチング テストです。このテストでは、ストレス テストとして、一組のポート間でパケットをラインレートでスイッチングします。このテストの実行中、すべてのポートはシャットダウンされ、リンク フラップが生じることもあります。リンク フラップは、テストの完了後に回復します。このテストの完了には数分かかります。

このテストを実行する前に、**no diagnostic monitor module 1 test all** コマンドを使用して、すべてのヘルス モニタリング テストをディセーブルにします。

ステップ 4　TestEobcStressPing テストを実行します。

これは中断を伴うテストであり、モジュールの Ethernet over Backplane Channel（EOBC）接続をテストします。このテストの完了には数分かかります。このテストの実行後は、上記の各ステップに示したすべてのパケット スイッチング テストが実行できなくなります。ただし、このテストの実行後も、これ以降に説明する各テストは実行できます。

このテストを実行する前に、**no diagnostic monitor module 1 test all** コマンドを使用して、すべてのヘルス モニタリング テストをディセーブルにします。このテスト中は EOBC 接続が中断されるため、ヘルス モニタリング テストが失敗し、回復アクションが実行されます。

ステップ 5　完全メモリ テストを実行します。

完全メモリ テストを実行する前に、すべてのヘルス モニタリング テストをディセーブルにする必要があります。これは、ヘルス モニタリングがイネーブルになっているとテストが失敗し、回復アクションが実行されてしまうためです。ヘルス モニタリング診断テストをディセーブルにするには、**no diagnostic monitor module 1 test all** コマンドを使用します。

完全メモリ テストは、次の順序で実行します。

1. TestFibTcamSSRAM
2. TestAclQosTcam
3. TestNetFlowTcam
4. TestAsicMemory
5. TestAsicMemory

完全メモリ テストの実行後は、スイッチを再起動して、動作可能な状態に戻す必要があります。完全メモリ テストの実行後は、スイッチ上で他のテストをすべて実行できなくなります。設定値はテスト中に変更されているため、再起動時に設定を保存しないでください。リブート後は、**diagnostic monitor module 1 test all** コマンドを使用して、ヘルス モニタリング テストを再度イネーブルにします。

ブートアップ診断レベルを設定するには、次の作業を行います。

コマンド	目的
Router# **diagnostic ondemand** {**iteration** *iteration_count*} | {**action-on-error** {**continue** | **stop**}[*error_count*]}	実行するオンデマンド診断テスト、実行回数（反復）、エラーを検出したときに実行する処置を設定します。

次に、オンデマンド テスト反復カウントを設定する例を示します。

```
Router# diagnostic ondemand iteration 3
Router#
```

次に、エラーを検出したときに実行する処置を設定する例を示します。

```
Router# diagnostic ondemand action-on-error continue 2
Router#
```

オンライン診断のスケジューリング

特定日の指定時間、または毎日、毎週、毎月ベースでオンライン診断をスケジューリングできます。あるインターバルで 1 回のみ、または繰り返しテストを実行するようにスケジューリングできます。スケジュールを削除する場合は、コマンドの **no** 形式を使用します。

オンライン診断をスケジューリングするには、次の作業を行います。

コマンド	目的
Router(config)# **diagnostic schedule module 1 test** {*test_id* | *test_id_range* | **all**} [**port** {*num* | *num_range* | **all**}] {**on** *mm dd yyyy hh*:*mm*} | {**daily** *hh*:*mm*} | {**weekly** *day_of_week hh*:*mm*}	特定の日時のオンデマンド診断テスト、実行回数（反復）、エラーを検出したときに実行する処置をスケジューリングします。

次に、特定のポートについて、特定の日時に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

次に、特定のポートについて、毎日一定の時間に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

次に、特定のポートについて、毎週一定の曜日に診断テストを実行するようにスケジューリングする例を示します。

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

ヘルス モニタリング診断の設定

スイッチが稼動中のネットワークに接続している間に、ヘルス モニタリング診断テストを設定できます。ヘルス モニタリング診断テストの実行間隔と、テストに障害が発生したときにシステム メッセージを生成するまたは生成しない、あるいは各テストをイネーブルまたはディセーブルにするように設定できます。テストをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

ヘルス モニタリング診断テストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **diagnostic monitor interval module 1 test** {*test_id* | *test_id_range* | **all**} [**hour** *hh*] [**min** *mm*] [**second** *ss*] [**millisec** *ms*] [**day** *day*]	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。このコマンドの **no** 形式は、間隔をデフォルトまたは 0 に変更します。
ステップ 2	Router(config)#[**no**] **diagnostic monitor module 1 test** {*test_id* | *test_id_range* | **all**}	ヘルス モニタリング診断テストをイネーブルまたはディセーブルにします。

次に、2 分ごとに指定されたテストを実行するように設定する例を示します。

```
Router(config)# diagnostic monitor interval module 1 test 1 min 2
Router(config)#
```

次に、ヘルス モニタリングがそれまでイネーブル状態でない場合に、テストを実行する例を示します。

```
Router(config)# diagnostic monitor module 1 test 1
```

次に、ヘルス モニタリング テストが失敗したときに Syslog メッセージを生成する例を示します。

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

オンライン診断テストの実行

オンライン診断を設定したあと、診断テストを開始または中止したり、またはテスト結果を表示したりできます。設定されているテスト、およびすでに実行された診断テストを表示できます。

ここでは、オンライン診断テストを設定したあとに実行する例を示します。

- 「オンライン診断テストの開始および停止」（P.55-6）
- 「オンライン診断テストおよびテスト結果の表示」（P.55-7）

（注）

- オンライン診断テイストをイネーブルにする前に、コンソール/モニタのロギングをイネーブルにしてすべての警告メッセージが表示されるようにしておくことをお勧めします。
- 中断テストを実行する場合は、コンソールを通じて接続されているときにだけテストを実行することをお勧めします。中断テストが完了すると、通常稼動に戻るためにシステムをリロードすること勧める警告メッセージがコンソールに表示されます。必ずこの警告に従ってください。
- テストでは、ポートを内部でループするストレス テストが実行され、外部トラフィックによってテストの結果が歪められる可能性があるため、テストの実行中はすべてのポートがシャットダウンされます。スイッチを正常な稼動に戻すために、スイッチ全体をリロードしなければなりません。スイッチをリロードするコマンドを発行すると、コンフィギュレーションを保存するかどうかを尋ねられます。
- コンフィギュレーションを保存することはしないでください。
- スーパーバイザ エンジン上でテストを実行した場合は、テストを開始してテストが完了したあとに、システム全体をリロードするか、またはシステム全体の電源を切って電源を入れ直さなければなりません。
- スーパーバイザ エンジンでないモジュール上でテストを実行した場合は、テストを開始してテストが完了したあとに、そのモジュールをリセットしなければなりません。

オンライン診断テストの開始および停止

実行する診断テストを設定したあと、診断テストを開始または停止するには **start** および **stop** を使用します。

オンライン診断コマンドを開始または停止するには、次の作業を行います。

コマンド	目的
diagnostic start module 1 test {*test_id* | *test_id_range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all**} [**port** {*num* | *port#_range* | **all**}]	単一ポートまたは一定範囲のポートで、診断テストを開始します。
diagnostic stop module 1	診断テストを停止します。

次に、診断テストを開始する例を示します。

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

次に、診断テストを停止する例を示します。

```
Router# diagnostic stop module 1
Router#
```

オンライン診断テストおよびテスト結果の表示

show コマンドを使用すると、設定されたオンライン診断テストを表示し、テスト結果を確認できます。

設定された診断テストを表示するには、次の作業を行います。

コマンド	目的
show diagnostic content [**module 1**]	設定されたオンライン診断テストを表示します。

次に、設定されたオンライン診断を表示する例を示します。

```
Router# show diagnostic content module 1

Module 1:

  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Power-down line cards and need reset supervisor / NA
      K/* - Require resetting the line card after the test has completed / NA
```

```
                                                    Testing Interval
  ID   Test Name                           Attributes   (day hh:mm:ss.ms)
  ==== ================================== ============ =================
    1) TestScratchRegister -------------> ***N****A**  000 00:00:30.00
    2) TestSPRPInbandPing --------------> ***N****A**  000 00:00:15.00
    3) TestTransceiverIntegrity --------> **PD****I**  not configured
    4) TestActiveToStandbyLoopback -----> M*PDS***I**  not configured
    5) TestLoopback --------------------> M*PD****I**  not configured
    6) TestNewLearn --------------------> M**N****I**  not configured
    7) TestIndexLearn ------------------> M**N****I**  not configured
    8) TestDontLearn -------------------> M**N****I**  not configured
    9) TestConditionalLearn ------------> M**N****I**  not configured
   10) TestBadBpdu ---------------------> M**D****I**  not configured
   11) TestTrap ------------------------> M**D****I**  not configured
   12) TestMatch -----------------------> M**D****I**  not configured
   13) TestCapture ---------------------> M**D****I**  not configured
   14) TestProtocolMatch ---------------> M**D****I**  not configured
   15) TestChannel ---------------------> M**D****I**  not configured
   16) TestFibDevices ------------------> M**N****I**  not configured
   17) TestIPv4FibShortcut -------------> M**N****I**  not configured
   18) TestL3Capture2 ------------------> M**N****I**  not configured
   19) TestIPv6FibShortcut -------------> M**N****I**  not configured
   20) TestMPLSFibShortcut -------------> M**N****I**  not configured
   21) TestNATFibShortcut --------------> M**N****I**  not configured
   22) TestAclPermit -------------------> M**N****I**  not configured
   23) TestAclDeny ---------------------> M**D****I**  not configured
   24) TestQoSTcam ---------------------> M**D****I**  not configured
   25) TestL3VlanMet -------------------> M**N****I**  not configured
   26) TestIngressSpan -----------------> M**N****I**  not configured
   27) TestEgressSpan ------------------> M**N****I**  not configured
   28) TestNetflowInlineRewrite --------> C*PD****I**  not configured
   29) TestFabricSnakeForward ----------> M**N****I**  not configured
   30) TestFabricSnakeBackward ---------> M**N****I**  not configured
   31) TestFibTcamSSRAM ----------------> ***D****IR*  not configured
   32) ScheduleSwitchover --------------> ***D****I**  not configured


Router#
```

次に、オンライン診断結果を表示する例を示します。

```
Router# show diagnostic result module 1
Current bootup diagnostic level:minimal

Module 1:

  Overall Diagnostic Result for Module 1 :PASS
  Diagnostic level at card bootup:minimal

  Test results:(. = Pass, F = Fail, U = Untested)

    1) TestScratchRegister -------------> .
    2) TestSPRPInbandPing --------------> .
    3) TestGBICIntegrity:

       Port  1  2
       ----------
             U  U
```

```
    4) TestActiveToStandbyLoopback:

      Port  1  2
      ----------
            U  U


    5) TestLoopback:

      Port  1  2
      ----------
            .  .


    6) TestNewLearn --------------------> .
    7) TestIndexLearn ------------------> .
    8) TestDontLearn -------------------> .
    9) TestConditionalLearn ------------> .
   10) TestBadBpdu ---------------------> .
   11) TestTrap ------------------------> .
   12) TestMatch -----------------------> .
   13) TestCapture ---------------------> .
   14) TestProtocolMatch ---------------> .
   15) TestChannel ---------------------> .
   16) TestIPv4FibShortcut -------------> .
   17) TestL3Capture2 ------------------> .
   18) TestL3VlanMet -------------------> .
   19) TestIngressSpan -----------------> .
   20) TestEgressSpan ------------------> .
   21) TestIPv6FibShortcut -------------> .
   22) TestMPLSFibShortcut -------------> .
   23) TestNATFibShortcut --------------> .
   24) TestAclPermit -------------------> .
   25) TestAclDeny ---------------------> .
   26) TestQoSTcam ---------------------> .
   27) TestNetflowInlineRewrite:

      Port  1  2
      ----------
            U  U


   28) TestFabricSnakeForward ----------> .
   29) TestFabricSnakeBackward ---------> .
   30) TestFibTcam - RESET -------------> U
Router#
```

次に、詳細なオンライン診断結果を表示する例を示します。

```
Router# show diagnostic result module 1 detail
Current bootup diagnostic level:minimal

Module 1:

  Overall Diagnostic Result for Module 1 :PASS
  Diagnostic level at card bootup:minimal

  Test results:(. = Pass, F = Fail, U = Untested)

  ____________________________________________________________________________

    1) TestScratchRegister -------------> .

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 330
          Last test execution time ----> May 12 2003 14:49:36
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> May 12 2003 14:49:36
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________

    2) TestSPRPInbandPing --------------> .

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 660
          Last test execution time ----> May 12 2003 14:49:38
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> May 12 2003 14:49:38
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________

    3) TestGBICIntegrity:

      Port  1  2
      ----------
            U  U


          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ____________________________________________________________________________
Router#
```

メモリ テストの実行

大半のオンライン診断テストでは、特別なセットアップまたは設定は不要です。ただし、TestFibTcamSSRAM および TestLinecardMemory テストに付属のメモリ テストの場合、テストを実行する前に必須の作業や推奨された作業をいくつか行う必要があります。

オンライン診断メモリ テストを実行する前に、次の作業を行います。

- 必須作業
  - すべての接続ポートをディセーブルにして、ネットワーク トラフィックを分離します。
  - メモリ テスト中はテスト パケットを送信しないでください。
  - システムをユーザ動作モードに戻す前に、システムをリセットしてください。
- すべてのバックグラウンド ヘルス モニタリング テストをディセーブルにするには、**no diagnostic monitor module 1 test all** コマンドを使用します。

CHAPTER 56

Web Cache Communication Protocol（WCCP）による Web キャッシュ サービスの設定

この章では、Web Cache Communication Protocol（WCCP）を使用して、キャッシュ エンジン（Web キャッシュ）へトラフィックをリダイレクトするように Catalyst 6500 シリーズ スイッチを設定する方法、およびキャッシュ エンジン クラスタ（キャッシュ ファーム）を管理する方法について説明します。

（注）

- この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Policy Feature Card（PFC; ポリシー フィーチャ カード）2 を使用する場合は、WCCP は Release 12.2(17d)SXB 以降のリリースでサポートされます。
- PFC3 を使用する場合は、WCCP は Release 12.2(18)SXD1 以降のリリースでサポートされます。
- WCCP レイヤ 2 PFC リダイレクション機能を使用するには、この章の説明に従って Catalyst 6500 シリーズ スイッチで WCCP を設定し、次のマニュアルに従ってキャッシュ エンジンに加速 WCCP を設定します。

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns42/cnfg42/transprt.htm#xtocid34
- Release 4.2.2 以降の Cisco Application and Content Networking System（ACNS）ソフトウェア リリースでは、PFC2 で **ip wccp** *service* **accelerated** コマンドをサポートします。
- マスク割り当て用に設定したキャッシュ エンジンがファームへの加入を試みる場合、このファームで選択された割り当て方式がハッシュであると、キャッシュ エンジンの割り当て方式が既存ファームの方式と一致しない限り、ファームには加入できません。
- サービス グループの転送方式が WCCP レイヤ 2 PFC リダイレクションの場合は、**show ip wccp** *service_name* コマンドによって出力されるパケット カウンタ値は、パケット数ではなくフロー数となります。

この章で説明する内容は、次のとおりです。

（注）　この章の作業では、ネットワークですでにキャッシュ エンジンを設定していることを前提とします。Cisco Cache Engine および WCCP に関するハードウェアおよびネットワーク プランニングの詳細については、次の URL の Cisco.com Web Scaling サイトにある「Product Literature and Documentation」リンクを参照してください。
http://www.cisco.com/warp/public/cc/pd/cxsr/ces/index.shtml

WCCP の概要

ここでは WCCP について説明します。

WCCP の概要

Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツ ルーティング技術で、キャッシュ エンジン（Cisco Cache Engine 550 など）をネットワーク インフラストラクチャに統合できます。

（注）　シスコシステムズは 2001 年 7 月、Cache Engine 500 シリーズ プラットフォームを Content Engine プラットフォームに置き換えました。Cache Engine 製品は、Cache Engine 505、550、570、および 550-DS3 です。Content Engine 製品には、Content Engine 507、560、590、および 7320 があります。

Cisco IOS WCCP 機能では、Cisco Cache Engine（または WCCP で動作する他のキャッシュ エンジン）を使用してネットワークの Web トラフィック パターンをローカライズし、コンテンツ要求にローカルで対応できるようにします。トラフィックのローカライズによって伝送コストを引き下げ、ダウンロード時間を短縮できます。

WCCP によって、Cisco IOS ルーティング プラットフォームはコンテンツ要求を透過的にリダイレクトできます。透過リダイレクションの大きな利点は、Web プロキシを使用するためのブラウザの設定が不要ということです。代わりに、ターゲット URL を使用してコンテンツを要求すると、要求が自動的にキャッシュ エンジンにリダイレクトされます。この場合の「透過」という用語は、要求対象のファイル（Web ページなど）が初めに指定したサーバからではなく、キャッシュ エンジンから送られてきたことがエンド ユーザにはわからないことを指します。

キャッシュ エンジンは要求を受け取ると、専用のローカル キャッシュから対応しようとします。要求された情報が存在しない場合、キャッシュ エンジンは自らの要求を元のターゲット サーバに送信して要求された情報を取得します。要求された情報をキャッシュ エンジンが取得すると、要求元のクライアントに転送し、またキャッシュして今後の要求に備えます。これにより、ダウンロード パフォーマンスが最大になり、伝送コストを大幅に削減できます。

WCCP では、*キャッシュ エンジン クラスタ*と呼ばれる一連のキャッシュ エンジンがイネーブルになり、1 つまたは複数のルータにコンテンツを提供します。ネットワーク管理者は、キャッシュ エンジンを簡単に拡張し、クラスタの機能を利用して大量のトラフィック ロードを処理できます。シスコ クラスタリング テクノロジーではキャッシュ メンバがパラレルに稼動でき、リニア スケーラビリティが得られます。キャッシュ エンジンをクラスタリングすると、キャッシング ソリューションのスケーラビリティ、冗長性、および可用性が向上します。目的の容量に応じて、最大 32 のキャッシュ エンジンをクラスタリングできます。

ハードウェアの加速

Catalyst 6500 シリーズ スイッチは、Cisco Cache Engine に直接接続されている場合には、WCCP レイヤ 2 PFC リダイレクションによってハードウェアを加速します。これは、Generic Route Encapsulation（GRE; 総称ルーティング カプセル化）を備えた Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）での、ソフトウェアによるレイヤ 3 リダイレクションより効率的です。

WCCP レイヤ 2 PFC リダイレクションでは、Cisco Cache Engine はハードウェアでサポートされているレイヤ 2 リダイレクションを使用できます。直接接続された Cache Engine を設定すると、WCCP レイヤ 2 PFC リダイレクション機能の使用をネゴシエートできます。WCCP レイヤ 2 PFC リダイレクション機能には、MSFC の設定は必要ありません。**show ip wccp web-cache detail** コマンドを実行すると、使用されているリダイレクション方法がキャッシュ別に表示されます。

WCCP レイヤ 2 PFC リダイレクションについては、次の注意事項があります。

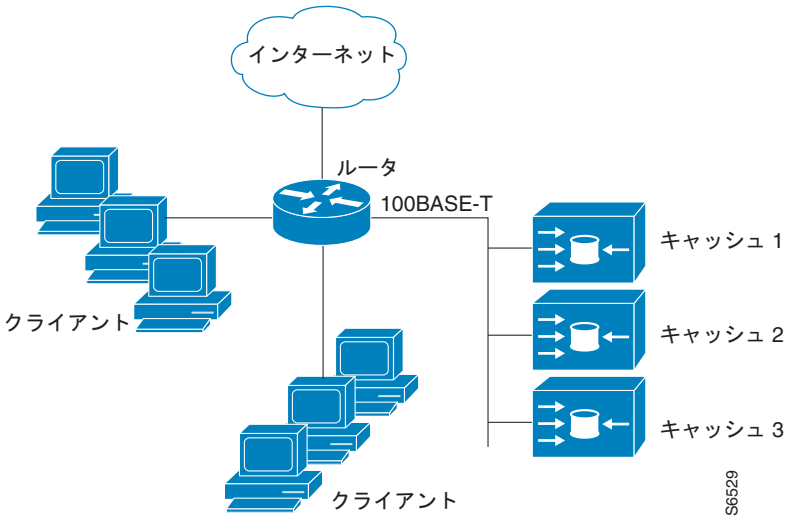
- WCCP レイヤ 2 PFC リダイレクション機能では、IP フロー マスクが full-flow モードに設定されます。
- Cisco Cache Engine ソフトウェア リリース 2.2 以降を設定すると、WCCP レイヤ 2 PFC リダイレクション機能を使用できます。
- レイヤ 2 リダイレクションは PFC で実行され、MSFC にはわかりません。MSFC で **show ip wccp web-cache detail** コマンドを実行すると、レイヤ 2 リダイレクションが行われたフローの 1 番目のパケットだけの統計情報が表示されます。これにより、パケットではなく、いくつのフローがレイヤ 2 リダイレクションを使用しているかがわかります。**show mls entries** コマンドを入力すると、レイヤ 2 リダイレクションの他のパケットも表示されます。

（注）
- PFC3 は、Generic Route Encapsulation（GRE）用にハードウェアを加速します。Generic Route Encapsulation（GRE）で WCCP レイヤ 3 リダイレクションを使用すると、カプセル化がハードウェアによってサポートされますが、WCCP GRE トラフィックのカプセル開放では PFC3 によるハードウェア サポートは行われません。
- PFC3 は、レイヤ 3 GRE カプセル化および Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）ラベル インポジションで WCCP をサポートしません。
- Release 4.2.1 以降の Cisco Application and Content Networking System（ACNS）ソフトウェア リリースでは、**accelerated** キーワードがサポートされます。

WCCPv1 設定の概要

WCCP-Version 1 の場合、1 つのルータだけがクラスタに対応します。このシナリオの場合、このルータがすべての IP パケットのリダイレクションを行う装置です。図 56-1 は、この構成図を示します。

図 56-1　WCCP-Version 1 による Cisco Cache Engine ネットワークの設定



コンテンツは、キャッシュ エンジンでは複製されません。複数のキャッシュを使用する利点は、複数の物理キャッシュを 1 つの論理キャッシュとしてクラスタリングすることによってキャッシング ソリューションを拡張できることです。

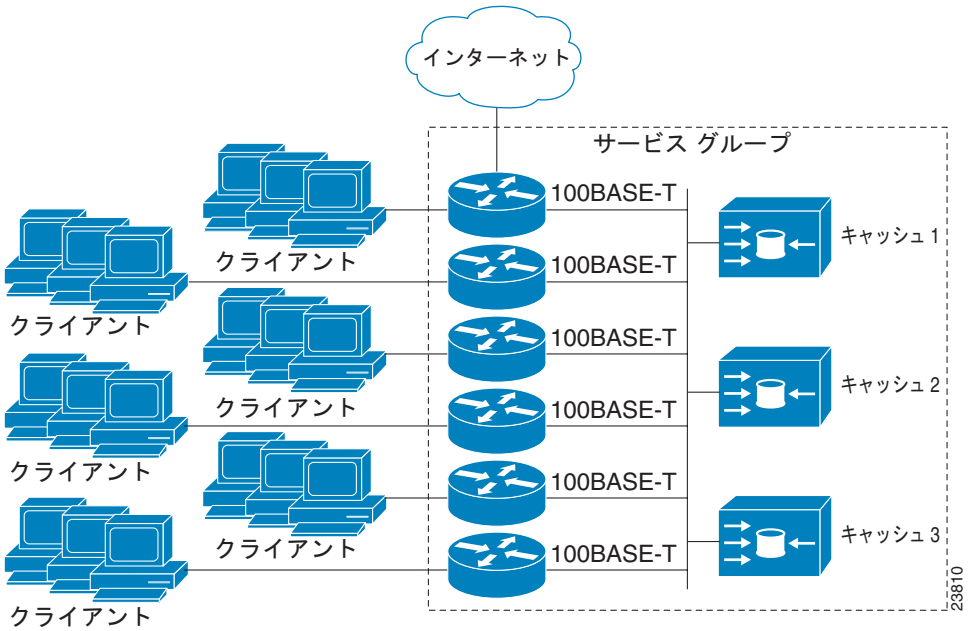
WCCPv1 設定の機能の詳細を次の一連のイベントで示します。

1. 各キャッシュ エンジンは、システム管理者が制御ルータの IP アドレスを使用して設定します。1 つの制御ルータには最大 32 のキャッシュ エンジンを接続できます。
2. キャッシュ エンジンは、WCCP で自らの存在を示して IP アドレスを制御ルータに送信します。ルータおよびキャッシュ エンジンは、User Datagram Protocol（UDP）ポート 2048 に基づいた制御チャネルを通して相互に通信します。
3. 制御ルータではこの情報が使用されて、クラスタ ビュー（クラスタ内のキャッシュの一覧）が作成されます。このビューはクラスタ内の各キャッシュに送信され、基本的にすべてのキャッシュ エンジンが相互の存在を認識できるようになります。クラスタのメンバシップが一定時間変わらないと、安定したビューが確立されます。
4. 安定したビューが確立されると、1 つのキャッシュ エンジンがリード キャッシュ エンジンに選択されます （このリード キャッシュ エンジンはクラスタ内のすべてのキャッシュ エンジンから IP アドレスが一番小さいと見なされます）。このリード キャッシュ エンジンは WCCP を使用して、IP パケット リダイレクションの実行の仕組みを制御ルータに示します。特にリード キャッシュ エンジンは、リダイレクトされたトラフィックをクラスタ内のキャッシュ エンジンに分配する方法を指定します。

WCCPv2 設定の概要

複数のルータは、キャッシュ クラスタに対応するために WCCPv2 を使用します。これは、1 つのルータだけがコンテンツ要求をクラスタにリダイレクトできる WCCPv1 とは対照的です。図 56-2 は、複数のルータを使用した構成例を示します。

図 56-2　WCCPv2 による Cisco Cache Engine ネットワークの設定



同じサービスを実行するクラスタに接続されているクラスタ内のキャッシュ エンジンのサブセットおよびルータを *サービス グループ*と呼びます。利用可能なサービスには、TCP および User Datagram Protocol（UDP）リダイレクションがあります。

WCCPv1 を使用して、1 つのルータのアドレスでキャッシュ エンジンが設定されます。WCCPv2 では、各キャッシュ エンジンがサービス グループ内のすべてのルータを認識する必要があります。サービス グループ内のすべてのルータのアドレスを指定するには、次のいずれかの方法を選択する必要があります。

- ユニキャスト - グループ内の各ルータのルータ アドレスの一覧が各キャッシュ エンジンに設定されます。この場合、グループ内の各ルータのアドレスは、設定中に各キャッシュ エンジンに明示的に指定する必要があります。
- マルチキャスト - 1 つのマルチキャスト アドレスを各キャッシュ エンジンに設定します。このマルチキャスト アドレス方式では、キャッシュ エンジンが、サービス グループ内のすべてのルータをカバーするシングル アドレス通知を送信します。たとえば、キャッシュ エンジンは、224.0.0.100 というマルチキャスト アドレスにパケットを送信するように指示することができます。この場合、マルチキャスト パケットは、サービス グループ内で WCCP を使用してグループで待ち受けるように設定されたすべてのルータに送信されます（詳細については、**ip wccp group-listen** 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）。

マルチキャスト オプションは、各キャッシュ エンジンに指定するアドレスが 1 つだけであるため、設定しやすくなっています。この方式では、サービス グループとの間でのルータの追加および削除がダイナミックにでき、毎回別のアドレス一覧を使用してキャッシュ エンジンを再設定する必要がありません。

WCCPv2 設定の機能の詳細を、次の一連のイベントで示します。

1. 各キャッシュ エンジンは、ルータの一覧を使用して設定します。
2. 各キャッシュ エンジンは自らの存在および全ルータの一覧をアナウンスして、通信を確立します。ルータは、グループ内のキャッシュ エンジンのビュー（一覧）を使用して応答します。
3. クラスタ内のすべてのキャッシュ エンジンについてビューに整合性があると、1 つのキャッシュ エンジンがリードとして指定され、パケットをリダイレクトする場合にルータが使用する必要のあるポリシーが設定されます。

次に、ルータをサービス グループに参加させるためにルータに WCCPv2 を設定する方法について説明します。

WCCPv2 の機能

ここでは、WCCPv2 機能について説明します。

- 非 HTTP サービスのサポート
- 複数ルータのサポート
- Message Digest 5（MD5）セキュリティ
- Web キャッシュ パケットのリターン
- 負荷分散

非 HTTP サービスのサポート

WCCPv2 では、さまざまな UDP および TCP トラフィックを含め、HTTP（TCP ポート 80 トラフィック）以外のトラフィックのリダイレクションが可能です。WCCPv1 では、HTTP（TCP ポート 80）トラフィックに限ってリダイレクションをサポートしています。WCCPv2 は、他のポート宛てのパケットのリダイレクションをサポートしています。これらのパケットには、プロキシ/Web キャッシュ処理用、File Transfer Protocol（FTP; ファイル転送プロトコル）キャッシング用、FTP プロキシ処理用、80 以外のポートの Web キャッシング用、オーディオ、ビデオ、テレフォニー アプリケーション用があります。

各種の利用可能なサービスに対応するために、WCCPv2 は複数の *サービス グループ*という概念を導入しています。ダイナミック サービス ID 番号（「98」など）または定義済みサービス キーワード（「web-cache」など）を使用して、WCCP 設定コマンドでサービス情報を指定します。この情報は、サービス グループ メンバが同じサービスを使用または提供していることを確認するために使用されます。

サービス グループ中のキャッシュ エンジンは、プロトコル（TCP または UDP）のリダイレクト対象にするトラフィックおよびポート（送信元または宛先）を指定します。各サービス グループにはプライオリティ ステータスが割り当てられます。パケットはプライオリティ順にサービス グループに対して照合が行われます。

複数ルータのサポート

WCCPv2 では、複数のルータをキャッシュ エンジンのクラスタに追加できます。サービス グループの複数のルータを使用すると、冗長構成、インターフェイスのアグリゲーション、およびリダイレクションの負荷分散が可能になります。

Message Digest 5（MD5）セキュリティ

WCCPv2 では、Hash-based Message Authentication Code（HMAC）Message Digest 5（MD5）標準およびパスワードを使用して、どのルータおよびキャッシュ エンジンをサービス グループに参加させるかを決めることができる認証をオプションで提供します。共有秘密鍵 MD5 ワンタイム認証（**ip wccp** [**password** [**0-7**] *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設定）では、メッセージの傍受、検査、およびリプレイから保護します。

Web キャッシュ パケットのリターン

キャッシュ エンジンはキャッシュしたオブジェクトのうちで要求されたものをエラーまたは過負荷のために提供できない場合、要求をルータに返して、最初に指定された宛先サーバに伝送されるようにします。WCCPv2 は、どの要求が対応されずにキャッシュ エンジンから返されたかをパケットごとにチェックします。ルータはこの情報を使用して、要求を元のターゲット サーバに転送できます（キャッシュ クラスタへの再送はしません）。これにより、エラー処理はクライアントには透過的になります。

キャッシュ エンジンがパケットを拒否してパケット リターン機能を実行する一般的な理由は、次のとおりです。

- キャッシュ エンジンが過負荷状態で、パケットに対応する余裕がない場合。
- キャッシュ エンジンが、パケットのキャッシングによって逆効果となる特定の状況（IP 認証をオンにしたときなど）でフィルタリングをする場合。

負荷分散

WCCPv2 を各キャッシュ エンジンに分散する負荷の調整に使用すると、利用可能なリソースを効率的に使用しながら高い Quality of Service（QoS; サービス品質）をクライアントに提供できます。WCCPv2 では指定キャッシュは、特定のキャッシュの負荷を調整し、クラスタ内のキャッシュ全体に負荷を分散できます。WCCPv2 では負荷分散を実行するために、次の 3 つの方法を使用します。

- ホット スポット処理 - 個々のハッシュ バケットをすべてのキャッシュ エンジンに分散できます。WCCPv2 以前は、1 つのハッシュ バケットの情報は 1 つのキャッシュ エンジンにだけ送ることができました。
- 負荷分散 - ハッシュ バケット セットをキャッシュ エンジンに割り当てて調整することにより、処理能力に余裕がないキャッシュ エンジンから余裕のある他のキャッシュ エンジンに負荷を送ることができます。
- 負荷制限 - ルータは負荷を選択的にリダイレクトして、キャッシュ エンジンの処理能力を超えないようにします。

こうしたハッシュ パラメータを使用すると、1 つのキャッシュが過負荷になることを防止し、輻輳の可能性を減らすことができます。

WCCPv2 の制約事項

WCCPv2 には次の制約事項があります。

- WCCP は IP ネットワークでだけ動作します。
- ルータをマルチキャスト クラスタに対応させるには、Time to Live（TTL; 存続可能時間）値を 15 以下に設定する必要があります。
- メッセージは IP マルチキャストされることがあるため、メンバは目的以外のまたは重複したメッセージを受け取ることがあります。適切なフィルタリングを実行する必要があります。
- サービス グループを構成できるのは、32 以下のキャッシュ エンジンおよび 32 以下のルータです。
- クラスタ内のすべてのキャッシュ エンジンは、クラスタに対応するすべてのルータと通信できるように設定する必要があります。
- マルチキャスト アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲にする必要があります。
- Customer Edge（CE; カスタマー エッジ）ルータはジャンボ イーサネット フレームの使用をサポートしないため、インターフェイスの IP MTU サイズがイーサネットのデフォルト値を超えることはできません。

WCCP の設定

次の設定作業では、ネットワークに導入したいキャッシュ エンジンがすでにインストールされ設定されていることを前提としています。ルータに WCCP 機能を設定する前に、クラスタ内のキャッシュ エンジンを設定する必要があります。キャッシュ エンジンの設定およびセットアップ作業の詳細については、『*Cisco Cache Engine User Guide*』を参照してください。

キャッシュ エンジンに接続されているルータ インターフェイス、およびインターネットに接続されているルータ インターフェイスで IP を設定してください。Cisco Cache Engine で直接接続するには、ファスト イーサネット インターフェイスを必要とします。ルータの設定例は、あとで説明します。コマンド構文の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

（注） スーパーバイザ エンジン 720 およびスーパーバイザ エンジン 32 で、トラフィックの転送またはトラフィックのリダイレクションにレイヤ 3 GRE 方式の WCCP サービスを使用している場合、同一のレイヤ 3 Virtual LAN（VLAN; 仮想 LAN）インターフェイスにインターネット接続、クライアント、およびキャッシュとして WCCP デバイスは存在できません。回避策としては、トラフィックの転送およびリダイレクションにレイヤ 2 GRE 方式を使用するか、または、それぞれのレイヤ 3 VLAN インターフェイスでネットワーク接続、クライアント、キャッシュを設定するかのいずれかです。

ここでは、WCCP の設定手順について説明します。

- 「WCCP のバージョンの指定」（P.56-9）（任意）
- 「WCCPv2 によるサービス グループの設定」（P.56-9）（必須）
- 「特定インターフェイスにおけるリダイレクションからのトラフィックの除外」（P.56-11）（任意）
- 「マルチキャスト アドレスへのルータの登録」（P.56-11）（任意）
- 「WCCP サービス グループのアクセス リストの使用」（P.56-12）（任意）
- 「ルータおよびキャッシュ エンジンのパスワードの設定」（P.56-12）（任意）

WCCP のバージョンの指定

ip wccp {**web-cache** | *service-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 WCCP を設定するまで、ルータでは WCCP はディセーブルです。**ip wccp** 形式のコマンドを最初に使用することによって、WCCP はイネーブルになります。デフォルトでは WCCPv2 はサービス用に使用されますが、代わりに WCCPv1 機能を使用することもできます。現在実行中の WCCP のバージョンを Version 2 から Version 1 に変更する、または最初の変更後に WCCPv2 に戻すには、EXEC モードで次の作業を行います。

コマンド	目的
`Router# ip wccp version {1 | 2}`	ルータに設定する WCCP のバージョンを指定します。WCCPv2 がデフォルトのバージョンです。

WCCPv1 では、以前の Cisco IOS バージョンの WCCP コマンドを使用できません。代わりに、この章で説明する WCCP コマンドを使用してください。WCCPv1 で許可されていない機能の場合は、エラープロンプトが画面に表示されます。たとえば、ルータで WCCPv1 を実行している場合にダイナミック サービスを設定しようとすると、[WCCP V1 only supports the web-cache service] というメッセージが表示されます。**show ip wccp** EXEC コマンドを使用すると、ルータ上で現在実行されている WCCP プロトコルのバージョン番号を表示できます。

WCCPv2 によるサービス グループの設定

WCCPv2 では、トラフィックの代行受信およびリダイレクションを行うために使用されている論理リダイレクション サービスを基にサービス グループを使用します。標準サービスは、TCP ポート 80（HTTP）トラフィックを代行受信し、キャッシュ エンジンにリダイレクトする Web キャッシュです。このサービスを *Well-known* と呼びます。ルータおよびキャッシュ エンジンの両方が Web キャッシュ サービスの特性をわかっているためです。サービス ID 以外の Well-known サービスの記述は不要です（この場合は Command-Line Interface（CLI; コマンドライン インターフェイス）がコマンド構文に **web-cache** キーワードを提供します）。

Web キャッシュ サービス以外にも、サービス グループでは最大 7 つのダイナミック サービスを同時に実行できます。

（注） 1 つのルータで複数のサービスを同時に実行することも、ルータおよびキャッシュ装置を複数のサービス グループに同時に参加させることもできます。

ダイナミック サービスはキャッシュ エンジンで定義され、キャッシュは代行受信するプロトコルまたはポートと、トラフィックの分散方法をルータに指示します。ルータ自体はダイナミック サービス グループのトラフィックの特性に関する情報を持っていません。この情報は、グループに最初に参加した Web キャッシュが提供するためです。ダイナミック サービスでは、1 つのプロトコルに最大 8 ポートを指定できます。

たとえば、Cisco Cache Engine はダイナミック サービス 99 を使用して、リバース プロキシ サービスを指定します。ただし、他のキャッシュ装置は、他のサービスのサービス番号を使用できます。次の設定情報は、シスコ ルータで汎用サービスをイネーブルにするためのものです。キャッシュ装置にサービスを設定する方法については、キャッシュ サーバの資料を参照してください。

Catalyst 6500 シリーズ スイッチでサービスをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip wccp {web-cache | service-number} [accelerated] [group-address groupaddress] [redirect-list access-list] [group-list access-list] [password password]`	ルータでイネーブルにする Web キャッシュまたはダイナミック サービスを指定します。サービス グループで使用する IP マルチキャスト アドレスを指定します。使用するアクセス リストを指定します。MD5 認証を使用するかどうかを指定します。WCCP サービスをイネーブルにします。
ステップ 2	`Router(config)# interface type number`	設定するインターフェイスを指定します。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	`Router(config-if)# ip wccp {web-cache | service-number} redirect {out | in}`	特定のインターフェイスで WCCP リダイレクションをイネーブルにします。

（注）　Cisco Application and Content Networking System（ACNS）ソフトウェアの今後のリリース（Release 4.2.2 以降）では、**ip wccp** *service* **accelerated** コマンドをサポートします。

ip wccp *service* **redirect** コマンド中の **out** および **in** キーワード オプションで示されるように、リダイレクションはインバウンド インターフェイスまたはアウトバウンド インターフェイスに指定できます。

インバウンド トラフィックは Cisco Express Forwarding（CEF）、distributed Cisco Express Forwarding（dCEF）、Fast Forwarding、または Process Forwarding を使用するように設定できます。

インターフェイスでインバウンド トラフィックに WCCP を設定すると、アウトバウンド トラフィックの CEF 転送に伴うオーバーヘッドを避けることができます。インターフェイスに出力機能を設定すると、全インターフェイスに到着するすべてのパケットが通過する機能のスイッチング パスが低速になります。インターフェイスに入力機能を設定すると、このインターフェイスに到着したパケットだけが設定済み機能パスを通り、他のインターフェイスに到着するパケットは高速なデフォルト パスを使用します。インバウンド トラフィックに WCCP を設定すると、パケットが分類されてからルーティング テーブルが検索され、パケットのリダイレクションが高速になります。

Web キャッシュ サービスの指定

Web キャッシュ サービスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip wccp web-cache`	ルータで Web キャッシュ サービスをイネーブルにします。
ステップ 2	`Router(config)# interface type number`	Web キャッシュ サービスを実行するインターフェイス番号を指定し、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。
ステップ 3	`Router(config-if)# ip wccp web-cache redirect {out | in}`	ステップ 2 で指定したインターフェイスを使用して、Web キャッシュにリダイレクトする資格があるかどうかを判別するためにパケットのチェックをイネーブルにします。

特定インターフェイスにおけるリダイレクションからのトラフィックの除外

インバウンド トラフィックのリダイレクションをインターフェイスで実行しないようにするには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type number`	設定するインターフェイスを指定します。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 2	`Router(config-if)# ip wccp redirect exclude in`	インターフェイス上でリダイレクションから除外するインバウンド パケットを許可します。

マルチキャスト アドレスへのルータの登録

サービス グループにマルチキャスト アドレス オプションを使用する場合、ルータがインターフェイスでマルチキャスト ブロードキャストを待ち受けるように設定する必要があります。ルータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip wccp {web-cache | service-number} group-address groupaddress`	サービス グループのマルチキャスト アドレスを指定します。
ステップ 2	`Router(config)# interface type number`	マルチキャスト受信用に設定するインターフェイスを指定します。
ステップ 3	`Router(config-if)# ip wccp {web-cache | service-number} group-listen`	ステップ 2 で指定したインターフェイスで IP マルチキャスト パケット（キャッシュ エンジンから送られるコンテンツ）の受信をイネーブルにします。

リダイレクトされたトラフィックが仲介ルータを経由する必要のあるネットワーク設定の場合、経由対象のルータは、IP マルチキャスト ルーティングを実行するように設定する必要があります。仲介ルータの経由をイネーブルにするには、次の 2 つのコンポーネントを設定してください。

- **ip multicast routing** インターフェイス コンフィギュレーション コマンドを使用して、IP マルチキャスト ルーティングをイネーブルにします。
- **ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを使用して、キャッシュ エンジンがマルチキャスト伝送を受信するために接続するインターフェイスをイネーブルにします（以前のバージョンの Cisco IOS では **ip pim** インターフェイス コンフィギュレーション コマンドの使用が必要でした）。

WCCP サービス グループのアクセス リストの使用

どのトラフィックをどのキャッシュ エンジンにリダイレクトするかを決めるためにアクセス リストを使用するようにルータを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# access-list access-list permit ip host host-address [destination-address | destination-host | any]`	キャッシュ エンジンへのトラフィックのリダイレクションをイネーブルまたはディセーブルにするアクセス リストを作成します。
ステップ 2	`Router(config)# ip wccp web-cache group-list access-list`	パケットを受け取るキャッシュ エンジンの IP アドレスをルータに指定します。

特定のクライアントのキャッシングをディセーブルにするには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# access-list access-list permit ip host host-address [destination-address | destination-host | any]`	キャッシュ エンジンへのトラフィックのリダイレクションをイネーブルまたはディセーブルにするアクセス リストを作成します。
ステップ 2	`Router(config)# ip wccp web-cache redirect-list access-list`	リダイレクションのイネーブル化に使用するアクセス リストを設定します。

ルータおよびキャッシュ エンジンのパスワードの設定

MD5 パスワード セキュリティでは、サービス グループ パスワードを使用して、サービス グループに参加させる各ルータおよびキャッシュ エンジンを設定する必要があります。パスワードは最大 7 文字にできます。サービス グループ内の各キャッシュ エンジンまたは各ルータは、WCCP メッセージ ヘッダーの確認後すぐに受信した WCCP パケット内のセキュリティ コンポーネントを認証します。認証に失敗したパケットは廃棄されます。

WCCP 通信においてルータが MD5 パスワードを使用するように設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

コマンド	目的
`Router(config)# ip wccp web-cache password password`	ルータで MD5 パスワードを設定します。

WCCP 設定の確認およびモニタ

WCCP の設定を確認およびモニタするには、EXEC モードで次の作業を行います。

コマンド	目的
Router# **show ip wccp** [**web-cache** | *service-number*]	WCCP に関連したグローバル情報を表示します。この情報には、現在使用中のプロトコル バージョン、ルータ サービス グループ内のキャッシュ エンジン数、ルータへの接続が許可されているキャッシュ エンジン グループ、使用されているアクセス リストなどがあります。
Router# **show ip wccp** {**web-cache** | *service-number*} **detail**	特定サービス グループのどのキャッシュ エンジンに関する情報を検出したかをルータに問い合わせます。Web キャッシュ サービスまたは指定のダイナミック サービスのいずれかの情報が表示されます。
Router# **show ip interface**	**ip wccp** リダイレクション コマンドがインターフェイスに設定されているかどうかについてのステータスを表示します。たとえば、「Web Cache Redirect is enabled / disabled」のように表示されます。
Router# **show ip wccp** {**web-cache** | *service-number*} **view**	特定のサービス グループのどの装置が検出され、どのキャッシュ エンジンが他のルータから認識可能か、また現在のルータの接続先がいずれであるかを表示します。**view** キーワードは、サービス グループのサービス一覧を示します。Web キャッシュ サービスまたは指定のダイナミック サービスのいずれかの情報が表示されます。トラブルシューティングの詳細については、**show ip wccp** {**web-cache** | *service number*} **service** コマンドを使用します。

WCCP の設定例

ここでは、次の設定例について説明します。

ルータでの WCCP バージョンの変更例

次に、WCCP バージョンをデフォルトの WCCPv2 から WCCPv1 に変更し、WCCPv1 で Web キャッシュ サービスをイネーブルにする処理例を示します。

```
Router# show ip wccp
% WCCP version 2 is not enabled
Router# configure terminal
Router(config)# ip wccp version 1
Router(config)# end
Router# show ip wccp
% WCCP version 1 is not enabled

Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip wccp web-cache
Router(config)# end
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  10.4.9.8
        Protocol Version:                   1.0
. . .
```

一般的な WCCPv2 設定の実行例

次に、一般的な WCCPv2 設定セッション例を示します。

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100 password alaska1
Router(config)# interface vlan 20
Router(config-if)# ip wccp web-cache redirect out
```

Web キャッシュ サービスの実行例

次に、Web キャッシュ サービス設定セッション例を示します。

```
router# configure terminal
router(config)# ip wccp web-cache
router(config)# interface vlan 20
router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ^Z
Router# copy running-config startup-config
```

次に、VLAN インターフェイス 30 に到着する HTTP トラフィックのリダイレクションをイネーブルにする設定セッション例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan 30
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# ^Z
Router# show ip interface vlan 30 | include WCCP Redirect
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
```

リバース プロキシ サービスの実行例

次の例では、リバース プロキシ サービスの実行にダイナミック サービス 99 を使用する Cisco Cache Engine を使用してサービス グループを設定することを前提としています。

```
router# configure terminal
router(config)# ip wccp 99
router(config)# interface vlan 40
router(config-if)# ip wccp 99 redirect out
```

マルチキャスト アドレスへのルータの登録例

次に、ルータをマルチキャスト アドレス 224.1.1.100 に登録する例を示します。

```
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface vlan 50
Router(config-if)# ip wccp web cache group-listen
```

次に、マルチキャスト アドレス 224.1.1.1 を使用してリバース プロキシ サービスを実行するようにルータを設定する例を示します。リダイレクションは、VLAN インターフェイス 60 から送信されるパケットに適用されます。

```
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface vlan 60
Router(config-if)# ip wccp 99 redirect out
```

アクセス リストの使用例

セキュリティを向上させるには、標準的なアクセス リストを使用して、現在のルータに登録しようとするキャッシュ エンジンにとってどの IP アドレスが有効なアドレスであるかをルータに通知します。次に、サンプル ホストのアクセス リスト番号が 10 である標準的なアクセス リストの設定セッション例を示します。

```
router(config)# access-list 10 permit host 11.1.1.1
router(config)# access-list 10 permit host 11.1.1.2
router(config)# access-list 10 permit host 11.1.1.3
router(config)# ip wccp web-cache group-list 10
```

特定のクライアント、サーバ、またはクライアント/サーバ ペアに対してキャッシングをディセーブルにするには、WCCP アクセス リストを使用します。次に、10.1.1.1 ～ 12.1.1.1 から送信される要求がキャッシュをバイパスするようにし、他のすべての要求には正常に対応させる例を示します。

```
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny tcp host 10.1.1.1 any
Router(config)# access-list 120 deny tcp any host 12.1.1.1
Router(config)# access-list 120 permit ip any any
```

次に、VLAN インターフェイス 70 で受信した Web 関連パケットを、209.165.196.51 以外のホスト宛てにリダイレクトするようにルータを設定する例を示します。

```
Router(config)# access-list 100 deny ip any host 209.165.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface vlan 70
Router(config-if)# ip wccp web-cache redirect in
```

ルータおよびキャッシュ エンジンのパスワード設定例

次に、パスワードを alaska1 とした場合の、WCCPv2 パスワード設定のセッション例を示します。

```
router# configure terminal
router(config)# ip wccp web-cache password alaska1
```

WCCP 設定の確認例

設定の変更を確認するには、**more system:running-config** EXEC コマンドを使用します。次は、Web キャッシュ サービスおよびダイナミック サービス 99 の両方がルータでイネーブルであることを示す例です。

```
router# more system:running-config

    Building configuration...
    Current configuration:
    !
    version 12.0
    service timestamps debug uptime
    service timestamps log uptime
    no service password-encryption
    service udp-small-servers
    service tcp-small-servers
    !
    hostname router4
    !
    enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
    enable password alabama1
    !
    ip subnet-zero
    ip wccp web-cache
    ip wccp 99
    ip domain-name cisco.com
    ip name-server 10.1.1.1
    ip name-server 10.1.1.2
    ip name-server 10.1.1.3
    !
    !
    !
    interface Vlan200
    ip address 10.3.1.2 255.255.255.0
    no ip directed-broadcast
    ip wccp web-cache redirect out
    ip wccp 99 redirect out
    no ip route-cache
    no ip mroute-cache
    !

    interface Vlan300
    ip address 10.4.1.1 255.255.255.0
    no ip directed-broadcast
    ip wccp 99 redirect out
    no ip route-cache
    no ip mroute-cache
    !
    interface Serial0
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
```

```
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
ip default-gateway 10.3.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password alaska1
login
!
end
```

CHAPTER 57

ユーティリティの使用上位 N

この章では、Catalyst 6500 シリーズ スイッチで 上位 N ユーティリティを使用する方法について説明します。上位 N ユーティリティは Release12.2(18)SXE 以降のリリースでサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

上位 N ユーティリティの概要

ここでは、上位 N ユーティリティについて説明します。

上位 N ユーティリティの概要

上位 N ユーティリティを使用すると、スイッチの各物理ポートからデータを収集し、分析できます。起動後、上位 N ユーティリティは適切なハードウェア カウンタから統計情報を取得してから、ユーザが指定したインターバルの間、スリープ モードに入ります。インターバルが経過すると、ユーティリティは同じハードウェア カウンタから現在の統計情報を取得して、前回収集した統計情報と比較し、その差分を保存します。各ポートの統計情報は、表 57-1 に示すいずれかの統計タイプによってソートされます。

表 57-1　有効な 上位 N の統計タイプ

統計タイプ	定義
broadcast	入力および出力ブロードキャスト パケット数
bytes	入力および出力バイト数
errors	入力エラー数
multicast	入力および出力マルチキャスト パケット数
overflow	発生したバッファ オーバーフローの回数
packets	入力および出力パケット数
utilization	利用率

（注）　上位 N ユーティリティはポート利用率を計算する際、Tx および Rx 回線を同一カウンタにまとめます。また、利用率の割合（%）の計算では、全二重帯域幅が対象となります。たとえば、ギガビット イーサネット ポートの場合は 2000 Mbps 全二重となります。

上位 N ユーティリティ操作の概要

collect top コマンドを入力すると、処理が開始され、システム プロンプトがただちに再び表示されます。処理が完了すると、レポートはその場で画面上に表示されるのではなく、あとで参照できるように保存されます。上位 N ユーティリティはレポートの生成が完了すると、画面に Syslog メッセージを送信して通知します。

生成が完了したレポートを表示するには、**show top counters interface report** コマンドを使用します。上位 N ユーティリティは、完了したレポートだけを表示します。まだ完了していないレポートに対しては、上位 N ユーティリティは 上位 N 処理についての簡単な概要情報を表示します。

上位 N の処理を終了するには、**clear top counters interface report** コマンドを使用します。**Ctrl+C** キーを押しても、上位 N の処理は中止されません。完了したレポートは、明示的に削除するまで表示可能です。削除するには、**clear top counters interface report** {**all** | *report_num*} コマンドを入力します。

上位 N ユーティリティの使用

ここでは、上位 N ユーティリティを使用する手順について説明します。

- 「上位 N ユーティリティによるレポート作成のイネーブル化」（P.57-3）
- 「上位 N ユーティリティ レポートの表示」（P.57-3）
- 「上位 N ユーティリティ レポートの消去」（P.57-4）

上位 N ユーティリティによるレポート作成のイネーブル化

上位 N ユーティリティによるレポートの作成をイネーブルにするには、次の作業を行います。

コマンド	目的
Router# **collect top** [*number_of_ports*] **counters interface** {*interface_type*[1] | **all** | **layer-2** | **layer-3**} [**sort-by** *statistic_type*[2]] [**interval** *seconds*]	上位 N ユーティリティによるレポート作成をイネーブルにします。

1. *interface type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**port-channel**
2. *statistic_type* = **broadcast**、**bytes**、**errors**、**multicast**、**overflow**、**packets**、**utilization**

上位 N ユーティリティによるレポートの作成をイネーブルにする場合は、次の点に注意してください。

- レポート作成の対象として、最も混雑しているポート数を指定できます（デフォルトは 20）。
- ポートが最も混雑していると見なされる統計タイプを指定できます（デフォルトは utilization）。
- 統計情報を収集するためのインターバルを指定できます（有効範囲は 0 ～ 999、デフォルトは 30 秒）。
- utilization レポートを除き（**sort-by utilization** キーワードを使用して設定）、レポート作成のインターバルを 0 に指定できます。この場合は、インターバル開始時のカウンタ値とインターバル終了時のカウンタ値の差分ではなく、現在のカウンタ値がレポートに表示されます。

次に、利用率が最も高い 4 つのポートに対し、上位 N ユーティリティによるレポートの作成をイネーブルにする例を示します。インターバルは 76 秒に設定します。

```
Router# collect top 4 counters interface all sort-by utilization interval 76
TopN collection started.
```

上位 N ユーティリティ レポートの表示

上位 N ユーティリティのレポートを表示するには、次の作業を行います。

コマンド	目的
Router# **show top counters interface report** [*report_num*]	上位 N ユーティリティ レポートを表示します。 **（注）**　すべてのレポート情報を表示する場合は、*report_num* 値を入力しないでください。

上位 N ユーティリティによる統計情報は、次の状況では表示されません。

- 最初のポーリング実行時にポートが存在しない場合。
- 2 度目のポーリング実行時にポートが存在しない場合。
- ポーリング インターバルの間にポートの速度またはデュプレックスが変更された場合。
- ポーリング インターバルの間にポート タイプがレイヤ 2 からレイヤ 3 に変更された場合。
- ポーリング インターバルの間にポート タイプがレイヤ 3 からレイヤ 2 に変更された場合。

次に、すべての 上位 N ユーティリティ レポート情報を表示する例を示します。

```
Router# show top counters interface report
Id Start Time                    Int N   Sort-By   Status  Owner
-- ----------------------------- --- --- --------- ------- ----------------------
1  08:18:25 UTC Tue Nov 23 2004 76  20  util      done    console
2  08:19:54 UTC Tue Nov 23 2004 76  20  util      done    console
3  08:21:34 UTC Tue Nov 23 2004 76  20  util      done    console
4  08:26:50 UTC Tue Nov 23 2004 90  20  util      done    console
```

（注） 統計情報の収集が完了していないレポートの場合は、ステータスが pending として表示されます。

次に、特定の 上位 N ユーティリティ レポートを表示する例を示します。

```
Router# show top counters interface report 1
Started By        : console
Start Time        : 08:18:25 UTC Tue Nov 23 2004
End Time          : 08:19:42 UTC Tue Nov 23 2004
Port Type         : All
Sort By           : util
Interval          : 76 seconds
Port    Band  Util Bytes       Packets     Broadcast  Multicast  In-  Buf-
        width      (Tx + Rx)   (Tx + Rx)   (Tx + Rx)  (Tx + Rx)  err  ovflw
------- ----- ---- ----------- ----------- ---------- ---------- ---- -----

Fa2/5   100   50   726047564   11344488    11344487   1          0    0
Fa2/48  100   35   508018905   7937789     0          43         0    0
Fa2/46  100   25   362860697   5669693     0          43         0    0
Fa2/47  100   22   323852889   4762539     4762495    43         0    0
```

上位 N ユーティリティ レポートの消去

上位 N ユーティリティ レポートを消去するには、次のいずれかの作業を行います。

コマンド	目的
`Router# clear top counters interface report`	ステータスが done のすべての 上位 N ユーティリティ レポートを消去します。
`Router# clear top counters interface report` [*report_num*]	ステータスに関係なく、番号が *report_num* の 上位 N ユーティリティ レポートを消去します。

次に、ステータスが done のすべてのレポートを消去する例を示します。

```
Router# clear top counters interface report
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 1 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 2 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 3 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console
```

次に、番号 4 のレポートを消去する例を示します。

```
Router# clear top counters interface report 4
04:52:12: %TOPN_COUNTERS-5-KILLED: TopN report 4 killed by the console
```

CHAPTER 58

レイヤ 2 traceroute ユーティリティの使用

この章では、レイヤ 2 traceroute ユーティリティの使用方法について説明します。レイヤ 2 traceroute ユーティリティは、Release12.2(18)SXE 以降のリリースでサポートされます。

（注） この章で使用してい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『*Cisco IOS Master Command List*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

この章で説明する内容は、次のとおりです。

レイヤ 2 traceroute ユーティリティの概要

レイヤ 2 traceroute ユーティリティは、送信元装置から宛先装置までパケットが通過するレイヤ 2 パスを識別します。レイヤ 2 traceroute は、ユニキャストの送信元および宛先 MAC アドレスのみをサポートします。このユーティリティは、パス上の各スイッチの持つ MAC（メディア アクセス制御）アドレス テーブルを使用して、パスを特定します。レイヤ 2 traceroute ユーティリティは、レイヤ 2 traceroute をサポートしない装置をパス上で検出すると、レイヤ 2 トレース クエリーを送信し続け、これらのクエリーをタイムアウトにします。

レイヤ 2 traceroute ユーティリティが識別できるのは、送信元装置から宛先装置までのパスのみです。パケットが送信元ホストから送信元装置に到達するパスや、宛先装置から宛先ホストへのパスは識別できません。

使用上の注意事項

レイヤ 2 traceroute ユーティリティを使用する際は、次の注意事項に従ってください。

- ネットワーク内のすべての装置で、Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）をイネーブルにする必要があります。CDP をディセーブルにすると、レイヤ 2 traceroute ユーティリティが正しく動作しません。レイヤ 2 パス内のいずれかの装置が CDP に対して透過的であると、レイヤ 2 traceroute ユーティリティはパス上でこの装置を識別できません。

（注）　CDP の詳細については、第 48 章「CDP の設定」を参照してください。

- **ping** イネーブル EXEC コマンドを使用して接続をテストできれば、このスイッチは別のスイッチから到達可能であると定義できます。レイヤ 2 パス内のすべての装置は、互いに到達可能である必要があります。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元装置から宛先装置までのレイヤ 2 パス上にないスイッチでは、**traceroute mac** または **traceroute mac ip** イネーブル EXEC コマンドを実行できます。パス内のすべての装置は、このスイッチから到達可能である必要があります。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合のみです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、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。
- マルチキャストの送信元または宛先 MAC アドレスを指定すると、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 に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。
- **traceroute mac ip** コマンドの出力結果にレイヤ 2 パスが表示されるのは、指定の送信元および宛先 IP アドレスが同一のサブネットに属している場合です。IP アドレスを指定すると、レイヤ 2 traceroute ユーティリティは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して、IP アドレスと、これに対応する MAC アドレスおよび VLAN ID を関連付けます。
  - 指定の IP アドレスに対する ARP エントリが存在する場合は、レイヤ 2 traceroute ユーティリティはこれに関連付けられた MAC アドレスを使用して、レイヤ 2 パスを識別します。
  - ARP エントリが存在しない場合は、レイヤ 2 traceroute ユーティリティは ARP クエリーを送信し、この IP アドレスの解決を試みます。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。
- 複数の装置がハブを介して 1 つのポートに接続されている場合は（1 つのポート上で複数の CDP ネイバが検出された場合など）、レイヤ 2 traceroute ユーティリティはこのホップで終了し、エラー メッセージが表示されます。
- レイヤ 2 traceroute ユーティリティは、トークン リング VLAN ではサポートされません。

レイヤ 2 traceroute ユーティリティの使用

パケットが通過した送信元装置から宛先装置までのレイヤ 2 パスを表示するには、イネーブル EXEC モードで、次のいずれかの作業を行います。

コマンド	目的
Router# **traceroute mac** [**interface** *type interface_number*] *source_mac_address* [**interface** *type interface_number*] *destination_mac_address* [**vlan** *vlan_id*] [**detail**]	MAC アドレスを使用して、パケットがネットワーク上で通過したパスを追跡します。
Router# **traceroute mac ip** {*source_ip_address* | *source_hostname*} {*destination_ip_address* | *destination_hostname*} [**detail**]	IP アドレスを使用して、パケットがネットワーク上で通過したパスを追跡します。

次に、**traceroute mac** および **traceroute mac ip** コマンドを使用して、パケットが宛先に到達するまでに通過したネットワーク上の物理パスを表示する例を示します。

```
Router# traceroute mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Router#
Router# traceroute mac 0001.0000.0204 0001.0000.0304 detail
Source 0001.0000.0204 found on VAYU[WS-C6509] (2.1.1.10)
1 VAYU / WS-C6509 / 2.1.1.10 :
               Gi6/1 [full, 1000M] => Po100 [auto, auto]
2 PANI / WS-C6509 / 2.1.1.12 :
               Po100 [auto, auto] => Po110 [auto, auto]
3 BUMI / WS-C6509 / 2.1.1.13 :
               Po110 [auto, auto] => Po120 [auto, auto]
4 AGNI / WS-C6509 / 2.1.1.11 :
               Po120 [auto, auto] => Gi8/12 [full, 1000M] Destination 0001.0000.0304
found on AGNI[WS-C6509] (2.1.1.11) Layer 2 trace completed.
Router#
```

オンライン診断テスト

この付録ではオンライン診断テストについて説明し、その使用方法についての推奨事項を示します。

オンライン診断テストには、次のカテゴリがあります。

（注）

- オンライン診断テストの設定については、第 55 章「総合オンライン診断の設定」を参照してください。
- オンライン診断テイストをイネーブルにする前に、コンソール/モニタのロギングをイネーブルにしてすべての警告メッセージが表示されるようにしておくことをお勧めします。
- 中断テストを実行する場合は、コンソールを通じて接続されているときにだけテストを実行することをお勧めします。中断テストが完了すると、通常稼動に戻るためにシステムをリロードすること勧める警告メッセージがコンソールに表示されます。必ずこの警告に従ってください。
- テストでは、ポートを内部でループするストレス テストが実行され、外部トラフィックによってテストの結果が歪められる可能性があるため、テストの実行中はすべてのポートがシャットダウンされます。スイッチを正常な稼動に戻すために、スイッチ全体をリロードしなければなりません。スイッチをリロードするコマンドを発行すると、コンフィギュレーションを保存するかどうかを尋ねられます。
- コンフィギュレーションを保存することはしないでください。
- スーパーバイザ エンジン上でテストを実行した場合は、テストを開始してテストが完了したあとに、システム全体をリロードするか、またはシステム全体の電源を切って電源を入れ直さなければなりません。
- スーパーバイザ エンジンでないモジュール上でテストを実行した場合は、テストを開始してテストが完了したあとに、そのモジュールをリセットしなければなりません。

グローバル ヘルス モニタリング テスト

グローバル ヘルス モニタリング テストには、次のテストが含まれます。

TestSPRPInbandPing

TestSPRPIinbandPing テストでは、スイッチ プロセッサからルート プロセッサへのパス上にあるレイヤ 2 転送エンジン、レイヤ 3 転送エンジン、レイヤ 4 転送エンジンおよびレプリケーション エンジンを使用して、診断パケット テストを実行することにより、スーパーバイザ エンジン上のランタイム ソフトウェア ドライバおよびハードウェアの大部分の問題を検出します。パケットは、15 秒ごとに送信されます。テストに 10 回連続して失敗すると、冗長スーパーバイザ エンジン（デフォルト）へのフェールオーバー、または冗長スーパーバイザ エンジンが搭載されていない場合は、スーパーバイザ エンジンのリロードが発生します。

表 A-1　TestSPRPInbandPing テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ディセーブルにしないでください。CPU 使用率の急上昇中は、テストは精度を維持するために自動的にディセーブルになります。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX ～ 12.2(17d)SXB5 および 12.2(18)SXD
修正措置	アクティブ スーパーバイザ エンジンをリセットします。
ハードウェア サポート	アクティブおよびスタンバイ スーパーバイザ エンジン

TestScratchRegister

TestScratchRegister テストでは、レジスタに値を書き込み、これらのレジスタから再度値を読み取ることによって、Application-Specific Integrated Circuit（ASIC; 特定用途向け IC）のヘルスをモニタします。このテストは、30 秒ごとに実行されます。5 回連続して失敗すると、スーパーバイザ エンジンのスイッチオーバー（またはリセット）（スーパーバイザ エンジンのテスト時)、またはモジュールの電源切断（モジュールのテスト時）が発生します。

表 A-2　TestScratchRegister テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ディセーブルにしないでください。
デフォルト	オン
リリース	12.2(14)SX
修正措置	故障しているスーパーバイザ エンジンをリセットするか、またはモジュールの電源を切断します。
ハードウェア サポート	Supervisor Engine 720、DFC 搭載モジュール、WS-X6148-FE-SFP、WS-X6148A-GE-TX、および WS-X6148A-RJ-45

TestMacNotification

TestMacNotification テストでは、DFC モジュールとスーパーバイザ エンジン間のデータ パスおよび制御パスが適切に動作していることを確認します。またこのテストでは、レイヤ 2 MAC アドレスとレイヤ 2 MAC アドレス テーブルとの整合性も確認します。このテストは、6 秒ごとに実行されます。10 回連続して失敗すると、ブートアップまたはランタイム（デフォルト）間にモジュールがリセットされます。モジュールは 3 回連続してリセットされたあと、切断されます。

表 A-3　TestMacNotification テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ディセーブルにしないでください。
デフォルト	オン
リリース	12.2(14)SX
修正措置	モジュールをリセットします。モジュールで連続して 10 回失敗するか、または連続して 3 回リセットされると、電源が切断されます。
ハードウェア サポート	DFC 搭載モジュール

ポート単位のテスト

ポート単位のテストには、次のテストが含まれます。

TestNonDisruptiveLoopback

TestNonDisruptiveLoopback テストでは、スーパーバイザ エンジンとモジュールのネットワーク ポート間のデータ パスを確認します。このテストでは、レイヤ 2 パケットがテスト ポートのグループを含む VLAN にフラッディングされます。テスト ポート グループは、ポート ASIC チャネルごとに 1 つのポートで構成されます。テスト ポート グループの各ポートでは、中断せずにパケットをループ バックして、スーパーバイザ エンジンの帯域内ポートに戻るように指定します。テスト ポート グループのポートは、パラレルにテストされます。

表 A-4　TestNonDisruptiveLoopback テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ディセーブルにしないでください。
デフォルト	オン
リリース	12.2(18)SXF
修正措置	10 回連続して失敗すると、ポートは errdisable になります。1 回のテスト サイクルでチャネルのすべてのポートがテストに失敗した場合、そのチャネルは errdisable になります。すべてのチャネルで失敗した場合は、モジュールをリセットします。
ハードウェア サポート	WS-X6148-FE-SFP、WS-X6148A-GE-TX、および WS-X6148A-RJ-45

TestLoopback

TestLoopback テストでは、スーパーバイザ エンジンとモジュールのネットワーク ポート間のデータ パスを確認します。このテストでは、レイヤ 2 パケットが、テスト ポートおよびスーパーバイザ エンジンの帯域内ポートのみを含む VLAN にフラッディングされます。パケットはポート内をループ バックして、同じ VLAN のスーパーバイザ エンジンに戻ります。

表 A-5　TestLoopback テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	ブートアップ時または Online Insertion and Removal（OIR; ホットスワップ）後に実行します。
リリース	12.1(13)E、12.2(14)SX
修正措置	ポートでループバック テストに失敗すると、ポートは errdisable になります。すべてのポートが失敗すると、モジュールはリセットされます。
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

TestActiveToStandbyLoopback

TestActiveToStandbyLoopback テストでは、アクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジンのネットワーク ポート間のデータ パスを確認します。このテストでは、レイヤ 2 パケットが、テスト ポートおよびスーパーバイザ エンジンの帯域内ポートのみを含む VLAN にフラッディングされます。テスト パケットは、ターゲット ポートでループ バックされ、フラッディングされる VLAN で待ち受けているアクティブ スーパーバイザ エンジンの帯域内ポートのみを含むバスにフラッディング バックされます。

表 A-6　TestActiveToStandbyLoopback テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループバック ポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	ブートアップ時または OIR のあとで実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	ポートでループバック テストに失敗すると、ポートは errdisable になります。すべてのポートが失敗すると、スーパーバイザ エンジンはリセットされます。
ハードウェア サポート	スタンバイ スーパーバイザ エンジンのみ

TestTransceiverIntegrity

TestTransceiverIntegrity テストは、トランシーバの OIR 中またはモジュールのブートアップ中に、トランシーバがサポートされていることを確認するためトランシーバで実行されるセキュリティ テストです。

表 A-7　TestTransceiverIntegrity テストの属性

属性	説明
中断の有無	中断なし
推奨事項	適用不可
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	ポートは errdisable になります。
ハードウェア サポート	トランシーバが搭載されたすべてのモジュール

TestNetflowInlineRewrite

TestNetflowInlineRewrite テストでは、Netflow のルックアップ動作、Access Control List（ACL; アクセス制御リスト）の許可および拒否機能、またポート ASIC のインライン書き換え機能について確認します。書き換え情報を入手するため、テスト パケットには Netflow テーブル ルックアップが行われます。パケットがターゲット ポートに到達すると、VLAN アドレス、送信元および宛先 MAC アドレスは書き換えられます。

表 A-8　TestNetflowInlineRewrite テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループバック ポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。ブートアップ中に限り、このテストを実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

PFC レイヤ 2 転送エンジンのテスト

PFC レイヤ 2 転送エンジンのテストには、次のテストが含まれます。

TestNewIndexLearn

TestNewIndexLearn テストは、TestNewLearn と TestIndexLearn テスト（「DFC レイヤ 2 転送エンジンのテスト」（P.A-11）を参照）を組み合わせたものです。

表 A-9　TestNewIndexLearn テストの属性

属性	説明
中断の有無	中断なし
推奨事項	レイヤ 2 転送エンジンの学習機能に関する問題がある場合は、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を確認します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンのみ

TestDontConditionalLearn

TestDontConditionalLearn テストは、TestDontLearn と TestConditionalLearn テスト（「DFC レイヤ 2 転送エンジンのテスト」（P.A-11）を参照）を組み合わせたものです。

表 A-10　TestDontConditionalLearn テストの属性

属性	説明
中断の有無	中断なし
推奨事項	レイヤ 2 転送エンジンの学習機能に関する問題がある場合は、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を確認します。またこのテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンのみ

TestBadBpduTrap

TestBadBpduTrap テストは、TestTrap と TestBadBpdu テスト（「DFC レイヤ 2 転送エンジンのテスト」（P.A-11）を参照）を組み合わせたものです。

表 A-11　TestBadBpduTrap テストの属性

属性	説明
中断の有無	中断なし
推奨事項	レイヤ 2 転送エンジンの学習機能に関する問題がある場合は、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を確認します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンのみ

TestMatchCapture

TestMatchCapture テストは、TestProtocolMatchChannel と TestCapture テスト（「DFC レイヤ 2 転送エンジンのテスト」（P.A-11）を参照）を組み合わせたものです。

表 A-12　TestMatchCapture テストの属性

属性	説明
中断の有無	中断なし
推奨事項	レイヤ 2 学習機能を確認するには、このテストをオンデマンドで実行します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンのみ

TestStaticEntry

TestStaticEntry テストでは、スタティック エントリがレイヤ 2 MAC アドレス テーブルで読み込まれることを確認します。この機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-13　TestStaticEntry テストの属性

属性	説明
中断の有無	中断なし
推奨事項	レイヤ 2 転送エンジンの学習機能に関する問題がある場合は、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を確認します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

DFC レイヤ 2 転送エンジンのテスト

DFC レイヤ 2 転送エンジンのテストには、次のテストが含まれます。

TestDontLearn

TestDontLearn テストでは、新しい送信元 MAC アドレスが学習されるべきではない場合に、MAC アドレス テーブルに読み込まれていないかを確認します。このテストでは、レイヤ 2 転送エンジンの「学習しない」機能が適切に動作していることを確認します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC 対応モジュール上のいずれかのポートからループ バックされます。「学習しない」機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-14　TestDontLearn テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestNewLearn

TestNewLearn では、レイヤ 2 転送エンジンのレイヤ 2 送信元 MAC アドレス学習機能について確認します。スーパーバイザ エンジンの場合、診断パケットはスーパーバイザ エンジン帯域内ポートから送信され、レイヤ 2 転送エンジンが診断パケットから新しい送信元 MAC アドレスを学習していることを確認します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC 対応モジュール上のいずれかのポートからループ バックされます。レイヤ 2 の学習機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-15　TestNewLearn テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestIndexLearn

TestIndexLearn テストでは、既存の MAC アドレス テーブル エントリを更新できることを確認します。このテストでは、レイヤ 2 転送エンジンの Index Learn 機能が適切に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Index Learn 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-16　TestIndexLearn テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestConditionalLearn

TestConditionalLearn テストでは、特定条件下でのレイヤ 2 送信元 MAC アドレスの学習機能について確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Condition Learn 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-17　TestConditionalLearn テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestTrap

TestTrap テストでは、トラップ機能またはスイッチ プロセッサへのパケットのリダイレクト機能について確認します。このテストでは、レイヤ 2 転送エンジンの Trap 機能が適切に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Trap 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-18　TestTrap テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestBadBpdu

TestBadBpdu テストでは、トラップ機能またはスイッチ プロセッサへのパケットのリダイレクト機能について確認します。このテストでは、レイヤ 2 転送エンジンの Trap 機能が適切に動作していることを確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。BPDU 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-19　TestBadBpdu テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestProtocolMatchChannel

TestProtocolMatchChannel テストでは、レイヤ 2 転送エンジンでの特定のレイヤ 2 プロトコルの一致機能について確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Match 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-20　TestProtocolMatchChannel テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestCapture

TestCapture テストでは、レイヤ 2 転送エンジンのキャプチャ機能が適切に動作していることを確認します。キャプチャ機能は、マルチキャスト レプリケーションで使用されます。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Capture 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-21　TestCapture テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

TestStaticEntry

TestStaticEntry テストでは、レイヤ 2 MAC アドレス テーブルでスタティック エントリを読み込む機能について確認します。スーパーバイザ エンジンでテストを実行する場合、診断パケットはスーパーバイザ エンジンの帯域内ポートから送信され、スーパーバイザ エンジンのレイヤ 2 転送エンジンを使用して、パケット ルックアップを実行します。DFC 対応モジュールの場合、診断パケットはスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックに送信され、DFC ポートのいずれかからループ バックされます。Static Entry 機能は、レイヤ 2 転送エンジンによる診断パケットのルックアップ中に確認されます。

表 A-22　TestStaticEntry テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	DFC 対応モジュール

PFC レイヤ 3 転送エンジンのテスト

PFC レイヤ 3 転送エンジンのテストには、次のテストが含まれます。

TestFibDevices

TestFibDevices テストでは、Forwarding Information Base（FIB; 転送情報ベース）Ternary CAM（TCAM）および隣接装置が機能しているかどうかを確認します。FIB TCAM 装置ごとに 1 つの FIB エントリがインストールされます。診断パケットは、TCAM 装置にインストールされている FIB TCAM エントリによりそのパケットがスイッチングされることを確認するために送信されます。これは、完全 TCAM 装置テストではありません。各 TCAM 装置には 1 つのエントリのみがインストールされます。

（注）　IPv4FibShortcut および IPv6FibShortcut テストと異なり、このテストでは IPv4 パケットまたは IPv6 パケット（設定に応じて）を使用して、すべての FIB および隣接装置をテストします。

表 A-23　TestFibDevices テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ルーティング機能に関する問題がある場合は、レイヤ 3 転送機能を確認するため、このテストをオンデマンドで実行します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestIPv4FibShortcut

TestIPv4FibShortcut テストでは、レイヤ 3 転送エンジンの IPv4 FIB 転送が適切に動作していることを確認します。1 つの診断 IPv4 FIB および隣接エントリがインストールされます。診断パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されていることを確認するために送信されます。

表 A-24　TestIPv4FibShortcut テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ルーティング機能に関する問題がある場合は、レイヤ 3 転送機能を確認するため、このテストをオンデマンドで実行します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestIPv6FibShortcut

TestIPv6FibShortcut テストでは、レイヤ 3 転送エンジンの IPv6 FIB 転送が適切に動作していることを確認します。1 つの診断 IPv6 FIB および隣接エントリがインストールされます。診断 IPv6 パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-25　TestIPv6FibShortcut テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ルーティング機能に関する問題がある場合は、レイヤ 3 転送機能を確認するため、このテストをオンデマンドで実行します。このテストは、ヘルス モニタリング テストとしても使用できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestMPLSFibShortcut

TestMPLSFibShortcut テストでは、レイヤ 3 転送エンジンの MPLS 転送が適切に動作していることを確認します。1 つの診断 MPLS FIB および隣接エントリがインストールされます。診断 MPLS パケットは、隣接エントリからの MPLS ラベルに従ってそのパケットが転送されることを確認するために送信されます。

表 A-26　TestMPLSFibShortcut テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストは、ヘルス モニタリング テストとしても使用できます。MPLS トラフィックをルーティングしている場合は、ヘルス モニタリング テストとして使用します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestNATFibShortcut

TestNATFibShortcut テストでは、Network Address Translation（NAT; ネットワーク アドレス変換）隣接情報に基づいてパケットを書き換えする機能について確認します。1 つの診断 NAT FIB および隣接エントリがインストールされます。診断パケットは、書き換えられた IP アドレスに従ってそのパケットが転送されることを確認するために送信されます。

表 A-27　TestNATFibShortcut テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストは、ヘルス モニタリング テストとしても使用できます。宛先 IP アドレスが書き換えられている場合（たとえば、NAT を使用している場合）、ヘルス モニタリング テストとして使用します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestL3Capture2

TestL3Capture2 テストでは、レイヤ 3 転送エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が適切に動作していることを確認します。このキャプチャ機能は、ACL ロギングおよび VACL ロギングで使用されます。キャプチャ 2 ビットが設定された 1 つの診断 FIB および隣接エントリがインストールされます。診断パケットは、キャプチャ ビット情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-28　TestL3Capture2 テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストは、ヘルス モニタリング テストとしても使用できます。ACL または VACL ロギングを使用する場合は、ヘルス モニタリング テストとして使用します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestAclPermit

TestAclPermit テストでは、ACL 許可機能が適切に動作していることを確認します。特定の診断パケットを許可する ACL エントリは、ACL TCAM にインストールされます。対応する診断パケットがスーパーバイザ エンジンから送信され、レイヤ 3 転送エンジンで検索されて、ACL TCAM エントリにヒットすること、および許可され適切に転送されることを確認します。

表 A-29　TestAclPermit テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストは、ヘルス モニタリング テストとしても使用できます。ACL を使用している場合は、ヘルス モニタリング テストとして使用します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestAclDeny

TestAclDeny テストでは、レイヤ 2 およびレイヤ 3 転送エンジンの ACL 拒否機能が適切に動作していることを確認します。このテストでは、各種 ACL 拒否シナリオ（入力、出力、レイヤ 2 リダイレクト、レイヤ 3 リダイレクト、およびレイヤ 3 ブリッジなど）を使用して、ACL 拒否機能が適切に動作していることを確認します。

表 A-30　TestAclDeny テストの属性

属性	説明
中断の有無	中断なし
推奨事項	ディセーブルにしないでください。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX
修正措置	自動的に ASIC をリセットして、回復します。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestNetflowShortcut

TestNetflowShortcut テストでは、レイヤ 3 転送エンジンの Netflow 転送機能が適切に動作していることを確認します。1 つの診断 Netflow エントリおよび隣接エントリがインストールされます。診断パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-31　TestNetflowShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、500 ミリ秒です。
推奨事項	Netflow が適切に動作していないことが疑われる場合は、このテストをオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestQoS

TestQoS テストでは、QoS の入力および出力 TCAM をプログラミングすることより、QoS の入力および出力 TCAM が機能しているかどうかを確認します。診断パケットの ToS 値は入力または出力のいずれかを反映して変更されます。

表 A-32　TestQoS テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、500 ミリ秒です。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

DFC レイヤ 3 転送エンジンのテスト

DFC レイヤ 3 転送エンジンのテストには、次のテストが含まれます。

TestFibDevices

TestFibDevices テストでは、FIB TCAM および隣接装置が機能していることを確認します。FIB TCAM 装置ごとに 1 つの FIB エントリがインストールされます。診断パケットは、TCAM 装置にインストールされた FIB TCAM エントリによりそのパケットがスイッチングされることを確認するために送信されます。これは、完全 TCAM 装置テストではありません。TCAM 装置ごとに 1 つのエントリがインストールされます。

（注）　IPv4FibShortcut および IPv6FibShortcut テストと異なり、TestFibDevices テストでは IPv4 または IPv6（設定に応じて）を使用して、すべての FIB および隣接装置をテストします。

表 A-33　TestFibDevices テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestIPv4FibShortcut

TestIPv4FibShortcut テストでは、レイヤ 3 転送エンジンの IPv4 FIB 転送機能が適切に動作していることを確認します。1 つの診断 IPv4 FIB および隣接エントリがインストールされます。診断パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-34　TestIPv4FibShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestIPv6FibShortcut

TestIPv6FibShortcut テストでは、レイヤ 3 転送エンジンの IPv6 FIB 転送機能が適切に動作していることを確認します。1 つの診断 IPv6 FIB および隣接エントリがインストールされます。診断 IPv6 パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-35　TestIPv6FibShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestMPLSFibShortcut

TestMPLSFibShortcut テストでは、レイヤ 3 転送エンジンの MPLS 転送機能が適切に動作していることを確認します。1 つの診断 MPLS FIB および隣接エントリがインストールされます。診断 MPLS パケットは、隣接エントリからの MPLS ラベルを使用してそのパケットが転送されることを確認するために送信されます。

表 A-36　TestMPLSFibShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestNATFibShortcut

TestNATFibShortcut テストでは、NAT 隣接情報（書き換え宛先 IP アドレスなど）に基づいてパケットを書き換えする機能について確認します。1 つの診断 NAT FIB および隣接エントリがインストールされます。診断パケットは、書き換えられた IP アドレスに従ってそのパケットが転送されることを確認するために送信されます。

表 A-37　TestNATFibShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestL3Capture2

TestL3Capture2 テストでは、レイヤ 3 転送エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が適切に動作していることを確認します。このキャプチャ機能は、ACL ロギングおよび VACL ロギングで使用されます。キャプチャ 2 ビットが設定された 1 つの診断 FIB および隣接エントリがインストールされます。診断パケットは、キャプチャ ビット情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-38　TestL3Capture2 テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestAclPermit

TestAclPermit テストでは、ACL 許可機能が適切に動作していることを確認します。特定の診断パケットを許可する ACL エントリは、ACL TCAM にインストールされます。対応する診断パケットがスーパーバイザ エンジンから送信され、レイヤ 3 転送エンジンで検索されて、ACL TCAM エントリにヒットすること、および許可され適切に転送されることを確認します。

表 A-39　TestAclPermit テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestAclDeny

TestAclDeny テストでは、レイヤ 2 およびレイヤ 3 転送エンジンの ACL 拒否機能が適切に動作していることを確認します。このテストでは、各種 ACL 拒否シナリオ（入力および出力 レイヤ 2 リダイレクト、レイヤ 3 リダイレクト、およびレイヤ 3 ブリッジなど）を使用します。

表 A-40　TestAclDeny テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。中断時間は、ループ バックされるポートの設定（たとえば、STP など）により異なります。
推奨事項	ACL を使用する場合は、ダウンタイム中にスケジューリングします。
デフォルト	オフ
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestQoS

TestQoS テストでは、QoS の入力および出力 TCAM をプログラミングすることより、QoS の入力および出力 TCAM が機能しているかどうかを確認します。診断パケットの ToS 値は入力または出力のいずれかを反映して変更されます。

表 A-41　TestQoS テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。
推奨事項	ダウンタイム中にスケジューリングします。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

TestNetflowShortcut

TestNetflowShortcut テストでは、レイヤ 3 転送エンジンの Netflow 転送機能が適切に動作していることを確認します。1 つの診断 Netflow エントリおよび隣接エントリがインストールされます。診断パケットは、書き換えられた MAC 情報および VLAN 情報に従ってそのパケットが転送されることを確認するために送信されます。

表 A-42　TestNetflowShortcut テストの属性

属性	説明
中断の有無	ループ バックされるポートに対しては中断あり。中断は、通常 1 秒未満です。
推奨事項	Netflow が適切に動作していないことが疑われる場合は、このテストをオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび DFC 対応モジュール

レプリケーション エンジン テスト

レプリケーション エンジン テストには、次のテストが含まれます。

TestL3VlanMet

TestL3VlanMet テストでは、レプリケーション エンジンのマルチキャスト機能が適切に動作していることを確認します。レプリケーション エンジンは、診断パケットのマルチキャスト レプリケーションが異なる 2 つの VLAN に対して実行されるよう設定されます。診断パケットがスーパーバイザ エンジンの帯域内ポートから送信されたあと、テストでは 2 つのパケットがレプリケーション エンジンで設定された 2 つの VLAN 上 の帯域内ポートで再度受信されることを確認します。

表 A-43　TestL3VlanMet テストの属性

属性	説明
中断の有無	スーパーバイザ エンジンでは中断なし DFC 搭載モジュールでは中断あり 中断は通常、ループ バックされたポート上で 1 秒未満で行われます。
推奨事項	レプリケーション エンジンのマルチキャスト レプリケーション機能をテストするには、このテストをオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび WS-65xx、WS-67xx、および WS-68xx モジュール

TestIngressSpan

TestIngressSpan テストでは、ポート ASIC が入力 Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）用にパケットをタグ付けできることを確認します。またこのテストでは、両方の SPAN キュー用の書き換えエンジンの入力 SPAN 処理が適切に動作していることを確認します。

表 A-44　TestIngressSpan テストの属性

属性	説明
中断の有無	両方の SPAN セッションに対しては中断あり。モジュール上のループバック ポートに対しても中断あり。中断時間は、ループバック ポートの設定（たとえば、STP など）により異なります。
推奨事項	このテストはオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび WS-65xx および WS-67xx モジュール

TestEgressSpan

TestEgressSpan テストでは、両方の SPAN キュー用の書き換えエンジンの出力 SPAN レプリケーション機能が適切に動作していることを確認します。

表 A-45　TestEgressSpan テストの属性

属性	説明
中断の有無	両方の SPAN セッションに対しては中断あり。中断は、通常 1 秒未満です。
推奨事項	このテストはオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンおよび WS-65xx および WS-67xx モジュール

ファブリック テスト

ファブリック テストには、次のテストが含まれます。

TestFabricSnakeForward

TestFabricSnakeForward テストには、内部スネーク テストと外部スネーク テストの 2 つのテスト ケースがあります。内部スネーク テストでは、テスト パケットがファブリック ASIC 内で生成され、テスト データ パスがファブリック ASIC 内に留まるように制限されます。外部スネーク テストでは、スーパーバイザ エンジンの帯域内ポートを使用してテスト パケットが生成され、テスト データ パスにはポート ASIC、スーパーバイザ エンジン内部の書き換えエンジン ASIC、およびファブリック ASIC が含まれます。スーパーバイザ エンジンのローカル チャネルがファブリック ASIC に同期化されるかどうかにより、使用されるテストが決定します。同期化された場合は外部スネーク テスト、同期化されない場合は内部スネーク テストが使用されます。両方のテストで、いずれのモジュールにも同期化されていないチャネルのみがテストに関わります。転送方向は、スネーキング方向が小さい値のチャネルから大きい値のチャネルであることを示します。

表 A-46　TestFabricSnakeForward テストの属性

属性	説明
中断の有無	中断なし
推奨事項	オンデマンドで実行します。このテストにより CPU 使用率が上がる可能性があります。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	スーパーバイザ エンジンはクラッシュして ROMMON となり、SFM はリセットされます。
ハードウェア サポート	Supervisor Engine 720 および SFM

TestFabricSnakeBackward

TestFabricSnakeBackward テストには、内部スネーク テストと外部スネーク テストの 2 つのテスト ケースがあります。内部スネーク テストでは、テスト パケットがファブリック ASIC 内で生成され、テスト データ パスがファブリック ASIC 内に留まるように制限されます。外部スネーク テストでは、スーパーバイザ エンジンの帯域内ポートを使用してテスト パケットが生成され、テスト データ パスにはポート ASIC、スーパーバイザ エンジン内の書き換えエンジン ASIC、およびファブリック ASIC が含まれます。スーパーバイザ エンジンのローカル チャネルがファブリック ASIC に同期化されるかどうかにより、使用されるテストが決定します。同期化された場合は外部スネーク テストが、同期化されない場合は内部スネーク テストが使用されます。両方のテストで、いずれのモジュールにも同期化されていないチャネルのみがテストに関わります。逆方向は、スネーキング方向が大きい値のチャネルから小さい値のチャネルであることを示します。

表 A-47　TestFabricSnakeBackward テストの属性

属性	説明
中断の有無	中断なし
推奨事項	オンデマンドで実行します。このテストにより CPU 使用率が上がる可能性があります。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.1(13)E、12.2(14)SX
修正措置	スーパーバイザ エンジンはクラッシュして ROMMON となり、SFM はリセットされます。
ハードウェア サポート	Supervisor Engine 720 および SFM

TestSynchedFabChannel

TestSynchedFabChannel テストでは、モジュールとファブリックの両方のファブリック同期ステータスを定期的に確認します。このテストは、ファブリック対応モジュールでのみ使用できます。このテストは、パケットスイッチング テストではないため、データ パスを含みません。このテストでは、モジュールおよびファブリックに SCP 制御メッセージを送信して、同期ステータスをクエリーします。

表 A-48　TestSynchedFabChannel テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストをオフにしないでください。ヘルスモニタリング テストとして使用します。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX
修正措置	5 回連続して失敗すると、モジュールがリセットされます。3 回連続してリセットされると、モジュールの電源が切断されます。失敗の種類によっては、ファブリック スイッチ オーバーが開始される場合があります。
ハードウェア サポート	ファブリック対応モジュール。

TestFabricCh0Health

TestFabricCh0Health テストでは、10 ギガビット モジュール上のファブリック チャネル 0 に対する入力および出力データ パスのヘルスを常にモニタします。このテストは、5 秒ごとに実行されます。10 回連続して失敗すると致命的障害と見なされ、モジュールがリセットされます。3 回連続してリセットされると、ファブリック スイッチオーバーが実行される場合があります。

表 A-49　TestFabricCh0Health テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストをオフにしないでください。ヘルスモニタリング テストとして使用します。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX
修正措置	10 回連続して失敗すると、モジュールがリセットされます。3 回連続してリセットされると、モジュールの電源が切断されます。
ハードウェア サポート	WS-X6704-10GE および WS-6702-10GE

TestFabricCh1Health

TestFabricCh1Health テストでは、10 ギガビット モジュール上のファブリック チャネル 1 に対する入力および出力データ パスのヘルスを常にモニタします。このテストは、5 秒ごとに実行されます。10 回連続して失敗すると致命的障害と見なされ、モジュールがリセットされます。3 回連続してリセットされると、ファブリック スイッチオーバーが実行される場合があります。

表 A-50　TestFabricCh1Health テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストをオフにしないでください。ヘルスモニタリング テストとして使用します。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX
修正措置	10 回連続して失敗すると、モジュールがリセットされます。3 回連続して失敗すると、モジュールの電源が切断されます。
ハードウェア サポート	WS-X6704-10GE モジュール

完全メモリ テスト

完全メモリ テストには、次のテストが含まれます。

「TestFibTcamSSRAM」（P.A-33）
「TestAsicMemory」（P.A-34）
「TestAclQosTcam」（P.A-34）
「TestNetFlowTcam」（P.A-35）
「TestQoSTcam」（P.A-35）

（注）　スーパーバイザ エンジンは、メモリ テストの実行後にリブートする必要があるため、他のモジュールでメモリ テストを実行してからスーパーバイザ エンジンで実行してください。オンデマンドのオンライン診断テストについての詳細は、「オンデマンド オンライン診断の設定」（P.55-3）を参照してください。

TestFibTcamSSRAM

TestFibTcamSSRAM テストでは、FIB TCAM およびレイヤ 3 隣接 SSRAM メモリを確認します。

表 A-51　TestFibTcamSSRAM テストの属性

属性	説明
中断の有無	中断あり。中断は、数時間になります。
推奨事項	このテストは、ハードウェアでの問題が疑われる場合に限り使用するか、またはハードウェアを実稼動中のネットワークに組み込む前に使用します。テスト中のモジュールのバックグラウンドでトラフィックを実行しないでください。スーパーバイザ エンジンを、このテスト後にリブートする必要があります。
デフォルト	オフ
リリース	12.1(20)E、12.2(14)SX、12.2(17a)SX
修正措置	適用不可
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

TestAsicMemory

TestAsicMemory テストでは、モジュールのメモリをテストするアルゴリズムを使用します。

表 A-52　TestAsicMemory テストの属性

属性	説明
中断の有無	中断あり。中断は約 1 時間となります。
推奨事項	このテストは、ハードウェアでの問題が疑われる場合に限り使用するか、またはハードウェアを実稼動中のネットワークに組み込む前に使用します。テスト中のモジュールのバックグラウンドでトラフィックを実行しないでください。スーパーバイザ エンジンを、このテスト後にリブートする必要があります。
デフォルト	オフ
リリース	12.2(17a)SX.
修正措置	適用不可
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

TestAclQosTcam

TestAclQosTcam ではすべてのビットをテストして、PFC3BXL および PFC3B 上の ACL および QoS TCAM の場所を確認します。PFC3A ではサポートされません。

表 A-53　TestAclQosTcam テストの属性

属性	説明
中断の有無	中断あり。中断は約 1 時間となります。
推奨事項	このテストは、ハードウェアでの問題が疑われる場合に限り使用するか、またはハードウェアを実稼動中のネットワークに組み込む前に使用します。テスト中のモジュールのバックグラウンドでトラフィックを実行しないでください。スーパーバイザ エンジンを、このテスト後にリブートする必要があります。
デフォルト	オフ
リリース	12.2(18)SXD
修正措置	適用不可
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

TestNetFlowTcam

TestNetFlowTcam テストでは、すべてのビットをテストして、Netflow TCAM の場所を確認します。

表 A-54　TestNetFlowTcam テストの属性

属性	説明
中断の有無	中断あり。中断時間は数分で、PFC3A、PFC3BXL、または PFC3B をのいずれをテストするかにより異なります。
推奨事項	このテストは、ハードウェアでの問題が疑われる場合に限り使用するか、またはハードウェアを実稼動中のネットワークに組み込む前に使用します。テスト中のモジュールのバックグラウンドでトラフィックを実行しないでください。スーパーバイザ エンジンを、このテスト後にリブートする必要があります。
デフォルト	オフ
リリース	12.2(18)SXD
修正措置	適用不可
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

TestQoSTcam

TestQoSTcam テストでは、QoS TCAM 装置の完全メモリ テストを実行します。

表 A-55　TestQoSTcam テストの属性

属性	説明
中断の有無	中断あり。中断時間は数分で、PFC3A、PFC3BXL、または PFC3B をのいずれをテストするかにより異なります。
推奨事項	このテストは、ハードウェアでの問題が疑われる場合に限り使用するか、またはハードウェアを実稼動中のネットワークに組み込む前に使用します。テスト中のモジュールのバックグラウンドでトラフィックを実行しないでください。スーパーバイザ エンジンを、このテスト後にリブートする必要があります。
デフォルト	オフ
リリース	12.2(18)SXD
修正措置	適用不可
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

IPSEC サービス モジュール テスト

IPSEC サービス モジュール テストには、次のテストが含まれます。

TestIPSecClearPkt

TestIPSecClearPkt テストでは、パケットをスーパーバイザ エンジンの帯域内ポートからスイッチ ファブリックまたはバスを介して、暗号エンジンに送信します。このパケットは、暗号エンジンからスーパーバイザ エンジンの帯域内ポートに暗号化されずに返送されます。パケットは、暗号化されていないことおよびパケット データ フィールドが確保されていることを確認されます。レイヤ 2 ルックアップは、スーパーバイザ帯域内ポートと暗号エンジン間のパケットに行われます。

表 A-56　TestIPSecClearPkt テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストはオンデマンドで実行します。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.2(18)SXE2.2.
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	VPN サービス モジュール

TestHapiEchoPkt

TestHapiEchoPkt テストでは、制御パスを使用して暗号エンジンに Hapi Echo パケットを送信します。暗号エンジンに送信された Hapi Echo パケットは、暗号エンジンからエコー バックされます。パケットは、インデックスダイレクトを使用してスーパーバイザ エンジンの帯域内ポートから暗号エンジンに送信され、ブロードキャストを使用して診断 VLAN に返送されます。

表 A-57　TestHapiEchoPkt テストの属性

属性	説明
中断の有無	中断あり。
推奨事項	このテストはオンデマンドで実行します。このテストは、オンデマンド Command-Line Interface（CLI; コマンドライン インターフェイス）から実行できません。
デフォルト	オン
リリース	12.2(18)SXE2
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	VPN サービス モジュール

TestIPSecEncryptDecryptPkt

TestIPSecEncryptDecryptPkt テストでは、スイッチ ファブリックまたはバス（適用可能ないずれか）を使用して、スーパーバイザ エンジンの帯域内ポートと IPSec サービス モジュール（WS-SVC-IPSEC、SPA-IPSEC）の暗号エンジン間でパケットを交換することにより、暗号化機能を確認します。パケットを何度か交換したら、暗号エンジンにより行われた暗号化および複合化プロセス後に元のデータが保持されていることを確認します。レイヤ 2 ルックアップは、スーパーバイザ帯域内ポートと暗号エンジン間のパケットに行われます。

表 A-58　TestIPSecEncryptDecryptPkt テストの属性

属性	説明
中断の有無	中断なし テストは、デフォルトで毎分実行されます。
推奨事項	このテストは、ブートアップ時にのみ実行できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.2(18)SXE2.2.
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	VPN サービス モジュール

ストレス テスト

ストレス テストには、次のテストが含まれます。

「TestTrafficStress」（P.A-38）
「TestEobcStressPing」（P.A-38）

TestTrafficStress

TestTrafficStress テストでは、モジュールのすべてのポートを、相互にパケットを送受信するペアに設定することにより、スイッチおよび搭載されたモジュールのストレス テストを行います。テストでは、パケットを所定の時間スイッチに通過させたあと、このパケットが廃棄されないことを確認します。

表 A-59　TestTrafficStress テストの属性

属性	説明
中断の有無	中断あり。中断は、数分になります。
推奨事項	このテストでハードウェアの状態を確認してから、ネットワークに搭載します。
デフォルト	オフ
リリース	12.2(18)SXF
修正措置	適用不可
ハードウェア サポート	Supervisor Engine 720 および Supervisor Engine 32

TestEobcStressPing

TestEobcStressPing テストでは、モジュールとスーパーバイザ エンジンとの EOBC リンクのストレス テストを行います。このテストは、スーパーバイザ エンジンが一定数（デフォルトでは 1）の sweep-ping プロセスを開始すると始まります。sweep-ping プロセスでは、20,000 個の SCP-ping パケットによりモジュールへの ping を実行します。各パケットの ping がタイムアウト（2 秒）になる前に 20,000 パケットすべての応答があった場合、テストは合格です。テストが成功でない場合は、テスト中の EOBC バス上のトラフィック バーストに対応するため 5 回の再試行が許可されます。

表 A-60　TestEobcStressPing テストの属性

属性	説明
中断の有無	中断あり。中断は、数分になります。
推奨事項	このテストでハードウェアの状態を確認してから、ネットワークに搭載します。
デフォルト	オフ
リリース	12.2(18)SXD
修正措置	適用不可
ハードウェア サポート	Supervisor Engine 720 および Supervisor Engine 32

クリティカル リカバリ テスト

クリティカル リカバリ テストには、次のテストが含まれます。

- 「TestL3HealthMonitoring」（P.A-39）
- 「TestTxPathMonitoring」（P.A-40）
- 「TestSynchedFabChannel」（P.A-40）

TestFabricCh0Health テストおよび TestFabricCh1Health テストもクリティカル リカバリ テストと見なされます。これらのテストの説明については、「ファブリック テスト」（P.A-30）を参照してください。

TestL3HealthMonitoring

TestL3HealthMonitoring テストは、検出されたハードウェア障害からシステムが自己回復を試行すると常に、ローカル DFC 上での IPv4 および IPv6 パケット スイッチングに関する一連の診断テストを開始します。このテストにより、前面パネル ポート（通常、ポート 1）がテスト用にシャット ダウンされます。診断テストに合格しない場合は、ハードウェア障害を回復できず、自己回復シーケンスが再度適用されることを意味します。

表 A-61　TestL3HealthMonitoring テストの属性

属性	説明
中断の有無	中断あり。中断は、通常 1 秒未満です。中断時間は、ループバックされるポートの設定（たとえば、STP など）により異なります。テスト中、転送およびポート機能は中断されます。
推奨事項	ディセーブルにしないでください。
デフォルト	オン
リリース	12.2(14)SX
修正措置	適用不可
ハードウェア サポート	DFC 搭載モジュール

TestTxPathMonitoring

TestTxPathMonitoring テストでは、Supervisor Engine 720 および WS-X67xx シリーズ モジュール上の各ポートにインデックスダイレクト パケットを定期的に送信して、ASIC 同期化を確認し、関連する問題をすべて修正します。このテストは、2 秒ごとに実行されます。

表 A-62　TestTxPathMonitoring テストの属性

属性	説明
中断の有無	中断なし
推奨事項	デフォルト設定を変更しないでください。
デフォルト	オン
リリース	12.2(14)SX
修正措置	適用できません（自己回復）。
ハードウェア サポート	Supervisor Engine 720 および WS-67xx シリーズ モジュール

TestSynchedFabChannel

TestSynchedFabChannel テストでは、モジュールとファブリックの両方のファブリック同期ステータスを定期的に確認します。このテストは、ファブリック対応モジュールでのみ使用できます。このテストは、パケットスイッチング テストではないため、データ パスを含みません。このテストでは、モジュールおよびファブリックに SCP 制御メッセージを送信して、同期ステータスをクエリーします。

表 A-63　TestSynchedFabChannel テストの属性

属性	説明
中断の有無	中断なし
推奨事項	オフにしないでください。ヘルスモニタリング テストとして使用します。
デフォルト	オン
リリース	12.1(13)E、12.2(14)SX
修正措置	なし 詳細については、システム メッセージ ガイドを参照してください。
ハードウェア サポート	ファブリック対応モジュール。

一般テスト

一般テストには、次のテストが含まれます。

ScheduleSwitchover

ScheduleSwitchover テストにより、オンライン診断のスケジューリング機能を使用して、いつでもスイッチオーバーを開始できるようになります。

表 A-64　ScheduleSwitchover テストの属性

属性	説明
中断の有無	中断あり。
推奨事項	このテストはダウンタイム中にスケジューリングして、スイッチオーバー後に引き継がれるスタンバイ スーパーバイザ エンジンの機能をテストします。
デフォルト	オフ
リリース	12.2(17B)SXA
修正措置	なし
ハードウェア サポート	スーパーバイザ エンジンのみ

TestFirmwareDiagStatus

TestFirmwareDiagStatus テストでは、モジュール ブートアップ中にファームウェアによって実行されるパワーオン診断テストの結果を表示します。

表 A-65　TestFirmwareDiagStatus テストの属性

属性	説明
中断の有無	中断なし
推奨事項	このテストは、ブートアップ時にのみ実行できます。
デフォルト	このテストはデフォルトで、ブートアップ中、リセット後または OIR 後に実行されます。
リリース	12.2(18)SXD
修正措置	なし システム メッセージ ガイドを参照してください。
ハードウェア サポート	スーパーバイザ エンジンを含むすべてのモジュール

略語

表 B-1 このマニュアルで使用している略語の定義を示します。

表 B-1　　略語リスト

略語	説明
AAL	ATM Adaptation Layer; ATM アダプテーション レイヤ
ACE	Access Control Entry; アクセス制御エントリ
ACL	Access Control List; アクセス制御リスト
AFI	Authority and Format Identifier
Agport	Aggregation Port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation; 自動パケット認識および変換
ARP	Address Resolution Protocol; アドレス解決プロトコル
ATA	アナログ電話アダプタ
ATM	Asynchronous Transfer Mode; 非同期転送モード
AV	Attribute Value; アトリビュート値
BDD	Binary Decision Diagrams
BECN	Backward Explicit Congestion Notification; 逆方向明示的輻輳通知
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit; ブリッジ プロトコル データ ユニット
BRF	Bridge Relay Function; ブリッジ リレー機能
BSC	Bisync
BSTUN	Block Serial Tunnel; ブロック シリアル トンネル
BUS	Broadcast and Unknown Server
BVI	Bridge-Group Virtual Interface; ブリッジ グループ仮想インターフェイス
CAM	Content-Addressable Memory; 連想メモリ
CAR	Committed Access Rate; 専用アクセス レート
CCA	Circuit Card Assembly
CDP	Cisco Discovery Protocol; Cisco 検出プロトコル

表 B-1　略語リスト （続き）

略語	説明
CEF	Cisco Express Forwarding; シスコ エクスプレス フォワーディング
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate; 認定情報速度
CIST	Common and Internal Spanning Tree
CLI	Command-Line Interface; コマンドライン インターフェイス
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service; コネクション モード ネットワーク サービス
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	Class of Service; サービス クラス
CPLD	Complex Programmable Logic Device
CRC	Cyclic Redundancy Check; 巡回冗長検査
CRF	Concentrator Relay Function; コンセントレータ リレー機能
CST	CST
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding; 分散 Cisco Express Forwarding
DDR	Dial-on-Demand Routing; ダイヤル オンデマンド ルーティング
DE	Discard Eligibility; 廃棄適性
DEC	Digital Equipment Corporation
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control; データ リンク制御
DLSw	Data Link Switching; データ リンク スイッチング
DMP	Data Movement Processor
DNS	Domain Name System; ドメイン ネーム システム
DoD	Department of Defense; 米国国防総省
DoS	Denial of Service; サービス拒絶
dot1q	802.1Q
DRAM	Dynamic RAM; ダイナミック RAM
DRiP	Dual Ring Protocol
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSPU	Downstream SNA Physical Units
DTP	Dynamic Trunking Protocol; ダイナミック トランキング プロトコル

表 B-1　略語リスト （続き）

略語	説明
DTR	Data Terminal Ready; データ端末動作可能
DXI	Data Exchange Interface; データ交換インターフェイス
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	Electrically Erasable Programmable Read-Only Memory; 電気的消去再書き込み可能 ROM
EHSA	Enhanced High System Availability; 拡張高システム可用性
EIA	Electronic Industries Association; 米国電子工業会
ELAN	Emulated Local Area Network; エミュレート LAN
EOBC	Ethernet Out-of-Band Channel
EOF	End Of File
ESI	End-System Identifier
FAT	File Allocation Table
FECN	Forward Explicit Congestion Notification; 前方明示的輻輳通知
FM	Feature Manager
FRU	Field Replaceable Unit; 現場交換可能ユニット
fsck	file system consistency check
FSM	Feasible Successor Metrics
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-Card Communication
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	Interface Descriptor Block
IDP	Initial Domain Part または Internet Datagram Protocol
IDSM	Intrusion Detection System Module
IFS	IOS File System
IGMP	Internet Group Management Protocol; インターネットグループ管理プロトコル
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	Interprocessor Communication; プロセッサ間通信
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link; スイッチ間リンク

表 B-1　略語リスト （続き）

略語	説明
ISO	International Organization of Standardization; 国際標準化機構
ISR	Integrated SONET Router
IST	Internal Spanning Tree
LAN	Local Area Network
LANE	LAN Emulation; LAN エミュレーション
LAPB	Link Access Procedure, Balanced; 平衡型リンク アクセス手順
LCP	Link Control Protocol; リンク制御プロトコル
LDA	Local Director Acceleration
LEC	LAN Emulation Client; LANE クライアント
LECS	LAN Emulation Configuration Server; LANE コンフィギュレーション サーバ
LEM	Link Error Monitor; リンク エラー モニタ
LER	Link Error Rate; リンク エラー レート
LES	LAN Emulation Server; LANE サーバ
LLC	Logical Link Control; 論理リンク制御
LTL	Local Target Logic
MAC	Media Access Control; メディア アクセス制御
MD5	Message Digest 5
MFD	Multicast Fast Drop
MSFC	Multilayer Switch Feature Card; マルチレイヤ スイッチ フィーチャ カード
MIB	Management Information Base; 管理情報ベース
MII	Media-Independent Interface; メディア独立型インターフェイス
MLS	Multilayer Switching; マルチレイヤ スイッチング
MLSE	Maintenance Loop Signaling Entity
MOP	Maintenance Operation Protocol
MOTD	Message-Of-The-Day
MLSE	Maintenance Loops Signaling Entity
MRM	Multicast Routing Monitor
MSDP	Multicast Source Discovery Protocol
MSFC	Multilayer Switching Feature Card; マルチレイヤ スイッチング フィーチャ カード
MSM	Multilayer Switch Module; マルチレイヤ スイッチ モジュール
MST	Multiple Spanning Tree; 多重スパニング ツリー
MTU	Maximum Transmission Unit; 最大伝送ユニット
MVAP	Multiple VLAN Access Port
NAM	Network Analysis Module; ネットワーク解析モジュール
NBP	Name Binding Protocol; ネーム バインディング プロトコル

表 B-1　略語リスト （続き）

略語	説明
NCIA	Native Client Interface Architecture; ネイティブ クライアント インターフェイス アーキテクチャ
NDE	NetFlow Data Export; NetFlow データ エクスポート
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card; NetFlow フィーチャ カード
NMP	Network Management Processor; ネットワーク管理プロセッサ
NSAP	Network Service Access Point; ネットワーク サービス アクセス ポイント
NSF	Nonstop Forwarding; ノンストップフォワーディング
NTP	Network Time Protocol
NVRAM	Nonvolatile RAM; 不揮発性 RAM
OAM	Operation, Administration, and Maintenance
ODM	Order Dependent Merge
OSI	Open System Interconnection; 開放型システム間相互接続
OSM	Optical Services Module; オプティカル サービス モジュール
OSPF	Open Shortest Path First
PAE	Port Access Entity
PAgP	Port Aggregation Protocol; ポート集約プロトコル
PBD	Packet Buffer Daughterboard
PC	Personal Computer; パーソナル コンピュータ（従来の PCMCIA）
PCM	Pulse Code Modulation; パルス符号変調
PCR	Peak Cell Rate; ピーク セル レート
PDP	Policy Decision Point; ポリシー デシジョン ポイント
PDU	Protocol Data Unit; プロトコル データ ユニット
PEP	Policy Enforcement Point
PFC	Policy Feature Card; ポリシー フィーチャ カード
PGM	Pragmatic General Multicast
PHY	Physical Sublayer; 物理サブレイヤ
PIB	Policy Information Base
PIM	Protocol Independent Multicast
PPP	Point-to-Point Protocol; ポイントツーポイント プロトコル
PRID	Policy Rule Identifiers
PVST+	Per-VLAN Spanning-Tree+
QDM	QoS Device Manager
QM	QoS Manager
QoS	Quality of Service; サービス品質
RACL	Router Interface Access Control List
RADIUS	Remote Access Dial-In User Service

表 B-1　略語リスト （続き）

略語	説明
RAM	Random-Access Memory; ランダムアクセス メモリ
RCP	Remote Copy Protocol
RGMP	Router-Ports Group Management Protocol
RIB	Routing Information Base
RIF	Routing Information Field; ルーティング情報フィールド
RMON	Remote Network Monitor
ROM	Read-Only Memory
ROMMON	ROM Monitor
RP	Route Processor; ルート プロセッサまたは Rendezvous Point; ランデブー ポイント
RPC	Remote Procedure Call; リモート プロシージャ コール
RPF	Reverse Path Forwarding
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy Plus
RSPAN	Remote SPAN
RST	Reset
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	Service Access Point; サービス アクセス ポイント
SCM	Service Connection Manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	Single In-line Memory Module
SLB	Server Load Balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol; シリアル ライン インターネット プロトコル
SMDS	Software Management and Delivery Systems
SMF	Software MAC Filter; ソフトウェア MAC フィルタ
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol; シンプル マルチキャスト ルーティング プロトコル
SMT	Station Management; ステーション管理
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol; 簡易ネットワーク管理プロトコル
SRM	Single Router Mode
SSO	Stateful Switchover

表 B-1　略語リスト （続き）

略語	説明
SPAN	Switched Port Analyzer; スイッチド ポート アナライザ
SREC	S-Record 形式、Motorola が定義した ROM 内容の形式
SSTP	Cisco Shared Spanning-Tree
STP	Spanning-Tree Protocol; スパニング ツリー プロトコル
SVC	Switched Virtual Circuit; 相手先選択接続
SVI	Switched Virtual Interface; スイッチ仮想インターフェイス
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	Table Contention Level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol; 簡易ファイル転送プロトコル
TIA	Telecommunications Industry Association; 米国電気通信工業会
TopN	ユーザがレポートでポート トラフィックを分析できるようにするユーティリティ
ToS	Type of Service; サービス タイプ
TLV	Type-Length-Value
TTL	Time to Live
TVX	Valid Transmission
UDLD	UniDirectional Link Detection Protocol; 単一方向リンク検出プロトコル
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time; 協定世界時
VACL	VLAN Access Control List; VLAN アクセス制御リスト
VCC	Virtual Channel Circuit; 仮想チャネル回線
VCI	Virtual Circuit Identifier; 仮想回線識別子
VCR	Virtual Configuration Register; 仮想コンフィギュレーション レジスタ
VINES	Virtual Network System
VLAN	Virtual LAN; 仮想 LAN
VMPS	VLAN Membership Policy Server; VLAN メンバシップ ポリシー サーバ
VPN	Virtual Private Network; バーチャル プライベート ネットワーク
VRF	VPN Routing and Forwarding; VPN ルーティング / 転送
VTP	VLAN Trunking Protocol; VLAN トランキング プロトコル
VVID	Voice VLAN ID
WAN	Wide Area Network
WCCP	Web Cache Communication Protocol
WFQ	Weighted Fair Queueing; 均等化キューイング
WRED	Weighted Random Early Detection; 重み付きランダム早期検出

表 B-1　略語リスト （続き）

略語	説明
WRR	Weighted Round-Robin; 重み付きラウンドロビン
XNS	Xerox Network System

数字

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

て

と

に

ね

の

は

ひ

ふ

ほ

ま

む

も

ゆ

よ

ら

り

る

れ

ろ