Cisco 7600 シリーズ ルータ Cisco IOS ソフトウェア コンフィギュレーション ガイド

2012 年 6 月 29 日

Text Part Number: OL-10113-24-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、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、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。

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

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に準拠しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

• 干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。

• テレビまたはラジオの左右どちらかの側に装置を移動させます。

• テレビまたはラジオから離れたところに装置を移動させます。

• テレビまたはラジオとは別の回路にあるコンセントに装置を接続します （装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

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

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

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

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

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

Cisco 7600 シリーズ ルータ 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 15 S
© 2010-12 Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに xlv

対象読者 xlv

マニュアルの変更履歴 xlv

マニュアルの構成 li

関連資料 liv

表記法 lvi

マニュアルの入手方法およびテクニカル サポート lvi

CHAPTER 1 製品概要 1-1

サポート対象ハードウェアおよびソフトウェア 1-1

ユーザ インターフェイス 1-1

組み込み CiscoView サポートの設定 1-2

組み込み CiscoView の概要 1-2

組み込み CiscoView のインストールおよび設定 1-2

組み込み CiscoView 情報の表示 1-3

PFC および DFC がハードウェアでサポートするソフトウェア機能 1-3

PFC3、DFC3、および DFC がハードウェアでサポートするソフトウェア機能 1-3

PFC3 および DFC3 がハードウェアでサポートするソフトウェア機能 1-4

CHAPTER 2 ルータの初期設定 2-1

デフォルト設定 2-1

ルータ の設定 2-2

セットアップ機能または setup コマンドの使用 2-2

コンフィギュレーション モードの使用 2-3

実行コンフィギュレーションを保存する前の確認 2-4

実行コンフィギュレーションの保存 2-5

設定の確認 2-5

スタティック ルートの設定 2-5

BOOTP サーバの設定 2-6

Cisco 7600 でのルート ヘルス インジェクション 2-7

特権 EXEC コマンドへのアクセスの保護 2-8

スタティック イネーブル パスワードの設定または変更 2-8

enable password コマンドおよび enable secret コマンドの使用 2-9

回線パスワードの設定または変更 2-9

特権 EXEC モードに対する TACACS+ パスワード保護の設定 2-10
パスワードの暗号化 2-11
複数の特権レベルの設定 2-11
コマンドの特権レベルの設定 2-12
回線のデフォルト特権レベルの変更 2-12
特権レベルへのログイン 2-12
特権レベルの終了 2-12
パスワード、アクセス レベル、および特権レベルの設定の表示 2-12
イネーブル パスワードを忘れた場合の回復方法 2-13
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 2-13
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 2-14
スーパーバイザ エンジンの起動プロセスの概要 2-14
ROM モニタの概要 2-14
ソフトウェア コンフィギュレーション レジスタの設定 2-15
ブート フィールドの変更および boot コマンドの使用 2-16
ブート フィールドの変更 2-16
コンフィギュレーション レジスタ設定値の確認 2-18
スタートアップ システム イメージの指定 2-18
フラッシュ メモリの概要 2-18
フラッシュ メモリの機能 2-19
セキュリティ機能 2-19
フラッシュ メモリの設定プロセス 2-19
CONFIG_FILE 環境変数 2-19
環境変数の制御 2-20

CHAPTER 3 **Supervisor Engine 720 の設定 3-1**
Supervisor Engine 720 におけるブートフラッシュまたはブートディスクの使用 3-1
Supervisor Engine 720 でのスロットの使用 3-2
Supervisor Engine 720 ポートの設定 3-2
スイッチ ファブリック機能の設定とモニタリング 3-2
スイッチ ファブリック機能の機能概要 3-2
スイッチ ファブリック機能の概要 3-3
レイヤ 3 スイッチド トラフィックの転送の決定 3-3
スイッチング モード 3-3
スイッチ ファブリック機能の設定 3-4
スイッチ ファブリック機能のモニタ 3-5
スイッチ ファブリック冗長ステータスの表示 3-5
ファブリック チャネルのスイッチング モードの表示 3-5
ファブリック ステータスの表示 3-6

ファブリック使用率の表示 3-6
ファブリック エラーの表示 3-6

CHAPTER 4 Route Switch Processor 720 の設定 4-1
RSP720 PFC の互換性のマトリクス 4-1
RSP720 の機能 4-2
RSP720 でのフラッシュ メモリのアクセス 4-6
ルート スイッチ プロセッサ 720 ポートの設定 4-6
スイッチ ファブリック機能の設定とモニタリング 4-7
スイッチ ファブリック機能の機能概要 4-7
スイッチ ファブリック機能の概要 4-7
レイヤ 3 スイッチド トラフィックの転送の決定 4-7
スイッチング モード 4-8
スイッチ ファブリック機能の設定 4-8
スイッチ ファブリック機能のモニタ 4-9
スイッチ ファブリック冗長ステータスの表示 4-9
ファブリック チャネルのスイッチング モードの表示 4-9
ファブリック ステータスの表示 4-10
ファブリック使用率の表示 4-10
ファブリック エラーの表示 4-11

CHAPTER 5 NSF with SSO スーパーバイザ エンジンの冗長構成の設定 5-1
NSF with SSO スーパーバイザ エンジンの冗長構成について 5-1
NSF with SSO スーパーバイザ エンジンの冗長構成の概要 5-2
SSO の動作 5-2
NSF の動作 5-3
シスコ エクスプレス フォワーディング 5-3
マルチキャスト MLS NSF with SSO 5-4
ルーティング プロトコル 5-4
BGP の動作 5-4
OSPF の動作 5-5
IS-IS の動作 5-6
EIGRP の動作 5-7
NSF の利点および制約事項 5-8
スーパーバイザ エンジンの設定の同期化 5-9
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 5-9
冗長構成設定時の注意事項および制約事項 5-9
ハードウェア設定時の注意事項および制約事項 5-10
コンフィギュレーション モードに関する制約事項 5-10

NSF の設定作業 5-11
SSO の設定 5-11
マルチキャスト MLS NSF with SSO の設定 5-12
マルチキャスト NSF with SSO の確認 5-12
CEF NSF の設定 5-13
CEF NSF の確認 5-13
BGP NSF の設定 5-13
BGP NSF の確認 5-14
OSPF NSF の設定 5-15
OSPF NSF の確認 5-15
IS-IS NSF の設定 5-16
IS-IS NSF の確認 5-17
EIGRP NSF の設定 5-18
EIGRP NSF の確認 5-18
スーパーバイザ エンジンの設定の同期化 5-19
冗長スーパーバイザ エンジンへのファイルのコピー 5-19

CHAPTER 6 **Cisco 7600 シリーズ ルータでの ISSU および eFSU 6-1**
ISSU および eFSU の概要 6-1
ISSU の概要 6-2
eFSU の概要 6-2
停止時間とサポートに関する考慮事項 6-3
ラインカード メモリの予約 6-3
eFSU の動作 6-4
ラインカード ソフトウェア プリロードのエラー処理 6-4
Cisco 7600ISSU および eFSU のサポート 6-5
ISSU のサポート 6-5
eFSU のサポート 6-7
Cisco 7600ISSU および eFSU の注意事項および制約事項 6-7
稼働中ソフトウェア アップグレードの実行 6-9
ソフトウェア アップグレード プロセスの概要 6-9
アップグレードの準備 6-11
互換性マトリクス チェックのディセーブル化 6-11
ブート イメージのバージョンとブート変数の確認 6-11
冗長モードの確認 6-12
ISSU ステートの確認 6-12
新しいソフトウェア イメージのコピー 6-13
スタンバイ RP への新しいソフトウェアのロード 6-13
インストールされているラインカードの最大停止時間の表示（任意） 6-15

スイッチオーバーのアクティブからスタンバイへの強制切り替え 6-16
新しいソフトウェア バージョンの許可とロールバック プロセスの停止（任意） 6-18
スタンバイに対する新しいソフトウェアの認定 6-19
ソフトウェア インストレーションの確認 6-20
アップグレード プロセスの中断 6-21
非 eFSU イメージの eFSU イメージへのアップグレード 6-21
コマンド リファレンス 6-21

CHAPTER 7 **RPR および RPR+ スーパーバイザ エンジンの冗長設定 7-1**
RPR および RPR+ の概要 7-1
スーパーバイザ エンジンの冗長構成の概要 7-2
RPR の動作 7-2
RPR+ の動作 7-3
スーパーバイザ エンジンの設定の同期化 7-3
RPR スーパーバイザ エンジンの設定の同期化 7-4
RPR+ スーパーバイザ エンジンの設定の同期化 7-4
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 7-4
冗長構成に関する注意事項および制約事項 7-4
RPR+ に関する注意事項および制約事項 7-5
ハードウェア設定時の注意事項および制約事項 7-6
コンフィギュレーション モードに関する制約事項 7-6
スーパーバイザ エンジンの冗長構成の設定 7-6
冗長構成の設定 7-7
スーパーバイザ エンジンの設定の同期化 7-7
冗長ステートの表示 7-8
Fast Software Upgrade の実行 7-8
冗長スーパーバイザ エンジンへのファイルのコピー 7-10

CHAPTER 8 **インターフェイスの設定 8-1**
インターフェイス設定の概要 8-1
interface コマンドの使用 8-2
インターフェイス範囲の設定 8-3
インターフェイス範囲マクロの定義および使用 8-4
オプションのインターフェイス機能の設定 8-5
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 8-5
速度およびデュプレックス モード設定上のガイドライン 8-6
イーサネット インターフェイス速度の設定 8-6
インターフェイスのデュプレックス モードの設定 8-7

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 8-7
速度およびデュプレックス モードの設定の表示 8-8
ジャンボ フレーム サポートの設定 8-9
ジャンボ フレーム サポートの概要 8-9
MTU サイズの設定 8-11
IEEE 802.3X フロー制御の設定 8-12
ポート デバウンス タイマーの設定 8-13
インターフェイスに関する記述の追加 8-14
活性挿抜の概要 8-15
インターフェイスのモニタおよびメンテナンス 8-15
TDR を使用したケーブル ステータスの確認 8-16

CHAPTER 9 **Supervisor Engine 32 の設定** 9-1
Supervisor Engine 32 のフラッシュ メモリ 9-1
Supervisor Engine 32 ポート 9-2

CHAPTER 10 **レイヤ 2 スイッチング用 LAN ポートの設定** 10-1
レイヤ 2 スイッチングの機能概要 10-1
レイヤ 2 イーサネット スイッチングの概要 10-1
レイヤ 2 イーサネット スイッチングの概要 10-2
セグメント間のフレーム スイッチング 10-2
アドレス テーブルの作成 10-2
VLAN トランクの概要 10-3
トランキングの概要 10-3
カプセル化タイプ 10-3
レイヤ 2 LAN ポート モード 10-4
レイヤ 2 LAN インターフェイスのデフォルト設定 10-5
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 10-5
レイヤ 2 スイッチング用の LAN インターフェイスの設定 10-6
レイヤ 2 スイッチング用の LAN ポートの設定 10-7
トランクとしてのレイヤ 2 スイッチング ポートの設定 10-8
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 10-8
DTP を使用するためのレイヤ 2 トランクの設定 10-9
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 10-9
アクセス VLAN の設定 10-10
802.1Q ネイティブ VLAN の設定 10-10
トランク上で許容される VLAN のリストの設定 10-11
プルーニング適格 VLAN のリストの設定 10-11
トランクの設定の完了 10-12

レイヤ 2 トランクの設定の確認 10-12
設定および確認の例 10-12
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 10-13
カスタム IEEE 802.1Q EtherType フィールド値の設定 10-15

CHAPTER 11 **Flex Link の設定 11-1**
Flex Link の概要 11-1
Flex Link の設定 11-2
Flex Link のデフォルト設定 11-2
Flex Link 設定時の注意事項および制約事項 11-2
Flex Link の設定 11-3
モニタリング :Flex Link 11-4

CHAPTER 12 **EtherChannel の設定 12-1**
EtherChannel の機能概要 12-1
EtherChannel 機能の概要 12-1
EtherChannel の設定方法の概要 12-2
EtherChannel の設定の概要 12-2
EtherChannel の手動設定の概要 12-3
PAgP による EtherChannel 設定 12-3
IEEE 802.3ad LACP EtherChannel 設定の概要 12-4
LACP 1:1 冗長性機能の概要 12-5
ポートチャネル インターフェイスの概要 12-5
ロード バランシングの概要 12-6
EtherChannel 機能の設定時の注意事項および制約事項 12-6
EtherChannel の設定 12-8
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 12-8
チャネル グループの設定 12-9
LACP のシステム プライオリティおよびシステム ID の設定 12-11
EtherChannel ロード バランシングの設定 12-12
EtherChannel Min-Links 機能の設定 12-12
ファスト スイッチオーバーでの LACP 1:1 冗長性機能の設定 12-13

CHAPTER 13 **VTP の設定 13-1**
VTP の機能概要 13-1
VTP ドメインの概要 13-2
VTP モードの概要 13-2
VTP アドバタイズの概要 13-3
VTP バージョンの概要 13-3

VTP バージョン 2 13-3
VTP バージョン 3 13-4
VTP プルーニングの概要 13-5
VTP のデフォルト設定 13-6
VTP 設定時の注意事項および制約事項 13-7
VTP の設定 13-8
VTP グローバル パラメータの設定 13-8
VTP パスワードの設定 13-9
VTP プルーニングのイネーブル化 13-10
VTP バージョン番号のイネーブル化 13-10
VTP モードの設定 13-11
テイクオーバーの起動 13-13
VTP 統計情報の表示 13-14
ドメインの VTP デバイスの表示 13-14

CHAPTER 14 **VLAN の設定** 14-1
VLAN の機能概要 14-1
VLAN の概要 14-1
VLAN の範囲 14-2
設定可能な VLAN パラメータ 14-2
トークンリング VLAN の概要 14-3
トークンリング TrBRF VLAN 14-3
トークンリング TrCRF VLAN 14-4
VLAN のデフォルト設定 14-6
自動保護スイッチング グループ内の Bridged Routed Encapsulation と VLAN の相互作用 14-8
サポートされるラインカード 14-8
要件および制限事項 14-8
警告メッセージ 14-9
VLAN 設定時の注意事項および制約事項 14-9
VLAN の設定 14-10
VLAN 設定のバックグラウンド情報 14-10
イーサネット VLAN の作成または変更 14-11
VLAN へのレイヤ 2 LAN インターフェイスの割り当て 14-13
内部 VLAN 割り当てポリシーの設定 14-13
VLAN 変換の設定 14-14
VLAN 変換に関する注意事項および制約事項 14-14
トランク ポート上の VLAN 変換の設定 14-16
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 14-16

802.1Q VLAN から ISL VLAN へのマッピング 14-17

CHAPTER 15 プライベート VLAN の設定 15-1

プライベート VLAN の機能概要 15-1
プライベート VLAN ドメイン 15-2
プライベート VLAN ポート 15-3
プライマリ VLAN、独立 VLAN、コミュニティ VLAN 15-3
プライベート VLAN ポートの分離 15-4
プライベート VLAN による IP アドレス指定方式 15-4
複数のルータにわたるプライベート VLAN 15-5
プライベート VLAN とその他の機能の相互作用 15-5
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 15-6
プライベート VLAN と SVI 15-6
プライベート VLAN 設定時の注意事項および制約事項 15-6
セカンダリ VLAN およびプライマリ VLAN の設定 15-7
プライベート VLAN ポートの設定 15-9
その他の機能の制限事項 15-9
プライベート VLAN の設定 15-11
プライベート VLAN としての VLAN の設定 15-12
セカンダリ VLAN とプライマリ VLAN の関連付け 15-13
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 15-14
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 15-15
プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 15-16
プライベート VLAN のモニタ 15-17

CHAPTER 16 Cisco IP Phone サポートの設定 16-1

Cisco IP Phone のサポートの概要 16-1
Cisco IP Phone の接続 16-1
Cisco IP Phone の音声トラフィック 16-2
Cisco IP Phone のデータ トラフィック 16-3
Cisco IP Phone の電源構成 16-3
Cisco IP Phone へのローカル電力供給 16-3
Cisco IP Phone へのインライン パワー供給 16-3
Cisco IP Phone サポートのデフォルト設定 16-4
Cisco IP Phone サポートの設定時の注意事項と制約事項 16-4
Cisco IP Phone サポートの設定 16-5
音声トラフィックのサポートの設定 16-5

データ トラフィックのサポートの設定 16-7
インライン パワー サポートの設定 16-8

CHAPTER 17 IEEE 802.1Q トンネリングの設定 17-1
802.1Q トンネリングの機能概要 17-1
802.1Q トンネリングの設定時の注意事項および制約事項 17-4
802.1Q トンネリングの設定 17-6
802.1Q トンネル ポートの設定 17-6
ネイティブ VLAN トラフィックにタグを付けるためのルータ設定 17-7
IEEE 802.1ab LLDP 17-7
LLDP の概要 17-8
制限事項 17-9
デフォルトの LLDP 設定 17-10
Cisco 7600 シリーズ ルータでの LLDP の設定 17-10
LLDP の設定 17-10
LLDP のモニタリングと維持 17-12
設定の確認 17-13
トラブルシューティングのヒント 17-16

CHAPTER 18 レイヤ 2 プロトコル トンネリングの設定 18-1
レイヤ 2 プロトコル トンネリングの機能概要 18-1
レイヤ 2 プロトコル トンネリングのサポートの設定 18-2

CHAPTER 19 L2TPv3 の設定 19-1
L2TPv3 の概要 19-1
L2TPv3 の制約事項 19-2
L2TPv3 の設定 19-2

CHAPTER 20 STP および MST の設定 20-1
STP の機能概要 20-1
STP の概要 20-2
ブリッジ ID の概要 20-2
ブリッジ プライオリティ値 20-3
拡張システム ID 20-3
STP MAC アドレス割り当て 20-3
BPDU の概要 20-3
ルート ブリッジの選定 20-4
STP プロトコル タイマー 20-4

スパニングツリー トポロジーの作成 20-5
STP ポート ステート 20-5
STP ポート ステートの概要 20-6
ブロッキング ステート 20-7
リスニング ステート 20-8
ラーニング ステート 20-9
フォワーディング ステート 20-10
ディセーブル ステート 20-11
STP および IEEE 802.1Q トランク 20-12
IEEE 802.1w RSTP の機能概要 20-13
ポートの役割およびアクティブ トポロジー 20-13
高速コンバージェンス 20-14
ポートの役割の同期 20-15
BPDU の形式および処理 20-16
BPDU の形式および処理の概要 20-16
優位 BPDU 情報の処理 20-17
下位 BPDU 情報の処理 20-17
トポロジの変更 20-18
Rapid PVST 20-18
MST の概要 20-18
MST の概要 20-19
MST 領域 20-19
IST、CIST、CST 20-20
IST、CIST、CST の概要 20-20
MST リージョン内におけるスパニングツリーの動作 20-21
MST リージョン間のスパニングツリーの動作 20-21
IEEE 802.1s の用語 20-22
ホップ カウント 20-23
境界ポート 20-23
規格準拠 MST 実装 20-24
ポートの役割の命名規則の変更点 20-24
レガシーおよび規格準拠ルータの間のスパニングツリー相互運用 20-24
単一方向リンク障害の検出 20-25
IEEE 802.1D-1998 STP とのインターオペラビリティ 20-26
STP の設定 20-26
STP のデフォルト設定 20-27
STP のイネーブル化 20-27
拡張システム ID のイネーブル化 20-29
ルート ブリッジの設定 20-29

セカンダリ ルート ブリッジの設定 20-30
STP ポート プライオリティの設定 20-31
STP ポート コストの設定 20-33
VLAN のブリッジ プライオリティの設定 20-34
hello タイムの設定 20-35
VLAN の転送遅延時間の設定 20-36
VLAN の最大エージング タイムの設定 20-36
Rapid-PVST のイネーブル化 20-37
リンク タイプの設定 20-37
プロトコル移行の再起動 20-37
MST の設定 20-37
デフォルト MST 設定 20-38
MST 設定時の注意事項および制約事項 20-38
MST リージョン設定の指定および MST のイネーブル化 20-39
ルート ブリッジの設定 20-41
セカンダリ ルート ブリッジの設定 20-42
ポート プライオリティの設定 20-43
パス コストの設定 20-44
スイッチのプライオリティの設定 20-45
hello タイムの設定 20-46
転送遅延時間の設定 20-47
送信保留カウントの設定 20-47
最大経過時間の設定 20-48
最大ホップ カウントの設定 20-48
高速移行を保証するリンク タイプの指定 20-49
ネイバー タイプの指定 20-49
プロトコル移行プロセスの再開 20-50
MST の設定およびステータスの表示 20-50

CHAPTER 21 **オプションの STP 機能の設定 21-1**
PortFast の機能概要 21-2
BPDU ガードの機能概要 21-2
PortFast BPDU フィルタリングの機能概要 21-2
UplinkFast の機能概要 21-3
BackboneFast の機能概要 21-4
EtherChannel ガードの機能概要 21-6
ルート ガードの機能概要 21-7
ループ ガードの機能概要 21-7

PortFast のイネーブル化 21-8
PortFast BPDU フィルタリングのイネーブル化 21-10
BPDU ガードのイネーブル化 21-12
UplinkFast のイネーブル化 21-12
BackboneFast のイネーブル化 21-13
EtherChannel ガードのイネーブル化 21-14
ルート ガードのイネーブル化 21-15
ループ ガードのイネーブル化 21-15

CHAPTER 22 レイヤ 3 インターフェイスの設定 22-1
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 22-1
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 22-2
IPv4 ルーティングおよびアドレスの設定 22-3
IPX ルーティングおよびネットワーク番号の設定 22-7
AppleTalk ルーティング、ケーブルの範囲、およびゾーンの設定 22-8
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 22-9

CHAPTER 23 GTP-SLB IPV6 サポートの設定 23-1
GTP-SLB の IPv6 サポート 23-1
GTP-SLB アーキテクチャの概要 23-2
PDP の作成コール フロー 23-2
GTP エコー要求コール フロー 23-3
GTP 通知メッセージ 23-3
制約事項および使用上の注意事項 23-4
GTP-SLB IPv6 サポートの設定 23-4
サーバファームの設定 23-5
仮想サーバの設定 23-7
例 23-12
検証 23-13
GTP-SLB IPv6 サポートの設定のトラブルシューティング 23-15

CHAPTER 24 IP Subscriber Awareness over Ethernet 24-1
概要 24-1
利点 24-2
IP 加入者のインターフェイス 24-3
IP 加入者セッション 24-3
IP 加入者セッションの機能 24-4

IP アドレス割り当て 24-5
IP サブネット（IP 範囲）セッション 24-5
IP インターフェイス セッション 24-6
ポート チャネル上での PPPoE セッションと IPoE セッションのサポート（1:1 冗長性） 24-6
IEEE 802.1AH Customer Ethertype を使用した QinQ サブインターフェイス上での PPPoE セッションと IPoE セッションのサポート 24-6
制約事項と使用上のガイドライン 24-7
検証 24-8
QoS に関する推奨事項 24-21
帯域幅余剰比率に関する推奨事項 24-21
BRR 設定時の注意事項 24-22
BRR の設定方法 24-22
プライオリティ レート伝播に関する推奨事項 24-26
サポートされない IP 加入者セッションの機能 24-28
IP Subscriber Awareness over Ethernet 設定時の注意事項 24-28
他の機能との相互作用 24-29
IP Subscriber Awareness over Ethernet の設定 24-29
設定の概要 24-29
設定例 24-31
コマンド リファレンス 24-33

CHAPTER 25 **UDE および UDLR の設定 25-1**
UDE および UDLR の概要 25-1
UDE および UDLR の概要 25-1
サポート対象ハードウェア 25-2
UDE の概要 25-2
UDE の概要 25-2
ハードウェアベース UDE の概要 25-2
ソフトウェアベース UDE の概要 25-3
UDLR の概要 25-3
UDE および UDLR の設定 25-3
UDE の設定 25-3
UDE 設定時の注意事項 25-4
ハードウェアベース UDE の設定 25-5
ソフトウェアベース UDE の設定 25-5
UDLR の設定 25-6
UDLR バックチャネル トンネル設定時の注意事項 25-6
UDE 送信専用ポートの受信専用トンネル インターフェイスの設定 25-7
UDE 受信専用ポートの送信専用トンネル インターフェイスの設定 25-7

CHAPTER 26 PFC のマルチプロトコル ラベル スイッチングの設定 26-1

PFC MPLS ラベル スイッチング 26-1
MPLS の概要 26-2
MPLS ラベル スイッチングの概要 26-2
IP から MPLS 26-3
MPLS から MPLS 26-4
MPLS から IP 26-4
MPLS VPN 転送 26-4
再循環 26-4
サポート対象ハードウェア機能 26-5
サポート対象 Cisco IOS 機能 26-5
MPLS に関する注意事項および制約事項 26-7
MPLS でサポートされるコマンド 26-8
MPLS の設定 26-8
MPLS のラベル単位ロード バランシング 26-8
基本的な MPLS ロード バランシング 26-9
MPLS レイヤ 2 VPN ロード バランシング 26-9
MPLS レイヤ 3 VPN ロード バランシング 26-9
MPLS の設定例 26-9
マルチキャスト隣接割り当て 26-10
マルチキャスト隣接割り当ての制限 26-10
マルチキャスト隣接割り当ての設定 26-11
設定例 26-12
設定の確認 26-12
PFC の VPN スイッチング 26-15
PFC の VPN スイッチングの動作 26-15
MPLS VPN に関する注意事項および制約事項 26-16
MPLS VPN でサポートされるコマンド 26-17
MPLS VPN の設定 26-17
MPLS VPN 設定例 26-17
Any Transport over MPLS 26-19
AToM ロード バランシング 26-19
EoMPLS の概要 26-19
EoMPLS に関する注意事項および制約事項 26-20
スケーラブル EoMPLS とポートモード EoMPLS 26-22
イーサネット AC の HSPW サポート 26-22
SwEoMPLS および VPLS のサンプル設定 26-22
ブリッジ プロトコル データ ユニットを可能にするためのスパニングツリー プロトコルの管理 26-24

EoMPLS の設定 26-25
前提条件 26-25
PFC モードの VLAN ベース EoMPLS の設定 26-25
PFC のポートベース EoMPLS の設定 26-29
LAN カードにおける 7600-MUX-UNI サポートの設定 26-32

CHAPTER 27 **IPv4 マルチキャスト VPN サポートの設定 27-1**
MVPN の機能概要 27-1
MVPN の概要 27-2
マルチキャスト ルーティング、転送、マルチキャスト ドメイン 27-2
マルチキャスト配信ツリー 27-2
Multicast Tunnel Interface 27-5
MVPN の PE ルータ ルーティング テーブルのサポート 27-6
Multicast Distributed Switching サポート 27-6
ハードウェア処理の IPv4 マルチキャスト 27-7
MVPN 設定時の注意事項および制約事項 27-7
MVPN の設定 27-8
出力および入力マルチキャスト レプリケーション モードの設定 27-9
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 27-10
VRF エントリの設定 27-11
ルート識別子の設定 27-11
ルートターゲット拡張コミュニティの設定 27-12
デフォルト MDT の設定 27-12
データ MDT の設定（任意） 27-13
データ MDT ロギングのイネーブル化 27-14
設定例 27-14
VRF 情報の表示 27-14
マルチキャスト VRF ルーティングの設定 27-16
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 27-17
IPv4 マルチキャスト VRF ルーティングのイネーブル化 27-17
PIM VRF 登録メッセージ送信元アドレスの設定 27-18
PIM VRF ランデブー ポイント（RP）アドレスの指定 27-18
Multicast Source Discovery Protocol（MSDP）ピアの設定 27-19
IPv4 マルチキャスト ヘッダー ストレージのイネーブル化 27-19
マルチキャスト ルートの最大数の設定 27-20
IPv4 マルチキャスト ルート フィルタリングの設定 27-20
設定例 27-20
IPv4 マルチキャスト VRF ルーティング情報の表示 27-21
MVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定 27-21

マルチキャスト ルーティング設定の概要 27-21
インターフェイスでの PIM の設定 27-22
IPv4 VRF 転送用インターフェイスの設定 27-23
設定例 27-23
MVPN の設定例 27-23
デフォルト MDT だけの MVPN 設定 27-24
デフォルト MDT およびデータ MDT を含む MVPN 設定 27-25

CHAPTER 28 マルチキャスト VPN エクストラネット サポートの設定 28-1
概要 28-1
エクストラネット MVPN アーキテクチャ 28-1
MVPN エクストラネットの設定 28-2
制約事項および使用上の注意事項 28-3

CHAPTER 29 IP ユニキャスト レイヤ 3 スイッチングの設定 29-1
レイヤ 3 スイッチングの機能概要 29-1
ハードウェア レイヤ 3 スイッチングの概要 29-2
レイヤ 3 スイッチド パケットの書き換え 29-2
ハードウェア レイヤ 3 スイッチングの例 29-3
ハードウェア レイヤ 3 スイッチングのデフォルト設定 29-4
設定時の注意事項および制約事項 29-4
ハードウェア レイヤ 3 スイッチングの設定 29-5
ハードウェア レイヤ 3 スイッチング統計情報の表示 29-6

CHAPTER 30 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 30-1
IPv6 マルチキャストをサポートする機能 30-1
IPv6 マルチキャストの注意事項および制約事項 30-2
IPv6 マルチキャスト レイヤ 3 スイッチングの設定 30-3
show コマンドを使用した IPv6 マルチキャスト レイヤ 3 スイッチングの確認 30-3
MFIB クライアントの確認 30-3
スイッチング機能の表示 30-4
（S,G）転送機能の確認 30-4
（*,G）転送機能の確認 30-4
サブネット エントリ サポート ステータスの確認 30-4
レプリケーション モード機能の表示 30-5
サブネット エントリの表示 30-5
IPv6 マルチキャスト概要の表示 30-5
NetFlow ハードウェア転送カウントの表示 30-5

FIB ハードウェア ブリッジングおよびドロップ カウントの表示 30-6
共有および well-known ハードウェア隣接カウンタの表示 30-6

CHAPTER 31 IPv4 マルチキャスト レイヤ 3 スイッチングの設定 31-1
IPv4 マルチキャスト レイヤ 3 スイッチングの機能概要 31-1
IPv4 マルチキャスト レイヤ 3 スイッチングの概要 31-2
マルチキャスト レイヤ 3 スイッチング キャッシュ 31-2
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 31-3
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 31-4
フローの部分的スイッチング 31-4
フローの完全スイッチング 31-5
非 RPF トラフィックの処理 31-5
非 RPF トラフィックの概要 31-5
スタブ ネットワークのための RPF 障害のフィルタリング 31-6
RPF 障害トラフィックのレート制限 31-6
IPv4 双方向 PIM の機能概要 31-7
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 31-7
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 31-8
制約事項 31-8
サポートされていない機能 31-9
IPv4 マルチキャスト レイヤ 3 スイッチングの設定 31-9
IGMPv3、IGMP v3lite、および URD を使用した Source Specific Multicast 31-10
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 31-10
レイヤ 3 インターフェイス上での IPv4 PIM のイネーブル化 31-10
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 31-11
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 31-11
レプリケーション モードの設定 31-12
ローカル出力レプリケーションのイネーブル化 31-14
レイヤ 3 スイッチングのグローバルしきい値の設定 31-15
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 31-15
フロー統計情報メッセージ インターバルの指定 31-16
RPF 障害に対する ACL ベースのフィルタリングの設定 31-16
レート リミッタ ステータスの確認 31-17
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 31-18
IPv4 マルチキャスト ルーティング テーブルの表示 31-21
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 31-22
IPv4 双方向 PIM の設定 31-23
IPv4 双方向 PIM のグローバルなイネーブル化 31-23

IPv4 双方向 PIM グループのランデブー ポイントの設定 31-24
IPv4 双方向 PIM スキャン インターバルの設定 31-24
IPv4 双方向 PIM 情報の表示 31-25
IPv4 デバッグ コマンドの使用 31-26
31-27

CHAPTER 32 **IPv6 マルチキャスト トラフィック用 MLDv2 スヌーピングの設定 32-1**
MLDv2 スヌーピングの機能概要 32-1
MLDv2 スヌーピングの概要 32-2
MLDv2 メッセージ 32-2
送信元ベース フィルタリング 32-3
明示的ホスト トラッキング 32-3
MLDv2 スヌーピング プロキシ レポート機能 32-3
IPv6 マルチキャスト グループへの加入 32-4
マルチキャスト グループからの脱退 32-6
通常の脱退処理 32-6
高速脱退処理 32-7
MLDv2 スヌーピング クエリアの概要 32-7
デフォルト MLDv2 スヌーピング設定 32-8
MLDv2 スヌーピング設定時の注意事項および制約事項 32-8
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 32-8
MLDv2 スヌーピング クエリアのイネーブル化 32-9
MLDv2 スヌーピングの設定 32-10
MLDv2 スヌーピングのイネーブル化 32-10
マルチキャスト レシーバへのスタティック接続の設定 32-11
マルチキャスト ルータ ポートのスタティックな設定 32-12
MLD スヌーピング クエリー時間の設定 32-12
高速脱退処理のイネーブル化 32-13
SSM セーフ レポート機能のイネーブル化 32-13
明示的ホスト トラッキングの設定 32-13
レポート抑制の設定 32-14
MLDv6 スヌーピング情報の表示 32-14
マルチキャスト ルータ インターフェイスの表示 32-15
MAC アドレス マルチキャスト エントリの表示 32-15
VLAN インターフェイスの MLDv2 スヌーピング情報の表示 32-16

CHAPTER 33 **IPv4 マルチキャスト トラフィック用 IGMP スヌーピングの設定 33-1**
IGMP スヌーピングの機能概要 33-1
IGMP スヌーピングの概要 33-2

マルチキャスト グループへの加入 33-2
マルチキャスト グループからの脱退 33-4
通常の脱退処理 33-4
高速脱退処理 33-5
IGMP スヌーピング クエリアの概要 33-5
IGMP バージョン 3 サポートの概要 33-5
IGMP バージョン 3 サポートの概要 33-6
IGMPv3 高速脱退処理 33-6
プロキシ レポート機能 33-6
明示的ホスト トラッキング 33-7
IGMP スヌーピングのデフォルト設定 33-8
IGMP スヌーピング設定時の注意事項および制約事項 33-8
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 33-8
IGMP スヌーピング クエリアのイネーブル化 33-9
IGMP スヌーピングの設定 33-10
IGMP スヌーピングのイネーブル化 33-10
マルチキャスト レシーバへのスタティック接続の設定 33-11
マルチキャスト ルータ ポートのスタティックな設定 33-12
IGMP スヌーピング クエリー時間の設定 33-12
IGMP 高速脱退処理のイネーブル化 33-13
送信元固有マルチキャスト（SSM）マッピングの設定 33-13
SSM セーフ レポート機能のイネーブル化 33-13
IGMPv3 明示的ホスト トラッキングの設定 33-14
IGMP スヌーピング情報の表示 33-14
マルチキャスト ルータ インターフェイスの表示 33-15
MAC アドレス マルチキャスト エントリの表示 33-15
VLAN インターフェイスの IGMP スヌーピング情報の表示 33-15
IGMP スヌーピング統計情報の表示 33-16
MVR の概要 33-17
マルチキャスト TV アプリケーションでの MVR の使用 33-17
MVR の設定 33-19
MVR のデフォルト設定 33-19
MVR 設定の制約事項 33-19
MVR グローバル パラメータの設定 33-20
MVR インターフェイスの設定 33-22
MVR 情報の表示 33-23
MVR カウンタのクリア 33-25
トラブルシューティング 33-25

CHAPTER 34 **PIM スヌーピングの設定** 34-1
PIM スヌーピングの機能概要 34-1
PIM スヌーピングのデフォルト設定 34-4
PIM スヌーピング設定時の注意事項および制約事項 34-4
PIM スヌーピングの設定 34-4
PIM スヌーピングのグローバルなイネーブル化 34-5
VLAN における PIM スヌーピングのイネーブル化 34-5
PIM スヌーピング指定ルータ フラッディングのディセーブル化 34-6

CHAPTER 35 **ネットワーク セキュリティの設定** 35-1
MAC アドレスベースのトラフィック ブロッキングの設定 35-1
TCP インターセプトの設定 35-2
ユニキャスト RPF チェックの設定 35-2
PFC3 ユニキャスト RPF チェックのサポートの概要 35-2
ユニキャスト RPF チェックに関する注意事項および制約事項 35-3
ユニキャスト RPF チェックの設定 35-3
ユニキャスト RPF チェック モードの設定 35-3
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 35-5
PFC3 での複数パスのインターフェイス グループの設定 35-6
self-ping のイネーブル化 35-6

CHAPTER 36 **Cisco IOS ACL サポートの概要** 36-1
Cisco IOS ACL 設定時の注意事項および制約事項 36-1
ハードウェアおよびソフトウェア ACL のサポート 36-2
PFC3 での最適化 ACL ロギング 36-3
OAL の概要 36-3
OAL に関する注意事項および制約事項 36-3
OAL の設定 36-4
OAL グローバル パラメータの設定 36-4
インターフェイスでの OAL の設定 36-5
OAL 情報の表示 36-5
キャッシュされた OAL エントリのクリア 36-5
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 36-5
レイヤ 4 演算の使用 36-6
論理演算ユニットの使用 36-6

CHAPTER 37 **VACL の設定** 37-1
VACL の概要 37-1

VACL の概要 37-1
ブリッジド パケット 37-2
ルーティング対象パケット 37-2
マルチキャスト パケット 37-3
VACL の設定 37-4
VACL の設定の概要 37-4
VLAN アクセス マップの定義 37-5
VLAN アクセス マップ シーケンスでの match 句の設定 37-6
VLAN アクセス マップ シーケンスでの action 句の設定 37-6
VLAN アクセス マップの適用 37-7
VLAN アクセス マップの設定の確認 37-8
VLAN アクセス マップの設定および確認の例 37-8
キャプチャ ポートの設定 37-9
VACL ロギングの設定 37-10

CHAPTER 38 **Private Hosts（PACL の使用） 38-1**
概要 38-1
VLAN でのホストの分離 38-2
トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用） 38-3
ポート ACL 38-5
設定時の注意事項および制限事項 38-5
他の機能との相互作用 38-8
スプーフィングからの保護 38-9
マルチキャスト動作 38-9
Private Hosts の設定 38-9
設定の概要 38-10
詳細設定手順 38-11
設定例 38-12
コマンド リファレンス 38-13

CHAPTER 39 **オンライン診断の設定 39-1**
オンライン診断の機能概要 39-1
オンライン診断の設定 39-2
ブートアップ オンライン診断レベルの設定 39-2
オンデマンド オンライン診断の設定 39-3
オンライン診断のスケジューリング 39-5
ヘルス モニタリング診断の設定 39-5
オンライン診断テストの実行 39-6
オンライン診断テストの開始または停止 39-6

オンライン診断テストおよびテスト結果の表示 39-7
スケジュール スイッチオーバー 39-10
メモリ テストの実行 39-10
診断の健全性チェック 39-11

CHAPTER 40 サービス拒絶保護の設定 40-1
コントロール プレーン保護の概要 40-1
Cisco 7600 におけるコントロール プレーン保護の実装 40-2
制御パケットのパス 40-2
ラインカードによるコントロール パネル保護のサポート 40-3
PFC または DFC 上の EARL 経由でパントされるパケットのパス 40-5
PFC または DFC におけるコントロール プレーン トラフィックのポリシング 40-6
PFC または DFC の後にパントされるパケットのパス 40-8
IOS 上のパントされたパケットのパス 40-10
コントロール プレーン保護のベスト プラクティス 40-11
DoS 保護の機能概要 40-11
PFC3 による DoS 保護 40-11
セキュリティ ACL および VACL 40-12
QoS レート制限 40-13
uRPF チェック 40-13
トラフィック ストーム制御 40-14
SYN 攻撃を受けているネットワーク 40-14
MLS プロトコル ポリシング 40-15
PFC3 におけるハードウェアベースのレート リミッタ 40-16
共有レート リミッタ 40-16
推奨レート リミッタ設定 40-16
MLS レート リミッタのデフォルト設定 40-24
DoS 保護の設定時の注意事項および制約事項 40-24
PFC3 40-24
パケット廃棄統計情報のモニタ 40-25
レート リミッタ情報の表示 40-28
MLS レート リミッタの設定例 40-29
制御プレーン ポリシングの機能概要 40-31
CoPP のデフォルト設定 40-31
CoPP の設定時の注意事項および制約事項 40-31
CoPP の設定 40-33
CoPP のモニタ 40-35
CoPP ポリシーのカスタマイズ 40-36

CoPP ポリシーの作成 40-36
トラフィック分類の定義 40-40
トラフィック分類の概要 40-40
トラフィック分類のガイドライン 40-41
CoPP トラフィック分類の基本 ACL 例 40-42
スティッキ ARP の設定 40-43

CHAPTER 41 DHCP スヌーピングの設定 41-1
DHCP スヌーピングの概要 41-1
DHCP スヌーピングの概要 41-2
信頼できるソースおよび信頼できないソース 41-2
DHCP スヌーピング バインディング データベース 41-3
パケット検証 41-3
DHCP スヌーピングの Option 82 データ挿入 41-4
DHCP スヌーピング データベース エージェントの概要 41-6
DHCP スヌーピングのデフォルト設定 41-7
DHCP スヌーピング設定時の制約事項および注意事項 41-8
DHCP スヌーピング設定時の制約事項 41-8
DHCP スヌーピング設定時の注意事項 41-8
DHCP スヌーピングの最小設定 41-9
DHCP スヌーピングの設定 41-9
DHCP スヌーピングのグローバルなイネーブル化 41-10
DHCP Option 82 データ挿入のイネーブル化 41-10
信頼できないポートの DHCP Option 82 機能のイネーブル化 41-11
DHCP スヌーピングの MAC アドレス検証のイネーブル化 41-12
VLAN 上での DHCP スヌーピングのイネーブル化 41-12
レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定 41-14
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 41-14
DHCP スヌーピング データベース エージェントの設定 41-15
データベース エージェントの設定例 41-16
例 1：データベース エージェントのイネーブル化 41-16
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 41-17
例 3：DHCP スヌーピング データベースへの情報の追加 41-19
バインディング テーブルの表示 41-19

CHAPTER 42 ダイナミック ARP インスペクションの設定 42-1
DAI の概要 42-1
ARP の概要 42-1
ARP スプーフィング攻撃の概要 42-2

DAI および ARP スプーフィング攻撃の概要 42-2
インターフェイスの信頼状態とネットワーク セキュリティ 42-3
ARP パケットのレート制限 42-4
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 42-5
ドロップされたパケットのロギング 42-5
DAI のデフォルト設定 42-5
DAI 設定時の注意事項および制約事項 42-6
DAI の設定 42-7
VLAN での DAI のイネーブル化 42-7
DAI インターフェイスの信頼状態の設定 42-8
DAI フィルタリングのための ARP ACL の適用 42-9
ARP パケットのレート制限の設定 42-10
DAI errdisable ステート回復のイネーブル化 42-11
追加検証のイネーブル化 42-12
DAI ログ機能の設定 42-13
DAI ログ機能の概要 42-13
DAI のログ バッファ サイズの設定 42-14
DAI のログ システム メッセージの設定 42-14
DAI のログ フィルタリングの設定 42-15
DAI 情報の表示 42-16
DAI の設定例 42-17
例 1：2 つのスイッチが DAI をサポートする場合 42-17
ルータ A の設定 42-17
ルータ B の設定 42-19
例 2：1 つのスイッチが DAI をサポートする場合 42-21

CHAPTER 43 **トラフィック ストーム制御の設定 43-1**
トラフィック ストーム制御の概要 43-1
トラフィック ストームの検出および制御 43-3
トラフィック ストーム制御のデフォルト設定 43-3
設定時の注意事項および制約事項 43-3
トラフィック ストーム制御のイネーブル化 43-4
トラフィック ストーム制御設定の表示 43-6

CHAPTER 44 **不明なユニキャスト フラッディングのブロック 44-1**
UUFB の概要 44-1
UUFB の設定 44-1

CHAPTER 45 PFC QoS の設定 45-1

PFC QoS の機能概要 45-2
PFC QoS でサポートされるポート タイプ 45-2
概要 45-2
コンポーネントの概要 45-5
入力 LAN ポートの PFC QoS 機能 45-6
PFC および DFC の QoS 機能 45-7
出力ポートの QoS 機能 45-10
分類とマーキングの概要 45-14
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 45-14
入力 OSM ポートでの分類とマーキング 45-16
サービス ポリシーとポリシー マップを使用した PFC での分類とマーキング 45-16
MSFC での分類とマーキング 45-17
ポリサー 45-17
ポリサーの概要 45-17
集約ポリサー 45-18
マイクロフロー ポリサー 45-19
ポートベースのキュー タイプの概要 45-20
入力および出力バッファとレイヤ 2 CoS ベース キュー 45-21
入力キュー タイプ 45-23
出力キューのタイプ 45-23
モジュールとキュー タイプのマッピング 45-24
PFC QoS のデフォルト設定 45-27
PFC QoS のグローバルな設定 45-27
PFC QoS がイネーブルの場合のデフォルト値 45-28
受信キュー サイズの割合 45-28
送信キュー サイズの割合 45-29
帯域幅割り当て比率 45-29
デフォルトのドロップしきい値の割合および CoS 値マッピング 45-29
PFC QoS がディセーブルの場合のデフォルト値 45-42
PFC QoS 設定時の注意事項および制約事項 45-42
全般的な注意事項 45-43
PFC の注意事項 45-44
クラス マップ コマンドの制約事項 45-45
ポリシー マップ コマンドの制約事項 45-45
ポリシー マップ クラス コマンドの制約事項 45-46
CIR および PIR レート値に対してサポートされる粒度 45-46
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 45-46
IP precedence 値と DSCP 値 45-48

PFC QoS の設定 45-48
PFC QoS のグローバルなイネーブル化 45-49
DSCP 透過性の設定 45-50
信頼状態の設定 45-50
queueing-only モードのイネーブル化 45-51
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 45-51
レイヤ 2 LAN ポートでの VLAN ベース PFC QoS のイネーブル化 45-52
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 45-53
名前付き集約ポリサーの作成 45-54
PFC QoS ポリシーの設定 45-56
PFC QoS ポリシー設定作業の概要 45-57
MAC ACL の設定 45-58
QoS フィルタリングに対する ARP ACL の設定 45-62
クラス マップの設定 45-62
クラス マップの設定の確認 45-65
ポリシー マップの設定 45-65
ポリシー マップの設定の確認 45-72
インターフェイスへのポリシー マップの対応付け 45-72
PFC による出力 DSCP 変換の設定 45-74
名前付き DSCP 変換マップの設定 45-74
インターフェイスへの出力 DSCP 変換マップの対応付け 45-75
IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定 45-76
入力 CoS 変換の設定に関する注意事項および制約事項 45-76
入力 CoS 変換マップの設定 45-77
IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用 45-78
DSCP 値マッピングの設定 45-78
受信 CoS 値から内部 DSCP 値へのマッピング 45-78
受信 IP precedence 値から内部 DSCP 値へのマッピング 45-79
DSCP マークダウン値の設定 45-80
内部 DSCP 値から出力 CoS 値へのマッピング 45-81
イーサネット LAN ポートおよび OSM 入力ポートの信頼状態の設定 45-82
入力 LAN ポート CoS 値の設定 45-83
標準キューのドロップしきい値の割合設定 45-84
テールドロップ受信キューの設定 45-85
WRED ドロップ送信キューの設定 45-86
WRED ドロップおよびテールドロップ受信キューの設定 45-86
WRED ドロップおよびテールドロップ送信キューの設定 45-87
1q4t/2q2t テールドロップしきい値の割合設定 45-88
QoS ラベルのキューおよびドロップしきい値へのマッピング 45-89

キューおよびドロップしきい値へのマッピングに関する注意事項および制約事項 45-90
DSCP ベースのキュー マッピングの設定 45-90
CoS ベースのキュー マッピングの設定 45-95
標準送信キュー間での帯域幅の割り当て 45-99
1p1q0t および 1p1q8t ポートでの受信キュー サイズ比の設定 45-100
LAN ポート送信キューのサイズ比の設定 45-101
一般的な QoS のシナリオ 45-102
サンプル ネットワークの設計の概要 45-102
アクセス レイヤ内の PC と IP 電話から送信されるトラフィックの分類 45-104
スイッチ間リンク上でのトラフィック プライオリティ値の受け入れ 45-106
スイッチ間リンクでのトラフィックの優先付け 45-107
ポリサーによる PC からのトラフィック量の制限 45-111
PFC QoS の用語 45-112

CHAPTER 46 **PFC QoS 統計データ エクスポートの設定 46-1**
PFC QoS 統計データ エクスポートの概要 46-1
PFC QoS 統計データ エクスポートのデフォルト設定 46-2
PFC QoS 統計データ エクスポートの設定 46-2
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 46-2
ポートの PFC QoS 統計データ エクスポートのイネーブル化 46-3
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 46-4
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 46-5
PFC QoS 統計データ エクスポート間隔の設定 46-7
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 46-8
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 46-9

CHAPTER 47 **Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート 47-1**
MLDP MVPN の設定 47-2
MLDP based MVPN ネットワークのパケット フロー 47-2
制約事項および使用上の注意事項 47-3
7600 での Label Switched Multicast の設定 47-3
MLDP MVPN の設定（イントラネット） 47-4
検証 47-7
エクストラネット サービスに対する MLDP MVPN の設定 47-9
MLDP TE-FRR サポートの設定 47-21
PIM based MVPN での MLDP の設定 47-22
ロード バランシングを伴う MLDP のサポート 47-22

ルート ノード冗長性 47-22
検証 47-23
MLDP MVPN のサンプル設定 47-27
SSM モードを使用した設定例 47-27
SM モードを使用した設定例 47-43
LSM MLDP based MVPN サポートのトラブルシューティング 47-59

CHAPTER 48 **PFC の MPLS QoS の設定 48-1**
用語 48-2
PFC モード MPLS QoS 機能 48-3
MPLS 実験フィールド 48-3
信頼 48-3
分類 48-3
ポリシングおよびマーキング 48-4
IP ToS の保持 48-4
EXP 変換 48-4
MPLS DiffServ トンネリング モード 48-4
PFC モード MPLS QoS の概要 48-4
IP precedence フィールドでの QoS の指定 48-5
PFC モード MPLS QoS 48-5
MPLS ネットワークの入力エッジでの LER 48-6
MPLS ネットワークのコアにある LSR 48-7
MPLS ネットワークの出力エッジでの LER 48-7
PFC モード MPLS QoS の機能概要 48-8
EoMPLS エッジの LER 48-8
イーサネットから MPLS 48-9
MPLS からイーサネット 48-9
IP エッジ（MPLS、MPLS VPN）での LER 48-9
IP から MPLS 48-9
MPLS から IP 48-11
MPLS VPN 48-12
MPLS コアでの LSR 48-13
MPLS から MPLS 48-13
PFC MPLS QoS のデフォルト設定 48-15
MPLS QoS コマンド 48-16
PFC モード MPLS QoS の注意事項および制約事項 48-17
PFC の MPLS QoS の設定 48-17
QoS のグローバルなイネーブル化 48-18
queueing-only モードのイネーブル化 48-19

制約事項および使用上の注意事項 48-19
MPLS パケットを分類するためのクラス マップの設定 48-20
制約事項および使用上の注意事項 48-22
入力ポートへの MPLS パケットの信頼状態の設定 48-22
制約事項および使用上の注意事項 48-23
ポリシー マップの設定 48-23
EXP 値をすべてのインポーズされたラベルに設定するためのポリシー マップの設定 48-23
police コマンドを使用したポリシー マップの設定 48-25
ポリシー マップの表示 48-28
PFC モード MPLS QoS ポリシー マップのクラス サマリーの表示 48-28
すべてのクラスのコンフィギュレーションの表示 48-28
PFC モード MPLS QoS の出力 EXP 変換の設定 48-29
名前付き EXP 変換マップの設定 48-29
インターフェイスへの出力 EXP 変換マップの付加 48-30
EXP 値マッピングの設定 48-30
入力 EXP から内部 DSCP へのマッピングの設定 48-30
名前付き出力 DSCP から出力 EXP へのマッピングの設定 48-31
MPLS DiffServ トンネリング モード 48-31
ショート パイプ モード 48-32
ショート パイプ モードの制約事項および注意事項 48-33
均一モード 48-33
均一モードの制約事項および注意事項 48-34
MPLS DiffServ トンネリングの制約事項および使用上のガイドライン 48-34
ショート パイプ モードの設定 48-35
入力 PE ルータ：カスタマー側に向かうインターフェイス 48-35
入力 PE ルータの設定：P 側に向かうインターフェイス 48-36
設定例 48-37
P ルータの設定：出力インターフェイス 48-38
設定例 48-38
出力 PE ルータの設定：カスタマー側に向かうインターフェイス 48-39
設定例 48-39
均一モードの設定 48-40
入力 PE ルータの設定：カスタマー側に向かうインターフェイス 48-40
設定例 48-41
入力 PE ルータの設定：P 側に向かうインターフェイス 48-41
出力 PE ルータの設定：カスタマー側に向かうインターフェイス 48-42

CHAPTER 49 IEEE 802.1x ポートベースの認証の設定 49-1
IEEE 802.1x ポートベースの認証の概要 49-1
デバイスの役割 49-2
認証の開始およびメッセージ交換 49-3
許可ステートおよび無許可ステートのポート 49-4
DHCP スヌーピングでの IEEE 802.1X 認証の使用 49-5
サポートされるトポロジ 49-5
IEEE 802.1x ポートベースの認証のデフォルト設定 49-6
IEEE 802.1x ポートベースの認証時の注意事項および制約事項 49-7
IEEE 802.1x ポートベースの認証の設定 49-7
IEEE 802.1x ポートベースの認証のイネーブル化 49-8
ルータと RADIUS サーバ間の通信設定 49-9
定期的な再認証のイネーブル化 49-11
手動によるポート接続クライアントの再認証 49-12
ポート接続クライアント認証の初期化 49-12
待機時間の変更 49-13
ルータとクライアント間の再送信時間の変更 49-13
ルータとクライアント間の EAP 要求フレーム再送信時間の設定 49-14
ルータと認証サーバ間のレイヤ 4 パケット再送信時間の設定 49-15
ルータとクライアント間のフレーム再送信回数の設定 49-15
複数ホストのイネーブル化 49-16
IEEE 802.1x 設定をデフォルト値にリセットする方法 49-17
IEEE 802.1x ステータスの表示 49-17

CHAPTER 50 ポート セキュリティの設定 50-1
ポート セキュリティの概要 50-1
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 50-1
スティッキ MAC アドレスによるポート セキュリティ 50-2
デフォルトのポート セキュリティ設定 50-3
ポートセキュリティに関する注意事項および制約事項 50-3
ポート セキュリティの設定 50-4
ポート セキュリティのイネーブル化 50-4
トランクでのポート セキュリティのイネーブル化 50-5
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 50-5
ポートでのポート セキュリティ違反モードの設定 50-6
ポートでのセキュア MAC アドレスの最大数の設定 50-7
スティッキ 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 50-8
ポートでのスタティック セキュア MAC アドレスの設定 50-9

ポートでのセキュア MAC アドレスのエージング設定 50-10
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 50-10
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 50-11
ポート セキュリティ設定の表示 50-11

CHAPTER 51 **UDLD の設定 51-1**
UDLD の機能概要 51-1
UDLD の概要 51-1
UDLD アグレッシブ モード 51-2
UDLD のデフォルト設定 51-3
UDLD の設定 51-3
UDLD のグローバルなイネーブル化 51-3
個別の LAN インターフェイス上での UDLD のイネーブル化 51-4
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 51-4
UDLD プローブ メッセージ間隔の設定 51-5
ディセーブルになった LAN インターフェイスのリセット 51-5

CHAPTER 52 **NetFlow および NDE の設定 52-1**
NetFlow および NDE の機能概要 52-1
NetFlow および NDE の概要 52-2
MSFC 上の NetFlow および NDE 52-2
PFC 上の NetFlow および NDE 52-2
フロー マスク 52-3
NDE のバージョン 52-4
MLS キャッシュ エントリ 52-7
NetFlow サンプリング 52-8
NetFlow アグリゲーション 52-10
インターフェイス単位の NetFlow および NDE 52-11
インターフェイス単位の NetFlow と NDE の使用上の注意事項および制限事項 52-12
インターフェイス単位の NetFlow および NDE の設定 52-13
インターフェイス単位の NetFlow および NDE の確認 52-13
IPv6 用 NetFlow バージョン 9 52-14
VRF インターフェイス上の NDE 52-14
NetFlow および NDE のデフォルト設定 52-15
NetFlow および NDE 設定時の注意事項および制約事項 52-15
NetFlow と NDE の設定 52-17
PFC 上のフローに対する NetFlow および NDE の設定 52-17
PFC 上のフローに対する NetFlow の設定 52-17

NDE のイネーブル化 52-23
MSFC 上のフローに対する NetFlow および NDE の設定 52-23
MSFC 上のフローに対する NetFlow のイネーブル化 52-24
MSFC 上のフローに対する NetFlow アグリゲーションの設定 52-24
MSFC NDE 送信元レイヤ 3 インターフェイスの設定 52-25
NDE の宛先の設定 52-25
入力ブリッジド IP トラフィックに対する NetFlow および NDE のイネーブル化 52-26
VLAN 上の入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化 52-26
VLAN 上の入力ブリッジド IP トラフィックに対する NDE のイネーブル化 52-27
NDE アドレスおよびポートの設定の表示 52-27
NDE フロー フィルタの設定 52-28
NDE フロー フィルタの概要 52-28
ポート フロー フィルタの設定 52-29
ホストおよびポート フロー フィルタの設定 52-29
ホスト フロー フィルタの設定 52-29
プロトコル フロー フィルタの設定 52-30
プロトコル フロー フィルタを設定するための使用上のガイドライン 52-30
NDE の設定の表示 52-30

CHAPTER 53 **ローカル SPAN、RSPAN、および ERSPAN の設定 53-1**
ローカル SPAN、RSPAN、および ERSPAN の機能概要 53-1
ローカル SPAN、RSPAN、および ERSPAN の概要 53-2
ローカル SPAN の概要 53-2
RSPAN の概要 53-3
ERSPAN の概要 53-4
SPAN 送信元でモニタされるトラフィックについて 53-4
ローカル SPAN、RSPAN、および ERSPAN の送信元 53-5
送信元ポートと EtherChannel 53-5
送信元 VLAN 53-5
ローカル SPAN、RSPAN、および ERSPAN の宛先 53-6
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 53-6
機能の非互換性 53-6
ローカル SPAN、RSPAN、および ERSPAN セッションの制限 53-7
ローカル SPAN、RSPAN、および ERSPAN の注意事項および制約事項 53-8
VSPAN に関する注意事項および制約事項 53-9
RSPAN に関する注意事項および制約事項 53-10
ERSPAN に関する注意事項および制約事項 53-11
ローカル SPAN、RSPAN、および ERSPAN の設定 53-12
無条件トランクとしての宛先ポートの設定（任意） 53-12

宛先トランクの VLAN フィルタリングの設定（任意） 53-13
宛先ポートの許可リストの設定（任意） 53-15
ローカル SPAN の設定 53-15
ローカル SPAN の設定（SPAN コンフィギュレーション モード） 53-15
ローカル SPAN の設定（グローバル コンフィギュレーション モード） 53-18
RSPAN の設定 53-20
RSPAN VLAN の設定 53-20
RSPAN セッションの設定（SPAN コンフィギュレーション モード） 53-20
RSPAN セッションの設定（グローバル コンフィギュレーション モード） 53-23
ERSPAN の設定 53-26
ERSPAN 送信元セッションの設定 53-26
ERSPAN 宛先セッションの設定 53-28
ローカル SPAN および RSPAN の送信元 VLAN フィルタリングの設定 53-30
設定の確認 53-31
設定例 53-31
SPAN on EVC の設定 53-33
制約事項および使用上の注意事項 53-33
SPAN on EVC の設定 53-33
設定例 53-35
SPAN on EVC の確認 53-35
トラブルシューティング 53-36
分散型出力 SPAN 53-36
DES 機能の制約事項 53-36
分散型出力 SPAN の設定 53-36
設定例 53-37
設定の確認 53-37
トラブルシューティング 53-38

CHAPTER 54 **SNMP ifIndex パーシステンスの設定** 54-1
SNMP ifIndex パーシステンス 54-1
SNMP ifIndex パーシステンスの設定 54-2
SNMP ifIndex パーシステンスのグローバルなイネーブル化 54-2
SNMP ifIndex パーシステンスのグローバルなディセーブル化 54-2
特定のインターフェイス上における SNMP ifIndex パーシステンスのイネーブル化およびディセーブル化 54-2
特定のインターフェイスにおける SNMP ifIndex パーシステンス設定の消去 54-3

CHAPTER 55 **電源管理および環境モニタリング** 55-1
電源管理の機能概要 55-1

電源の冗長構成のイネーブル化およびディセーブル化 55-2
モジュールの電源切断および電源投入 55-3
システムの電力ステータスの確認 55-4
モジュールの電源オフ / オン 55-4
電源のオフ / オン 55-5
システムの所要電力の判別 55-5
システムのハードウェア容量の判別 55-5
センサーの温度しきい値の判別 55-9
環境モニタリングの機能概要 55-10
システム環境ステータスのモニタリング 55-10
LED 環境表示の概要 55-12

CHAPTER 56 **WCCP による Web キャッシュ サービスの設定 56-1**
WCCP の概要 56-2
WCCP の概要 56-2
ハードウェア アクセラレーション 56-3
WCCPv1 設定の概要 56-4
WCCPv2 設定の概要 56-5
WCCPv2 の機能 56-6
非 HTTP サービスのサポート 56-6
複数ルータのサポート 56-6
MD5 セキュリティ 56-7
Web キャッシュ パケットのリターン 56-7
負荷分散 56-7
WCCPv2 の制約事項 56-7
WCCP の設定 56-8
WCCP のバージョンの指定 56-8
WCCPv2 によるサービス グループの設定 56-9
Web キャッシュ サービスの指定 56-10
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 56-10
マルチキャスト アドレスへのルータの登録 56-10
WCCP サービス グループのアクセス リストの使用 56-11
ルータおよびキャッシュ エンジンのパスワードの設定 56-12
WCCP 設定の確認およびモニタリング 56-12
WCCP の設定例 56-12
ルータでの WCCP のバージョン変更例 56-13
一般的な WCCPv2 設定の実行例 56-13
Web キャッシュ サービスの実行例 56-13
逆プロキシ サービスの実行例 56-14

マルチキャスト アドレスへのルータの登録例 56-14
アクセス リストの使用例 56-14
ルータおよびキャッシュ エンジンのパスワード設定例 56-15
WCCP 設定の確認例 56-15
WCCP での VRF サポート 56-16
WCCP での VRF サポートの設定 56-16
手順の概要 56-17
手順の詳細 56-17
例 56-19
検証 56-19
トラブルシューティングのヒント 56-20

CHAPTER 57 **Top N ユーティリティの使用 57-1**
Top N ユーティリティの概要 57-1
Top N ユーティリティの概要 57-1
Top N ユーティリティ操作の概要 57-2
Top N ユーティリティの使用 57-2
Top N ユーティリティによるレポート作成のイネーブル化 57-2
Top N ユーティリティ レポートの表示 57-3
Top N ユーティリティ レポートの消去 57-4

CHAPTER 58 **スイッチ仮想インターフェイス上の双方向フォワーディングおよび検出の設定 58-1**
BFD over SVI の概要 58-1
制約事項および使用上の注意事項 58-1
BFD over SVI を使用したサンプル ネットワーク 58-2
ノード障害 58-3
リンク障害 58-3
BFD over SVI の設定 58-4

CHAPTER 59 **レイヤ 2 Traceroute ユーティリティの使用 59-1**
レイヤ 2 Traceroute ユーティリティの概要 59-1
使用上のガイドライン 59-1
レイヤ 2 Traceroute ユーティリティの使用 59-2

CHAPTER 60 **Call Home の設定 60-1**
Call Home の概要 60-1
Smart Call Home の取得 60-2
Call Home の設定 60-2

連絡先情報の設定 60-3
宛先プロファイルの設定 60-4
宛先プロファイルのコピー 60-6
アラート グループへの登録 60-6
定期的な通知の設定 60-8
メッセージ重大度しきい値の設定 60-8
Syslog パターンマッチの設定 60-9
一般的な E メール オプションの設定 60-9
Call Home のイネーブル化 60-11
Call Home の通信のテスト 60-11
Call Home テスト メッセージの手動送信 60-11
Call Home アラート グループ メッセージの手動送信 60-12
分析およびレポート要求の送信 60-12
Smart Call Home の設定とイネーブル化 60-13
Call Home 設定情報の表示 60-14
デフォルト設定値 60-18
アラート グループの起動イベントとコマンド 60-18
メッセージの内容 60-24
ロング テキスト形式での Syslog アラート通知の例 60-28
XML 形式での Syslog アラート通知の例 60-29

CHAPTER 61 **IPv6 ポリシーベース ルーティングの設定 61-1**
IPv6 ポリシーベース ルーティングの概要 61-1
ポリシー ベース ルーティング 61-2
パケット マッチング 61-2
set ステートメントを使用したパケット転送 61-2
IPv6 PBR の制限 61-3
IPv6 PBR の設定 61-4
検証 61-5
トラブルシューティングのヒント 61-10

CHAPTER 62 **Mini Protocol Analyzer の使用 62-1**
Mini Protocol Analyzer の機能概要 62-1
Mini Protocol Analyzer の設定 62-2
キャプチャ対象となるパケットのフィルタリング 62-3
キャプチャの開始および停止 62-4
キャプチャ バッファの表示およびエクスポート 62-6
Mini Protocol Analyzer の設定、操作、表示例 62-7

一般的な設定例 62-7
フィルタリング設定例 62-8
操作例 62-9
表示例 62-9
コンフィギュレーションの表示 62-9
キャプチャ セッション ステータスの表示 62-10
キャプチャ バッファの内容の表示 62-11

CHAPTER 63 Resilient Ethernet Protocol の設定 63-1
Resilient Ethernet Protocol の概要 63-1
REP 非ネイバー エッジ 63-2
Resilient Ethernet Protocol の設定 63-2

CHAPTER 64 同期イーサネットと 1588V2 の設定 64-1
同期イーサネットについて 64-1
スケルチング 64-2
SSM および ESMC 64-3
同期ステータス メッセージ 64-3
イーサネット同期メッセージング チャネル 64-3
制約事項および使用上の注意事項 64-4
Cisco 7600 ルータでの同期イーサネットの設定 64-5
SyncE からのクロック回復の設定 64-5
BITS ポートからのクロック回復の設定 64-7
外部へのシステムの設定 64-9
外部へのラインの設定 64-10
ES+ カードでの同期の管理 64-12
検証 64-14
同期イーサネット設定のトラブルシューティング 64-17
トラブルシューティング 64-19
ネットワーク クロッキング 64-22
ネットワーク クロッキングの設定方法 64-24
BITS クロック サポートの設定 64-24
使用上のガイドライン 64-24
例 64-25
クロック ソースとしての 10GE インターフェイスの設定 64-26
使用上のガイドライン 64-26
例 64-27
クロック ソースの検証 64-27
クロック ソースの回復 64-29

1588V2 について 64-29
Timing over Packet 64-29
1588V2 の基本的な動作 64-30
1588V2 でサポートされるモデル 64-30
サポートされるトランスポート モード 64-31
Time of Day（TOD） 64-32
1588V2 マスターの Time of Day 64-32
1588V2 スレーブの Time of Day 64-33
制限事項 64-33
1588V2 マスターでの ToD の設定 64-33
1588V2 マスターでの ToD 設定の検証 64-33
1588V2 スレーブでの ToD の設定 64-34
1588V2 スレーブでの ToD 設定の検証 64-34

CHAPTER 65 リンク ステート トラッキングの設定 65-1
リンク ステート トラッキングの機能概要 65-1
制約事項および使用上の注意事項 65-2
リンク ステート トラッキングの設定 65-2
リンク ステート トラッキングのトラブルシューティング 65-3

CHAPTER 66 IP および MPLS 向け BGP PIC エッジおよびコアの設定 66-1
IP および MPLS 向け BGP PIC エッジおよびコア 66-1
BGP PIC の前提条件 66-1
制約事項 66-2
IP および MPLS 向け BGP PIC の設定 66-2

CHAPTER 67 IPv4 トランスポートを介した VRF 対応 IPv6 トンネルの設定 67-1
VRF 対応 IPv6 トンネルの概要 67-1
VRF 対応 IPv6 トンネルの制約事項 67-2
VRF 対応 IPv6 トンネルの設定 67-2
IPv6 over IPv4 GRE トンネルの概要 67-3
IPv6 over IPv4 GRE トンネルの制約事項 67-3
IPv6 over IPv4 GRE トンネルの設定 67-4

CHAPTER 68 ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR） 68-1
ISISI LFA FRR の制約事項 68-1
Cisco 7600 シリーズ ルータでの IOS IPFRR サポートの設定 68-2
検証 68-2

CHAPTER 69 Y.1731 パフォーマンス モニタリング 69-1
Y.1731 パフォーマンス モニタリングの概要 69-1
接続 69-2
フレーム遅延とフレーム遅延変動 69-2
フレームの損失率および可用性 69-3
サポートされるインターフェイス 69-4
制約事項および使用上の注意事項 69-4
Y.1731 PM の設定 69-5

CHAPTER 70 マルチキャスト サービス リフレクション 70-1
マルチキャスト サービス リフレクションの機能アーキテクチャ 70-1
マルチキャスト サービス リフレクションの制約事項 70-2
マルチキャスト サービス リフレクションの設定 70-3

APPENDIX A オンライン診断テスト A-1
グローバル ヘルス モニタリング テスト A-1
TestSPRPInbandPing A-2
TestScratchRegister A-2
TestMacNotification A-3
ポート単位のテスト A-3
TestNonDisruptiveLoopback A-3
TestLoopback A-4
TestActiveToStandbyLoopback A-4
TestTransceiverIntegrity A-5
TestNetflowInlineRewrite A-5
PFC レイヤ 2 フォワーディング エンジン テスト A-6
TestNewIndexLearn A-6
TestDontConditionalLearn A-7
TestBadBpduTrap A-7
TestMatchCapture A-8
TestStaticEntry A-8
DFC レイヤ 2 フォワーディング エンジン テスト A-8
TestDontLearn A-9
TestNewLearn A-9
TestIndexLearn A-10
TestConditionalLearn A-10
TestTrap A-11
TestBadBpdu A-12
TestProtocolMatchChannel A-12

TestCapture A-13
TestStaticEntry A-13
PFC レイヤ 3 フォワーディング エンジン テスト A-14
TestFibDevices A-14
TestIPv4FibShortcut A-15
TestIPv6FibShortcut A-15
TestMPLSFibShortcut A-16
TestNATFibShortcut A-16
TestL3Capture2 A-17
TestAclPermit A-17
TestAclDeny A-18
TestNetflowShortcut A-18
TestQoS A-19
DFC レイヤ 3 フォワーディング エンジン テスト A-19
TestFibDevices A-20
TestIPv4FibShortcut A-20
TestIPv6FibShortcut A-21
TestMPLSFibShortcut A-21
TestNATFibShortcut A-22
TestL3Capture2 A-22
TestAclPermit A-23
TestAclDeny A-23
TestQoS A-24
TestNetflowShortcut A-24
レプリケーション エンジン テスト A-25
TestL3VlanMet A-25
TestIngressSpan A-25
TestEgressSpan A-26
ファブリック テスト A-26
TestFabricSnakeForward A-27
TestFabricSnakeBackward A-27
TestSynchedFabChannel A-28
TestFabricCh0Health A-28
TestFabricCh1Health A-29
完全メモリ テスト A-29
TestFibTcamSSRAM A-30
TestAsicMemory A-30
TestAclQosTcam A-30
TestNetflowTcam A-31

TestQoSTcam A-31
IPSEC サービス モジュール テスト A-32
TestIPSecClearPkt A-32
TestHapiEchoPkt A-33
TestIPSecEncryptDecryptPkt A-33
ストレス テスト A-33
TestTrafficStress A-34
TestEobcStressPing A-34
クリティカル リカバリ テスト A-34
TestL3HealthMonitoring A-35
TestTxPathMonitoring A-35
TestSynchedFabChannel A-36
一般的なテスト A-36
ScheduleSwitchover A-36
TestFirmwareDiagStatus A-37

APPENDIX B 略語 B-1

APPENDIX C Cisco IOS Release 15.S ソフトウェア イメージ C-1
非準拠プラットフォームのソフトウェア イメージ メッセージ C-2

INDEX

はじめに

ここでは、『*Cisco 7600 シリーズ ルータ 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 15S*』の対象読者、マニュアルの構成、および表記法について説明します。

対象読者

このマニュアルは、Cisco 7600 シリーズ ルータ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。

マニュアルの変更履歴

次の変更履歴表は、このマニュアルにおける技術的な変更内容を記録したものです。この表には、変更に対応する Cisco IOS ソフトウェアのリリース番号とマニュアルのリビジョン番号、変更した日付、および変更点を示します。

リリース番号	リビジョン	日付	変更点
15.0(1)S6	OL-10113-24-J	2012 年 6 月	**platform ipv4 pbr optimize tcam** コマンドに関して「IPv4 ルーティングおよびアドレスの設定」（P.22-3）を更新しました。
15.1(3)S3	OL-10113-23	2012 年 4 月	**platform ipv4 pbr optimize tcam** コマンドに関して「IPv4 ルーティングおよびアドレスの設定」（P.22-3）を更新しました。

リリース番号	リビジョン	日付	変更点
15.2(2)S	OL-10113-22	2012 年 3 月	次のサポートが追加されました。 • 第 67 章「IPv4 トランスポートを介した VRF 対応 IPv6 トンネルの設定」の IPv4 トランスポートを介した VRF 対応 IPv6 トンネル • 第 53 章「分散型出力 SPAN」の分散型出力 SPAN • 第 26 章「マルチキャスト隣接割り当て」のマルチキャスト隣接スケール • 第 70 章「マルチキャスト サービス リフレクション」のマルチキャスト サービス リフレクション
12.2(33)SRE6	OL-10113-21	2012 年 3 月	**platform ipv4 pbr optimize tcam** コマンドに関して「IPv4 ルーティングおよびアドレスの設定」（P.22-3）を更新しました。
15.2(1)S1	OL-10113-20	2012 年 2 月	**platform ipv4 pbr optimize tcam** コマンドに関して「IPv4 ルーティングおよびアドレスの設定」（P.22-3）を更新しました。
15.1(3)S2	OL-10113-19	2011 年 12 月	「インターフェイス単位の NetFlow と NDE の使用上の注意事項および制限事項」（P.52-12）に記載されているインターフェイス単位の NetFlow および QoS マイクロポリシングのサポート情報を更新しました。
15.2(1)S	OL-10113-18	2011 年 11 月	次のサポートが追加されました。 • 第 61 章「IPv6 ポリシーベース ルーティングの設定」の IPv6 ポリシー ベース ルーティング
15.1(3)S1	OL-10113-17	2011 年 10 月	次のサポートが更新されました。 • 第 66 章「IP および MPLS 向け BGP PIC エッジおよびコアの設定」

リリース番号	リビジョン	日付	変更点
15.1(3)S	OL-10113-16	2011 年 7 月	次のサポートが追加されました。 • 第 2 章「ルータの初期設定」の IPv6 ルート ヘルス インジェクション • 第 33 章「IPv4 マルチキャスト トラフィック用 IGMP スヌーピングの設定」のマルチキャスト VLAN レジストレーション • 第 19 章「L2TPv3 の設定」のレイヤ 2 トンネリング プロトコル バージョン 3 • 第 56 章「WCCP による Web キャッシュ サービスの設定」の WCCP での VRF サポート 次のサポートが更新されました。 • 第 68 章「ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR）」の ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR; ループ フリー代替高速再ルーティング）
15.0(1)S3a	OL-10113-15	2011 年 4 月	推奨レート リミッタ設定の項に追加された制限事項に関してサポートが拡張されました。
15.1(2)S	OL-10113-14	2011 年 3 月	次のサポートが追加されました。 • 第 53 章「ローカル SPAN、RSPAN、および ERSPAN の設定」の EVC サービス インスタンスでの SPAN • 第 66 章「IP および MPLS 向け BGP PIC エッジおよびコアの設定」の IP/MPLS 向け BGP IPv6 PIC エッジおよびコア • 第 68 章「ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR）」の ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR; ループ フリー代替高速再ルーティング） • 第 69 章「Y.1731 パフォーマンス モニタリング」の Y.1731 パフォーマンス モニタリング
15.1(1)S1	OL-10113-13	2011 年 2 月	推奨レート リミッタ設定の項に制限事項を追加しました。

リリース番号	リビジョン	日付	変更点
15.0(1)S2	OL-10113-12	2010 年 12 月	次のサポートが追加されました。 第 47 章「Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート」の Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート。
15.1(1)S	OL-10113-11	2010 年 11 月	次のサポートが追加されました。 • 第 47 章「Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート」の Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート。 • 第 58 章「スイッチ仮想インターフェイス上の双方向フォワーディングおよび検出の設定」の BFD over SVI の設定。 • リンク ステート トラッキングの設定の LST の設定。 • Resilient Ethernet Protocol の設定の REP 非ネイバー機能。 • ホット スタンバイ疑似回線。PFC のマルチプロトコル ラベル スイッチングの設定 のサポート。

リリース番号	リビジョン	日付	変更点
15.0(1)S	OL-10113-10	2010 年 7 月	次の機能のサポートが導入されました。 • 第 23 章「GTP-SLB IPV6 サポートの設定」の GTP-SLB IPV6 サポートの設定 • 第 28 章「マルチキャスト VPN エクストラネット サポートの設定」のマルチキャスト VPN エクストラネット サポートの設定 • 第 63 章「Resilient Ethernet Protocol の設定」の Resilient Ethernet Protocol の設定 • 第 64 章「同期イーサネットと 1588V2 の設定」の同期イーサネットの設定 • 第 43 章「トラフィック ストーム制御の設定」を更新しました。設定時の注意事項および制約事項を更新しました。
12.2(33)SRE1	OL-10113-09	2010 年 5 月	• 第 12 章の「Configuring LACP 1:1 Redundancy with Fast-Switchover」の項を更新し、第 14 章の「Configuring VLANs」にある表を更新しました。
12.2(33)SRE1	OL-10113-09	2010 年 4 月	• 第 52 章「NetFlow と NDE の設定」にプロトコル フロー フィルタの設定に関する使用上のガイドラインを追加しました。
12.2(33)SRE1	OL-10113-09	2010 年 4 月	• 第 38 章「Private Hosts の設定」の Private Host for VPLS に対するサポートと第 14 章「VLAN の設定」の自動保護サービス グループに対する Bridged Routing Encapsulation を拡張しました。
12.2(33)SRD4	OL-10113-08	2010 年 2 月	次の機能のサポートが導入されました。 • 第 38 章「Private Hosts の設定」の Private Host for VPLS • 第 14 章「VLAN の設定」の自動保護サービス グループに対する Bridged Routing Encapsulation • UDLD 設定に関する制約事項 • 新しいコマンドの **mls qos recirc untrust** を更新しました。

リリース番号	リビジョン	日付	変更点
12.2(33)SRE	OL-10113-07	2010 年 2 月	第 26 章「PFC のマルチプロトコル ラベル スイッチングの設定」にスケーラブル EoMPLS とポートモード EoMPLS に関する新しいセクションと対応するサンプル設定を追加しました。
12.2(33)SRE	OL-10113-07	2010 年 1 月	「SSO スーパーバイザ エンジンの冗長設定」の章の「NSF の利点および制約事項」の項を更新しました。
12.2(33)SRE	OL-10113-07	2009 年 12 月	「PFC QoS の設定」の章で priority-queue queue-limit interface コマンドを更新しました。
12.2(33)SRE	OL-10113-07	2009 年 11 月	次の機能のサポートが導入されました。 • Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）上での IPv4 マルチキャスト サポート • マルチキャスト MFIB Bi-Dir、MVPN、および P2P • ISSU - IPv4 マルチキャスト • ISSU for IP マルチキャスト
12.2(33)SRD2	OL-10113-06	2009 年 5 月	512k までの ARP スケールに対するサポートを追加。
12.2(33)SRD	OL-10113-05	2008 年 10 月	Mini Protocol Analyzer の使用に関する章を追加。
12.2(33)SRC	OL-10113-04	2007 年 12 月 31 日	次の機能のサポートが追加されました。 • DHCP での IEEE 802.1x • VTP v3 • ファスト スイッチオーバーでの LACP 1:1 冗長性 • スイッチド ポート アナライザ（SPAN）：学習機能をオフにするオプションの付いた入力パケット • SPAN 出力セッションの増加 • EtherChannel 上の SPAN 宛先ポートのサポート • Call Home

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	「製品概要」	Cisco 7600 シリーズ ルータの概要について説明します。
第 2 章	「ルータの初期設定」	ルータを初めて設定する方法について説明します。
第 3 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 4 章	「Route Switch Processor 720 の設定」	Route Switch Processor 720（RSP720）を設定する方法について説明します。
第 5 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の設定について説明します。
第 6 章	「Cisco 7600 シリーズ ルータでの ISSU および eFSU」	In Service Software Upgrade（ISSU）と enhanced Fast Software Upgrade（eFSU）プロセスについて説明します。ルータの実行中、Cisco IOS ソフトウェアをアップグレードできます。
第 7 章	「RPR および RPR+ スーパーバイザ エンジンの冗長設定」	RPR および 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 8 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 9 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 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（VLAN 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 の設定方法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	「VTP の設定」	VLAN トランキング プロトコル（VTP）を設定する手順について説明します。
第 14 章	「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 トンネリングの設定方法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 トンネリングの設定方法について説明します。
第 19 章	「L2TPv3 の設定」	L2TPv3 の設定方法について説明します。
第 20 章	「STP および MST の設定」	スパニングツリー プロトコル（STP）および準規格 IEEE 802.1s Multiple Spanning Tree（MST）の設定方法について説明します。

章	タイトル	説明
第 21 章	「オプションの STP 機能の設定」	オプションの STP 機能の設定方法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	「GTP-SLB IPV6 サポートの設定」	Cisco 7600 シリーズ ルータ上で GPRS Tunneling Protocol - Server Load Balancing（GTP-SLB;GPRS トンネリング プロトコル - サーバ ロード バランシング）IPV6 サポートを設定する方法について説明します。
第 24 章	「IP Subscriber Awareness over Ethernet」	Ethernet 機能を介して IP Subscriber Awareness を設定する方法について説明します。この機能では、ルータ上での IP セッションの終了と集約を実行できます。
第 25 章	「UDE および UDLR の設定」	Unidirectional Ethernet（UDE）および Unidirectional Link Routing（UDLR）の設定方法について説明します。
第 26 章	「PFC のマルチプロトコル ラベル スイッチングの設定」	PFC 上での Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）の設定方法について説明します。
第 27 章	「IPv4 マルチキャスト VPN 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）の設定方法について説明します。
第 28 章	「マルチキャスト VPN エクストラネット サポートの設定」	Cisco 7600 シリーズ ルータ上で 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）エクストラネット サポートを設定する方法について説明します。
第 29 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 スイッチングの設定方法について説明します。
第 30 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 31 章	「IPv4 マルチキャスト レイヤ 3 スイッチングの設定」	IPv4 MMLS を設定する手順について説明します。
第 32 章	「IPv6 マルチキャスト トラフィック用 MLDv2 スヌーピングの設定」	Multicast Listener Discovery version 2（MLDv2）スヌーピングの設定方法について説明します。
第 33 章	「IPv4 マルチキャスト トラフィック用 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 34 章	「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 35 章	「ネットワーク セキュリティの設定」	Cisco 7600 シリーズ ルータ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 36 章	「Cisco IOS ACL サポートの概要」	Cisco 7600 シリーズ ルータが Cisco IOS ACL をサポートする手順について説明します。

章	タイトル	説明
第 37 章	「VACL の設定」	VLAN ACL（VACL）を設定する手順について説明します。
第 38 章	「Private Hosts（PACL の使用）」	Private Hosts 機能を介してポート ベースの ACL を設定する方法について説明します。この機能では、同じ VLAN のホスト間でのレイヤ 2 の分離を行えます。
第 39 章	「オンライン診断の設定」	オンライン診断を設定し、診断テストを実行する方法について説明します。
第 40 章	「サービス拒絶保護の設定」	DoS 保護を設定する手順について説明します。
第 41 章	「DHCP スヌーピングの設定」	DHCP スヌーピングの設定方法について説明します。
第 42 章	「ダイナミック ARP インスペクションの設定」	Dynamic ARP Inspection（DAI）の設定方法について説明します。
第 43 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 44 章	「不明なユニキャスト フラッディングのブロック」	Unknown Unicast Flood Blocking（UUFB; 不明ユニキャスト フラッディング ブロッキング）の設定方法について説明します。
第 45 章	「PFC QoS の設定」	Quality of Service（QoS）を設定する手順について説明します。
第 46 章	「PFC QoS 統計データ エクスポートの設定」	PFC QoS 統計データ エクスポートの設定方法について説明します。
第 47 章	「Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート」	既存の IPv4 MPLS バックボーン ネットワークを IPv4 マルチキャスト サービス用に拡張します。
第 48 章	「PFC の MPLS QoS の設定」	MPLS QoS の設定方法について説明します。
第 49 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 50 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 51 章	「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 52 章	「NetFlow および NDE の設定」	NetFlow 統計収集および NetFlow Data Export（NDE; NetFlow データ エクスポート）の設定方法について説明します。
第 53 章	「ローカル SPAN、RSPAN、および ERSPAN の設定」	スイッチド ポート アナライザ（SPAN）を設定する手順について説明します。
第 54 章	「SNMP ifIndex パーシステンスの設定」	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 55 章	「電源管理および環境モニタリング」	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。

章	タイトル	説明
第 56 章	「WCCP による Web キャッシュ サービスの設定」	Web Cache Communication Protocol（WCCP）の設定方法について説明します。
第 57 章	「Top N ユーティリティの使用」	Top N ユーティリティの使用方法について説明します。
第 59 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。
第 60 章	「Call Home の設定」	Call Home 機能を設定する方法について説明します。
第 61 章	「IPv6 ポリシーベース ルーティングの設定」	IPv6 ポリシー ベース ルーティング（PBR）を設定する方法について説明します。
第 62 章	「Mini Protocol Analyzer の使用」	Mini Protocol Analyzer を設定する方法について説明します。
第 63 章	「Resilient Ethernet Protocol の設定」	Cisco 7600 シリーズ ルータ上で Resilient Ethernet Protocol を設定する方法について説明します。
第 64 章	「同期イーサネットと 1588V2 の設定」	Cisco 7600 シリーズ ルータ上で同期イーサネットを設定する方法について説明します。
第 65 章	「リンク ステート トラッキングの設定」	Cisco 7600 シリーズ ルータ上でリンク ステート トラッキングを設定する方法について説明します。
第 66 章	「IP および MPLS 向け BGP PIC エッジおよびコアの設定」	Cisco 7600 シリーズ ルータ上で IP および MPLS 向け Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）PIC エッジおよびコアを設定する方法について説明します。
第 67 章	「IPv4 トランスポートを介した VRF 対応 IPv6 トンネルの設定」	IPv4 トランスポートを介した VRF 対応 IPv6 トンネルを設定する方法について説明します。
第 68 章	「ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR）」	Cisco 7600 シリーズ ルータ上で ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR; ループ フリー代替高速再ルーティング）を設定する方法について説明します。
第 69 章	「Y.1731 パフォーマンス モニタリング」	Cisco 7600 シリーズ ルータ上で Y.1731 パフォーマンス モニタリングを設定する方法について説明します。
第 70 章	マルチキャスト サービス リフレクション	マルチキャスト サービス リフレクション機能およびその設定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の推奨事項を提供します。
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。
付録 C	「Cisco IOS Release 15.S ソフトウェア イメージ」	Cisco IOS Release 12.2SRB に付属のソフトウェア イメージを一覧表示しています。

関連資料

Cisco 7600 シリーズ ルータの関連資料は、次のとおりです。

- 『*Cisco 7600 Series Router Installation Guide*』

- 『*Cisco 7600 Series Router Module Installation Guide*』
- 『*Cisco 7600 Series Router Cisco IOS Command Reference*』
- 『*Cisco 7600 Series Router Cisco IOS System Message Guide*』
- 『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』
- 『*Cisco IOS Configuration Guides and Command References*』: Cisco 7600 シリーズ ルータのマニュアルで扱っていない Cisco IOS ソフトウェア機能を設定する場合には、次の資料を参照してください。
  - 『*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
- 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。
string	引用符を付けない一組の文字。string 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 string 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、山カッコ（<>）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

CHAPTER 1

製品概要

この章で説明する内容は、次のとおりです。

- 「サポート対象ハードウェアおよびソフトウェア」（P.1-1）
- 「ユーザ インターフェイス」（P.1-1）
- 「組み込み CiscoView サポートの設定」（P.1-2）
- 「PFC および DFC がハードウェアでサポートするソフトウェア機能」（P.1-3）

サポート対象ハードウェアおよびソフトウェア

Cisco 7600 シリーズ ルータによってサポートされるシャーシ、モジュール、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。

このリリースで使用できる Cisco IOS ソフトウェア イメージの詳細については、付録 C「Cisco IOS Release 15.S ソフトウェア イメージ」を参照してください。

（注） Cisco IOS Release 12.2SR 以降のリリースの場合、Supervisor Engine 2、Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）、FlexWAN モジュールは、Cisco 7600 シリーズ ルータでサポートされません。

ユーザ インターフェイス

Release 12.2SR では、次のインターフェイスを使用する設定がサポートされます。

- CLI：次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』の「Using the Command-Line Interface」を参照してください。

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- SNMP：次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』および『*Cisco IOS Command Reference*』を参照してください。

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- 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/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- 組み込み CiscoView：「組み込み CiscoView サポートの設定」（P.1-2）を参照してください。

組み込み CiscoView サポートの設定

ここでは、組み込み CiscoView サポートの設定について説明します。

- 「組み込み CiscoView の概要」（P.1-2）
- 「組み込み CiscoView のインストールおよび設定」（P.1-2）
- 「組み込み CiscoView 情報の表示」（P.1-3）

組み込み CiscoView の概要

組み込み CiscoView ネットワーク管理システムは、Web ベースのインターフェイスです。HTTP および SNMP を使用してルータをグラフィック表示し、GUI ベースの管理および設定インターフェイスを提供します。組み込み CiscoView の Java Archive（JAR）ファイルは、次の URL からダウンロードできます。

http://www.cisco.com/cisco/software/navigator.html

組み込み CiscoView のインストールおよび設定

組み込み CiscoView のインストールおよび設定を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **dir** *device_name*	デバイスの内容を表示します。 組み込み CiscoView を初めて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には、ステップ 4 に進んでください。
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 システムのスペースを回復します。
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*:	デバイスの内容を表示します。 冗長構成の場合は、冗長スーパーバイザ エンジンのファイル システムについてステップ 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。

	コマンド	目的
ステップ 8	`Router(config)# snmp-server community string ro`	読み取り専用動作の 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 / 書き込み用動作の SNMP パスワードを設定します。

（注）　ルータ Web ページにアクセスするためのデフォルトのパスワードは、ルータのイネーブルレベル パスワードです。

ルータへの Web アクセスの詳細については、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/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt1/fcf005.htm

組み込み CiscoView 情報の表示

組み込み 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`	組み込み CiscoView ファイルに関する情報を表示します。
`Router# show ciscoview version`	組み込み CiscoView のバージョンを表示します。

PFC および DFC がハードウェアでサポートす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）、Distributed Forwarding Card 3（DFC3; 分散型フォワーディング カード 3）、および Distributed Forwarding Card（DFC; 分散型フォワーディング カード）が提供するハードウェア サポートについて説明します。

- 「PFC3、DFC3、および DFC がハードウェアでサポートするソフトウェア機能」（P.1-3）
- 「PFC3 および DFC3 がハードウェアでサポートするソフトウェア機能」（P.1-4）

PFC3、DFC3、および DFC がハードウェアでサポートするソフトウェア機能

PFC3、DFC3、および DFC では、次に示す Cisco IOS ソフトウェア機能がハードウェアでサポートされます。

- レイヤ 3 ポートおよび VLAN インターフェイスのアクセス コントロール リスト（ACL）
  - 入 / 出力標準 ACL および拡張 ACL の許可アクションおよび拒否アクション

    （注）　ACL ロギングが必要なフローは、MSFC 上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が MSFC 上のソフトウェアで処理されたあとの再帰 ACL フロー
  - ダイナミック ACL フロー

（注）　MSFC 上のソフトウェアで処理されるアイドル タイムアウト

ACL の PFC および DFC サポートの詳細については、第 36 章「Cisco IOS ACL サポートの概要」を参照してください。ACL の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/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

- VLAN ACL（VACL）：VACL を設定するには、第 37 章「VACL の設定」を参照してください。
- **match ip address**、**set ip next-hop**、および **ip default next-hop** Policy-Base 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」および「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

（注）　MSFC3 アドレスまたは MSFC4 アドレスが PBR ACL の範囲内にある場合、MSFC にアドレス指定されたトラフィックは MSFC に転送されないで、ハードウェアでポリシー ルーティングされます。MSFC3 または MSFC4 にアドレス指定されたトラフィックのポリシー ルーティングを禁止するには、その 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。

- MPLS インターフェイスを除く 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.35-2）を参照してください。
- ハードウェアが処理する NetFlow 集約：次の URL を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nde.html

PFC3 および DFC3 がハードウェアでサポートするソフトウェア機能

PFC3 および DFC3 では、次に示す Cisco IOS ソフトウェア機能がハードウェアでサポートされます。

- ポイントツーポイント Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル上の IPv4 マルチキャスト：次の URL のマニュアルを参照してください。

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

- 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.31-7）を参照してください。
- 複数パスによるユニキャスト Reverse Path Forwarding（RPF; リバース パス転送）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.35-2）を参照してください。
- MPLS インターフェイスを除く、IPv4 ユニキャストおよびマルチキャスト トラフィックのネットワーク アドレス変換（NAT）

  ハードウェアが処理する NAT については、次の点に注意してください。

  - UDP トラフィックの NAT は、PFC3A モードではサポートされません。
  - 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た NAT をサポートしません。
- インターフェイスで NAT および NDE が設定されている場合、PFC3 はすべてのトラフィックを分割パケットに格納して MSFC3 または MSFC4 に送信し、そこでソフトウェア処理します（CSCdz51590）。

NAT を設定するには、次の URL にある『*Cisco IOS IP Configuration Guide*, Release 12.2』の「IP Addressing and Services」、「Configuring IP Addressing」、および「Configuring Network Address Translation」を参照してください。

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

DoS 攻撃や設定ミスが原因で大量の NAT トラフィックが MSFC3 に送信されることがないようにするには、**mls rate-limit unicast acl** {**ingress** | **egress**} コマンドを入力します（次の URL を参照）。

http://www.cisco.com/en/US/products/hw/switches/ps700/prod_command_reference_list.html

- PFC3 および DFC3 では、ポイントツーポイント GRE トンネル上の IPv4 マルチキャストがハードウェアでサポートされます。
- GRE トンネリングおよび IP-in-IP トンネリング：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 および MSFC4 では、その他の **tunnel** コマンドで設定したトンネリングがサポートされます。

tunnel ttl コマンド（デフォルトは 255）は、カプセル化パケットの TTL を設定します。

tunnel tos コマンドでは、パケットがカプセル化される際にパケットの ToS バイトを設定します。**tunnel tos** コマンドが存在せず、QoS がイネーブルでない場合、パケットがカプセル化される際にパケットの ToS バイトには、元のパケットの ToS バイトが設定されます。**tunnel tos** コマンドが存在せず、QoS がイネーブルである場合、パケットがカプセル化される際にパケットの ToS バイトには、PFC QoS によって変更されたパケットの ToS バイトが設定されます。

GRE トンネリングおよび IP-in-IP トンネリングを設定するには、次の資料を参照してください。

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

http://www.cisco.com/en/US/docs/ios/12_2/interface/command/reference/irfshoip.html

tunnel tos コマンドおよび **tunnel ttl** コマンドを設定するには、次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

トンネルについては、次の点に注意してください。

- ハードウェアが処理する各トンネルには固有の送信元が必要です。ハードウェアが処理するトンネルは宛先が異なる場合でも送信元を共有できません。ループバック インターフェイス上のセカンダリ 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 固有の送信元アドレスを使用できないと、ソフトウェア パスの輻輳中にコントロール プレーンに失敗する場合があります。
- 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 アドレスごとに追加ルータ MAC アドレス エントリを 1 つ使用します。
- PFC3A はトンネル インターフェイスの PFC QoS 機能をサポートしません。その他の PFC はすべてサポートします。
- MSFC3 および MSFC4 は、トンネル インターフェイスに出力機能が設定されたトンネルをサポートします。出力機能の例は、出力 Cisco IOS ACL、NAT（内部から外部への変換の場合）、TCP インターセプト、CBAC、暗号化などです。

CHAPTER 2

ルータの初期設定

この章では、Cisco 7600 シリーズ ルータの初期設定方法について説明します。この章の情報により、次のマニュアルの管理に関する情報および手順が補完されます。

- 次の URL の『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html
- 次の URL の『*Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

（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、次の資料を参照してください。

- 次の URL の『*Cisco 7600 Series Router Cisco IOS Command Reference*』
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「デフォルト設定」（P.2-1）
- 「ルータ の設定」（P.2-2）
- 「特権 EXEC コマンドへのアクセスの保護」（P.2-8）
- 「イネーブル パスワードを忘れた場合の回復方法」（P.2-13）
- 「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」（P.2-13）

デフォルト設定

表 2-1 に、デフォルト設定を示します。

表 2-1　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>`

ルータ の設定

ここでは、ルータ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.2-2）
- 「コンフィギュレーション モードの使用」（P.2-3）
- 「実行コンフィギュレーションを保存する前の確認」（P.2-4）
- 「実行コンフィギュレーションの保存」（P.2-5）
- 「設定の確認」（P.2-5）
- 「スタティック ルートの設定」（P.2-5）
- 「スタティック ルートの設定」（P.2-5）
- 「BOOTP サーバの設定」（P.2-6）

セットアップ機能または setup コマンドの使用

ルータ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。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呼び出すこともできます。

セットアップ機能ではシステム設定ダイアログが提供されます。これは対話型 CLI モードであり、これによって手順を追ってルータの初期設定を実行できるようになります。このダイアログでは、ネットワークにおけるルータの機能を開始するために必要な情報を要求されます。

システム設定ダイアログでは、グローバル パラメータの設定を最初に要求されます。このパラメータは、システム全体の設定を制御するために使用されます。このダイアログでは、次にインターフェイスを設定するための情報を要求されます。変更する項目に達するまで、システム設定ダイアログを進める必要があります。

このダイアログを進めるとき、各プロンプトの横に表示される角カッコには、その項目のデフォルト設定、または前回の設定値が表示されます。項目のデフォルト値を受け入れるには、Return または Enter を押します。その項目の値を変更するには、目的の値を入力します。

プロンプトのヘルプを表示するには、プロンプトに疑問符（**?**）を入力します。

変更が完了すると、セットアップ セッション中に作成されたコンフィギュレーション ファイルが自動的に表示されます。ダイアログにより、この設定を使用するかどうかを質問されます。Yes で答えると、設定がスタートアップ コンフィギュレーション ファイルとして NVRAM に保存されます。No で答えると、設定は保存されずにプロセスが再開されます。

セットアップを終了し、変更せずに、またダイアログ全体を進めずに特権 EXEC モードに戻るには、Ctrl+C を押します。

設定プロセスを完了したら、インターフェイスを限定的に使用できます。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。

（注） ルータの現在の状態を確認するには、**show version** コマンドを使用します。

インターフェイスの詳しい設定手順については、次の URL の『*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 モードからルータを設定できます。

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。

プロンプトが特権 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.2-5）を参照）。

これで最小限のルータ設定が行われ、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確認するには、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、特権 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、特権 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
```

このコマンドを使用すると、コンフィギュレーション モードで入力した設定値が保存されます。この手順を実行しない場合、システムを次回リロードするときに設定が失われます。

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。

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ルータ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生じる場合があります。

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、ルータ上で **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、ルータ上で **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、サブネット マスクと接続されている VLAN 1 を使用します。

```
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 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。ルータは起動時に、BOOTP サーバから IP アドレスを自動的に取得します。

ルータが 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、ルータまたは **erase** コマンドを使用して startup-config ファイルを削除したルータのデフォルトの IP アドレスです）。

ルータが 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、最初にルータの 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、各ルータ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 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>
```

Cisco 7600 でのルート ヘルス インジェクション

Route Health Injection（RHI; ルート ヘルス インジェクション）を使用すると、Cisco Application Control Engine（ACE）からイントラネット全体に、ホスト ルートとしての Virtual IP（VIP; 仮想 IP）アドレスの可用性をアドバタイズできます。ACE は、受信した RHI 情報に従って定期的に VIP の可用性を伝播する Cisco 7600 シリーズ ルータのマルチレイヤ スイッチ フィーチャ カード（MSFC）に RHI 情報を送信します。MSFC はインターネットにホストルートの可用性をブロードキャストしないため、RHI は通常イントラネットに制限されます。

VIP が使用不可になると、ACE は RHI 情報を取り消します。MSFC は、ACE から受信した各 VIP アドレスのエントリをルーティング テーブルに追加します。MSFC で実行中のルーティング プロトコルは、VIP アドレスの各インスタンスの可用性やホップカウント ルーティング情報などのルーティング テーブルの更新を、他のルータに送信します。クライアント ルータは、ルーティング情報を使用し、VIP アドレスへの最適な使用可能パスに基づいてルートを選択します。また、Cisco アプリケーション スイッチがクライアント システムに論理的に近くなるルートも選択します。

デフォルトでは、ACE は RHI 用に VIP インターフェイスの VLAN をアドバタイズします。VIP インターフェイスの VLAN とは異なる VLAN を Route Health Injection（RHI; ルート ヘルス インジェクション）用にアドバタイズするには、インターフェイス コンフィギュレーション モードで **ip route inject vlan** を使用します。デフォルトでは、ACE は RHI 用に VIP インターフェイスの VLAN をアドバタイズします。

Cisco IOS Release 15.1(3)S、Cisco 7600 ルータでは、IPv6 スタティック ルートの挿入がサポートされます。

設定の詳細および例については、次のガイドを参照してください。

次の URL にある『*Routing and Bridging Guide vA2(1.0), Cisco ACE Application Control Engine Module*』
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/rtg_brdg/guide/rtbrgdgd.html

次の URL にある『*Getting Started Guide, Cisco ACE Application Control Engine Module*』

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/getting/started/guide/ace_module_gsg.html

特権 EXEC コマンドへのアクセスの保護

ここでは、システム コンフィギュレーション ファイルおよび特権 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」（P.2-8）
- 「enable password コマンドおよび enable secret コマンドの使用」（P.2-9）
- 「回線パスワードの設定または変更」（P.2-9）
- 「特権 EXEC モードに対する TACACS+ パスワード保護の設定」（P.2-10）
- 「パスワードの暗号化」（P.2-11）
- 「複数の特権レベルの設定」（P.2-11）

スタティック イネーブル パスワードの設定または変更

特権 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*	特権 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、特権 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、および特権レベルの設定の表示」（P.2-12）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 TFTP 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）または指定された特権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することはできません。

ルータがイネーブル 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}`	特権 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、特定の特権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、このレベルにアクセスする必要のあるユーザにのみパスワードを提供してください。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 Cisco 7600 シリーズ ルータ 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、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.2-13）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、および特権レベルの設定の表示」（P.2-12）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*	特権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、および特権レベルの設定の表示」（P.2-12）を参照してください。

特権 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、次の資料を参照してください。

- 次の URL の『*Cisco IOS Security Configuration Guide*, Release 12.2』の「Authentication, Authorization, and Accounting（AAA）」

  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

- 次の URL の『*Cisco IOS Security Command Reference*』Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

TACACS+ プロトコルを設定してユーザが特権 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**	特権 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。

特権 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、特権 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特権 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。この問題は、**enable** コマンドの入力によりクエリーが生成された場合と、拡張 TACACS を使用しないでログインしようとした場合を、ルータが区別できないために発生します。

（注）　AAA サーバへの接続、またはトラフィックおよび認証関連機能のためにスタンバイ スーパーバイザ ポートを使用しないでください。スタンバイ スーパーバイザ ポートが使用されている場合、リロード後 5 分間はルータがアクセス不可になる場合があります。

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らないようにすることができます。

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、特権コマンド 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、およびボーダー ゲートウェイ プロトコル（BGP）ネイバー 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、未認可ユーザによるコンフィギュレーション ファイルのパスワードの表示を防ぐことができます。

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、ルータ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.2-13）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、および特権レベルの設定の表示」（P.2-12）を参照してください。

複数の特権レベルの設定

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 モードおよび特権 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。

- 「コマンドの特権レベルの設定」（P.2-12）
- 「回線のデフォルト特権レベルの変更」（P.2-12）
- 「特権レベルへのログイン」（P.2-12）
- 「特権レベルの終了」（P.2-12）
- 「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.2-12）

コマンドの特権レベルの設定

コマンドの特権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*	コマンドの特権レベルを設定します。
ステップ 2	Router(config)# **enable password level** *level* [*encryption-type*] *password*	特権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、および特権レベルの設定の表示」（P.2-12）を参照してください。

回線のデフォルト特権レベルの変更

特定の回線または回線グループのデフォルト特権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*	回線のデフォルト特権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、および特権レベルの設定の表示」（P.2-12）を参照してください。

特権レベルへのログイン

特定の特権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*	指定された特権レベルにログインします。

特権レベルの終了

特定の特権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*	指定した特権レベルを終了します。

パスワード、アクセス レベル、および特権レベルの設定の表示

パスワード、アクセス レベル、および特権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**	特権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、特権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　ルータ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　システムをリブートします。

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、設定を消去します。

ステップ 6　ルータが通常どおり 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　システムをリブートします。

（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」（P.2-14）
- 「ソフトウェア コンフィギュレーション レジスタの設定」（P.2-15）
- 「スタートアップ システム イメージの指定」（P.2-18）
- 「フラッシュ メモリの概要」（P.2-18）
- 「CONFIG_FILE 環境変数」（P.2-19）
- 「環境変数の制御」（P.2-20）

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 エンジンのブート プロセスには、ROM モニタとスーパーバイザ エンジン ソフトウェアの 2 つのソフトウェア イメージが関与します。ルータ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、ルータ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.2-16）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.2-18）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。ルータで ROM モニタ モードが開始されるのは、ルータ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 7600 Series Router Cisco IOS Command Reference*』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
- 起動機能（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

ルータは 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
- Break 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 2-2 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 2-3 に、ブート フィールドの定義を示します。

注意　推奨コンフィギュレーション レジスタ設定は 0x2102（出荷時のデフォルト値）です。Break をイネーブルのままにし、コンソール接続を介してブレーク シーケンスを送信するように設定した場合、ルータは ROMMON になります。

表 2-2　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	16 進数	意味
00 ～ 03	0x0000 ～ 0x000F	ブート フィールド（表 2-3 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[1] 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. OEM = Original Equipment Manufacturer

表 2-3　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 bootsystem 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、ルータが 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 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、ルータはスタートアップ 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`	ルータのシステム イメージ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。

ルータ上で Cisco IOS ソフトウェアが動作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、特権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（#）で次のように **configure** terminal コマンドを入力します。

```
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。ここで、*value* は、先頭が 0x の 16 進数です（表 2-2（P.2-15）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.2-5）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　システムをリブートします。

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、ルータが OS 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、ルータはスタートアップ 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:** デバイスです（Route Switch Processor 720 および Supervisor Engine 720 だけに、**disk1:** があります）。
- システム ソフトウェア イメージは **bootflash:** デバイスに保存しないでください。イメージは MSFC 上にあるので起動時に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*』の「Loading and Maintaining System Images」の章の「Specifying the Startup System Image in the Configuration File」の項にも説明があります。

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.2-19）
- 「セキュリティ機能」（P.2-19）
- 「フラッシュ メモリの設定プロセス」（P.2-19）

（注） ここでは、ブートフラッシュ デバイス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、コンソール端末の特権 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

ルータがフラッシュ 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/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

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.2-16）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 の『*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、ルータ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、ルータは NVRAM コンフィギュレーションを初期化に使用します。ルータで NVRAM に伴う問題またはチェックサム エラーが検出された場合は、ルータが **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.2-2）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 環境変数および CONFIG_FILE 環境変数の作成または修正を行うには、**boot system** および **boot config** グローバル 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*』の「Loading and Maintaining System Images」の章の「Specifying the Startup System Image in the Configuration File」の項を参照してください。CONFIG_FILE 環境変数の詳しい設定手順については、『*Configuration Fundamentals Configuration Guide*』の「Managing Configuration Files」の章の「Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems」の項を参照してください。

（注）　**boot system** および **boot config** 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場合、実行コンフィギュレーションだけが影響されます。環境変数の情報を 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、環境変数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 および CONFIG_FILE 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、BOOT および CONFIG_FILE 環境変数を確認する例を示します。

```
Router# show bootvar
BOOT variable = disk0:c6sup22-jsv-mz.121-5c.EX.bin,1;
CONFIG_FILE variable does not exist
Configuration register is 0x2
Router#
```

CONFIG_FILE 環境変数によって指定されるコンフィギュレーション ファイルの内容を表示するには、**more nvram:startup-config** コマンドを使用します。

CHAPTER 3

Supervisor Engine 720 の設定

この章では、Cisco 7600 シリーズ ルータに搭載された Supervisor Engine720 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。

- 「Supervisor Engine 720 におけるブートフラッシュまたはブートディスクの使用」（P.3-1）
- 「Supervisor Engine 720 でのスロットの使用」（P.3-2）
- 「Supervisor Engine 720 ポートの設定」（P.3-2）
- 「スイッチ ファブリック機能の設定とモニタリング」（P.3-2）

（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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- 3 スロットのシャーシの場合、Supervisor Engine 720 はスロット 1 またはスロット 2 のいずれかに搭載します。
- 6 スロットまたは 9 スロットのシャーシの場合、Supervisor Engine 720 はスロット 5 またはスロット 6 のいずれかに搭載します。
- 13 スロットのシャーシの場合、Supervisor Engine 720 はスロット 7 またはスロット 8 のいずれかに搭載します。

Supervisor Engine 720 におけるブートフラッシュまたはブートディスクの使用

Release 12.2SR では、Supervisor Engine 720 64 MB ブートフラッシュ デバイス（**sup-bootflash:**）がサポートされます。
Release 12.2(18)SXE5 とリビルド、および Release 12.2(18)SXF で使用可能な WS-CF-UPG= の使用方法については、次の資料を参照してください。

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

（注）
Release 12.2SRB およびそれ以降を実行するには、すべての Sup720 モジュールでは、最小で 128 MB ブートフラッシュが必要です。512 MB のブートフラッシュが搭載された CompactFlash（CF）アダプタは、Release 12.2(18)SXF およびそれ以降のリリースの Sup720 モジュールで使用できます。注文の場合は、Cisco Part Number CF-ADAPTER= を使用してください。

Supervisor Engine 720 でのスロットの使用

Supervisor Engine 720 には Type II のコンパクト フラッシュ スロットが 2 つあります。CompactFlash Type II スロットでは、シスコが販売する CompactFlash Type II Flash PC カードがサポートされます。アクティブな Supervisor Engine 720 のスロットのキーワードは、**disk0:** および **disk1:** です。冗長 Supervisor Engine 720 のスロットに対応するキーワードは、**slavedisk0:** および **slavedisk1:** です。

Supervisor Engine 720 ポートの設定

Supervisor Engine 720 のポート 1 には、Small Form-Factor Pluggable（SFP）コネクタが 1 つ装備されています（ほかに特別な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）が装備されています。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 が RJ-45 コネクタまたは SFP コネクタのいずれか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 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、RJ-45 コネクタを使用するように、スロット 5 に搭載された Supervisor Engine 720 のポート 2 を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とモニタリング

ここでは、スイッチング モードの設定手順、および Supervisor Engine 720 に組み込まれたスイッチ ファブリック機能のモニタ手順について説明します。

- 「スイッチ ファブリック機能の機能概要」（P.3-2）
- 「スイッチ ファブリック機能の設定」（P.3-4）
- 「スイッチ ファブリック機能のモニタ」（P.3-5）

スイッチ ファブリック機能の機能概要

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

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 に内蔵された機能です。ファブリック対応モジュール間の専用接続を作成し、これらのモジュール間で連続的なフレーム伝送を行います。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

PFC3 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 を搭載していないモジュールを介してルータに着信する各パケットの転送先をすべて決定します。
- DFC3 は、次の場合に、DFC3 対応モジュールを介してルータに着信する各パケットの転送先をすべて決定します。
  - 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 Engine720 に送信します。Supervisor Engine 720 のファブリック インターフェイスが 32 Gbps スイッチング バスにパケットを転送し、パケットは出力モジュールで受信されたあと、出力ポートから送信されます。

スイッチング モード

Supervisor Engine 720 が搭載されている場合、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：ルータに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は、すべてのトラフィックに対してこのモードが使用されます。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：ルータに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が両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して、このモードが使用されます。このモードでは、ルータはスイッチ 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（フレームの最初の 64 バイト）を送信します。
- bus モード：ルータは、ファブリック非対応モジュール間のトラフィックや、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対して、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 3-1 に、搭載されているファブリック対応モジュール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 3-1　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 モードの使用を防止するには、**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、ルータ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 モードのしきい値に戻すには、**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」（P.3-5）
- 「ファブリック チャネルのスイッチング モードの表示」（P.3-5）
- 「ファブリック ステータスの表示」（P.3-6）
- 「ファブリック使用率の表示」（P.3-6）
- 「ファブリック エラーの表示」（P.3-6）

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、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
%Truncated mode is allowed
%System is allowed to operate in legacy mode

Module Slot     Switching Mode     Bus Mode
    5                     DCEF     Compact
    9                 Crossbar     Compact
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#
```

ファブリック使用率の表示

特定のモジュールまたは全モジュールのファブリック使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**]	ファブリック使用率を表示します。

次に、全モジュールのファブリック使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 4

Route Switch Processor 720 の設定

この章では、Route Switch Processor 720（RSP720）を設定する手順について説明します。RSP720 は、Cisco 7600 シリーズ ルータで使用可能な最新タイプのスーパーバイザ エンジンです。RSP720 は、1 枚のフルサイズ ボードと 2 枚の統合ドーター カードで構成されており、そのボードやカードとは、MSFC4 と、PFC3C または PFC3CXL です。RSP720 には、Cisco 7600 のすべてのラインカードを、ポイントツーポイント 20 Gbps 全二重シリアル チャネルで接続する、統合スイッチ ファブリックがあります。

RSP720、Sup720、Sup32 で使用可能な Cisco IOS ソフトウェア イメージの詳細については、付録 C「Cisco IOS Release 15.S ソフトウェア イメージ」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。

- 「RSP720 PFC の互換性のマトリクス」（P.4-1）
- 「RSP720 の機能」（P.4-2）
- 「RSP720 でのフラッシュ メモリのアクセス」（P.4-6）
- 「ルート スイッチ プロセッサ 720 ポートの設定」（P.4-6）
- 「スイッチ ファブリック機能の設定とモニタリング」（P.4-7）

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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

（注）

- RSP720 は、Cisco 7603 および Cisco OSR-7609 を除くすべての Cisco 7600 シャーシでサポートされます。
- 4 スロットのシャーシの場合、RSP720 はスロット 1 またはスロット 2 に搭載します。
- 6 スロットまたは 9 スロットのシャーシの場合（拡張（-S）シャーシを含む）、RSP720 はスロット 5 またはスロット 6 に搭載します。
- 13 スロットのシャーシの場合、RSP720 はスロット 7 またはスロット 8 に搭載します。

RSP720 PFC の互換性のマトリクス

ルート スイッチ プロセッサ 720（RSP720）は、PFC3C または PFC3CXL の 2 つのタイプのポリシー フィーチャ カードで構成されます。RSP720 の PFC は、バージョン 3B の Distributed Forwarding Card（DFC; 分散型フォワーディング カード）である DFC3B などの、より低いバージョンのカードとともに動作します。カード バージョン番号は、3B、3BXL、3C、3CXL など、動作モードを示します。

RSP720 をより低いバージョンのカードと動作させる場合、システムでは、すべてのインストール済みカードの最も低い動作モード（3B、3BXL、3C、3CXL）を特定し、このモードがすべてのカードに適用されます。カードにより、（カードがより高いバージョン番号の場合でも）選択された動作モードでサポートされる機能が提供されます。たとえば、3B モードの PFC3C の動作では、PFC3B によってサポートされるこれらの機能だけが提供されます。

異なるバージョン カードでのモード設定の例を、次に示します。

- RSP720-3CXL、DFC3BXL、イーサネット サービス モジュール（ES20-3C）を搭載しているシステムは、3BXL モード（すべてのカードで最も低いバージョンの動作モード）で動作します。
- RSP720-3CXL と ES20-3C を搭載しているシステムは、3C モードで動作します。
- RSP720-3C と DFC3B を搭載しているシステムは、3B モードで動作します。
- RSP720-3CXL と ES20-3CXL を搭載しているシステムは、3CXL モードで動作します。

（注）　**show platform hardware pfc mode** コマンドを使用すると、PFC の動作モードが表示されます。

RSP720 の機能

RSP720 は、Cisco 7600 シリーズ ルータの最新タイプのスーパーバイザ エンジンです。2 枚の統合ドーター カード（PFC3C または PFC3CXL と、MSFC4）が搭載された RSP720 では、前のスーパーバイザ エンジンに対して多くの拡張機能と新機能が用意されています。これらの拡張機能や新機能は、次のセクションで説明します。

（注）　では、（PFC3B または PFC3BXL 搭載の）Supervisor Engine 720 の機能がすべてサポートされます。RSP720 特に注意書きがない限り、このマニュアルの後の章で説明する機能の設定と動作は、両方のタイプのプロセッサ（RSP720 と Sup720）で同じです。

ハードウェア

- 2 枚の統合ドーター カード（PFC3C または PFC3CXL と、MSFC4 ）
- ルート プロセッサ（RP）とスイッチ プロセッサ（SP）での、より高速な CPU と、より容量の大きいデフォルト メモリ
  - RSP720-3C-GE : RP と SP の 1-GB DRAM
  - RSP720-3CXL-GE : 2-GB DRAM（RP）と 1-GB DRAM（SP）
- より大きな MAC アドレス テーブルが提供される追加メモリ
- レイヤ 2 およびレイヤ 3 の機能は、1 つの ASIC に統合済み
- ASIC（ハードウェア）による IP トラフィックと MPLS トラフィックの転送

RSP720 でサポートされているハードウェアの詳細については、『*Cisco 7600 Series Router Supervisor Engine and Route Switch Processor Guide*』の第 2 章のルート スイッチ プロセッサ 720 の項を参照してください。

パフォーマンス

- より高速なソフトウェア ブートアップ
- より高速なプロトコル統合（BGP、OSPF）と ARP ラーニング
- IGMP スヌーピング回数の改善

- DHCP サーバ、Label Distribution Protocol（LDP; ラベル配布プロトコル）セッション、IP セッション、トラフィック エンジニアリング（TE）の確立における速度の高速化
- Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）、Resource Reservation Setup Protocol（RSVP; リソース予約プロトコル）、その他のコントロール プレーン機能でのより高速な処理
- ローカル ファイルへのアクセスとコピーの速度の改善

スケーラビリティ

- レイヤ 2 およびレイヤ 3 のトラフィックの転送レートは、1 秒あたり 3000 万パケット（Mpps）。RSP720 ハードウェア ベースの Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）が使用されます。転送レートは次のとおりです。
  - IP 転送レート：30 Mpps
  - MPLS 転送レート：20 Mpps
- より大規模なカスタマー環境の設定とより多くのインターフェイスに対するサポートは、次のとおりです。
  - 32000 IP 登録者のセッション
  - 100 万のルート
  - 最大 96000 の MAC アドレス（実際には 80000）、64000 から
  - 32000 の VLAN
  - 128000 のアドレス解決プロトコル（ARP）エントリ
- VLAN の拡張性を実現する 802.1ad のサポート

ハイ アベイラビリティ機能

- Online Insertion and Removal（OIR; ホットスワップ）
- Route Processor Redundancy（RPR と RPR+）
- Nonstop Forwarding with Stateful Switchover（NSF/SSO）
- ファブリック スイッチオーバー
- In Service Software Upgrade（ISSU）と enhanced Fast Software Upgrade（eFSU）（Cisco IOS Release 12.2SRB1 およびそれ以降）

IPv6 ACL の機能拡張（セキュリティ）

2K アクセス コントロール リスト（ACL）のラベルと 16K アクセス コントロール エントリ（ACE）が、1K マスクと 8K ACE から改善

未知のユニキャスト パケットのレート制限

ルータが処理する未知のユニキャスト パケットの数を制限でき、パケットがネットワークにフラッディングすることを防ぐ。ルータが受信する未知のパケットの数が、指定されたレートを超えた場合、超過分のパケットは転送されません。設定のガイドラインについては、次のセクション（「未知のユニキャスト パケット レート制限の設定時の注意事項」）を参照してください。

この機能を設定し、確認するために、次の新しいコマンドが用意されています。

- 次のコマンドを使用して、レート制限を設定します。*pps* は、1 秒間に認められる未知のユニキャスト パケットの最大数（10 から 1000000）で、*packets-in-burst* は、オプションのパケット バースト率（1 から 255 で、デフォルト値は 10）です。コマンドの **no** 形式により、未知のパケットのレート制限がオフに設定されます。

```
Router(config)# mls rate-limit layer2 unknown pps [packets-in-burst]
Router(config)# no mls rate-limit layer2 unknown
```

（注）　ルータの物理ポートでルーティングを設定する場合、これらの各ポートで **mac-address-table learning interface** *interface* コマンド（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。このコマンドを使用しなかった場合、レート制限の数が正確ではなくなる可能性があります。

- 未知のユニキャスト パケットのレート制限がイネーブルであるか確認するには、**show mls rate-limit** コマンドを使用します。未知のユニキャスト パケットのレート制限がイネーブルの場合、出力には次のレート制限タイプが含まれます。

```
Router(config)# 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
---------------------   ----------   ---------   -----   -------
UCAST IP TINY FRAG         On          100000     100   Not sharing
```

未知のユニキャスト パケット レート制限の設定時の注意事項

未知のユニキャスト パケット レート制限を構成する際には、次の事項に注意してください。

- この機能は、PFC3C と PFC3CXL（RSP720）でのみ使用できます。これは、PFC3B または PFC3BXL では使用できません。
- 未知のユニキャスト レート制限が設定された状態で、Remote Switched Port Analyzer（RSPAN; リモート スイッチ ポート アナライザ）を実行する場合、RSPAN の送信元ポートと宛先ポートでは、トラフィック量が異なる場合があります。モニタされているトラフィックに未知のユニキャスト パケットが含まれている場合、この違いが発生します。この場合、RSPAN の宛先ポートに送信する前に、未知のユニキャスト トラフィックがレート制限され、この結果、RSPAN の送信元ポートと宛先ポートでのトラフィック量の間にミスマッチが生じます。

GRE トンネル上のパケット フラグメンテーション

Generic Routed Encapsulation（GRE）トンネル上のパケット フラグメンテーションのサポート。PFC3C および PFC3CXL では、[**no**] **mls cef tunnelfragment** コマンドを使用して don't fragment（DF）ビットをゼロに設定できます。これによって、PFC3C または PFC3CXL を使用して、フラグメント化された GRE トラフィックを再構成できます。コマンドの **no** 形式により、トンネルのフラグメンテーションがオフに設定され、フラグメント化された GRE トラフィックが破棄されます。

（注）　この機能を使用するには、トンネルのもう一方の端にあるルータで、トンネルのフラグメンテーションがサポートされている必要があります。

GE バンドルでのロード バランシングの改良

802.1q トランクとして設定されているギガビット イーサネット（GE）バンドルでの、ロード バランシングの改良

- VLAN ID は、マルチキャスト トラフィックのバンドル ハッシュに含まれるようになっています。
- 複数の VLAN でマルチキャスト トラフィックを処理するマルチキャスト レシーバーでは、バンドルのメンバー リンク間でのトラフィックのロード バランシングを行うことができます。
- ルータでは、フラグメント化されたトラフィックについて、より効率的なロード バランシングを行えます。

QoS の機能拡張

- PFC3C と PFC3CXL では、（*シリアル モード*で）お互いに独立して動作するよう、入出力のポリシング機能を設定できます。通常、入出力のポリシング機能はパラレル モードで動作し、1 つのポリシング機能によるアクションが、他での対応するアクションを引き起こします。たとえば、出力ポリシング機能でパケットが破棄される場合、入力ポリシング機能でもパケットは数えられません。この変更は、ポリシング機能を使用したマーキングには影響しないことに、注意してください。

  PFC3C または PFC3CXL で入出力ポリシング機能のシリアル モード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 モードで次のコマンドを使用します。コマンドの **no** 形式により、シリアル モードがディセーブルに設定され、ポリシング モードがパラレルにリセットされます。

  [no] mls qos police serial

- 再循環後のパケットのマーキング。PFC3C と PFC3CXL では、元のインターフェイスの信頼を使用するのではなく、再循環パケットが信頼できないパケットとして扱われます。この機能拡張では、再循環パケットが入力ポリシーによってマークされます。
- IP/MPLS エッジでの、入力 IP DSCP と MPLS EXP マーキング。PFC3C と PFC3CXL のこの機能拡張により、MPLS のラベル インポジション中に、IP DSCP ビット（**set ip dscp**）と MPLS EXP ビット（**set mpls exp**）の両方をマークできます。**set mpls exp** コマンドを使用しなかった場合、ルータでは、IP DSCP ビットが EXP にコピーされることに注意してください。
- 入力 EXP マーキングでは、ローカル ルートを経由する IP/IP トラフィックには影響が及ぼされません。PFC3C と PFC3CXL では、**no mls qos rewrite ip dscp** コマンドを使用して、PFC QoS ロジックの出力 QoS 再書き込みがオフに設定されます。このロジックでは、ローカル ルートを経由する IP/IP トラフィックが EXP マーキングから影響を受けます。
- レイヤ 2 VPN の並列 CoS と DSCP の透過性。PFC3C と PFC3CXL のこの拡張機能を使用すると、トリプル プレイ ネットワーク（ビデオ、Voice over IP（VoIP）、データ アクセス（Internet））で使用するために、レイヤ 2 VPN とレイヤ 3 VPN を組み合わせて導入できます。トラフィックの Quality of Service（QoS）の保証もサポートされます。この機能により、次のような機能拡張も導入されます。
  - **no mls qos rewrite ip dscp** コマンドとの組み合わせで **platform vfi dot1q-transparency** コマンドを使用すると、VPLS と SVI ベースの EoMPLS の CoS 設定と DSCP 設定を保護できます。
  - **no mls qos rewrite ip dscp** コマンドは、MPLS とともに使用できるようになりました。ルータは、PFC3C モードまたは PFC3CXL モードである必要があります。これは、ルータには、Cisco 7600 SIP-600 または WS-X6*xxx* カード（DFC3B または DFC3BXL とともに）を搭載できないことを意味します。
  - **no mls qos rewrite ip dscp** コマンドが MPLS との互換性を持つことになったため、レイヤ 3 VPN は、同じプロバイダー エッジ（PE）で終了できます。
- 新しい CLI コマンドの **mls qos recirc untrust** は、MVPN ケースの内部 VLAN 上での第 2 パス検索中に QoS データがリセットされないようにするために使用します。

（注）　**mls qos recirc untrust** コマンドの完全な構文と使用方法については、次の URL にある『Cisco 7600 Series Routers Command References』を参照してください。
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html

その他の機能拡張

- Ethernet over MPLS（EoMPLS）制御ワードのサポート

- ACL カウンタが、ルート プロセッサ（RP）から受信するパケットの数が含まれるように、機能が拡張
- ハードウェアで処理される IPv6 パケット フラグメント

サポートされない機能

RSP720 では、次の Sup720 機能はサポートされていません。

- Server Load Balancing（SLB）

RSP720 でのフラッシュ メモリのアクセス

表 4-1 に、RSP720 のフラッシュ メモリ デバイスの名前を示します。適切な（内部または外部の）フラッシュ メモリにアクセスするには、コマンドライン インターフェイス（CLI）でソフトウェア コマンドを発行する際に、これらのキーワードを使用します。

表 4-1　RSP720 フラッシュ メモリ デバイスの CLI キーワード

CLI キーワード	アクセス先
bootdisk:	アクティブ ルート プロセッサ（RP）の内部フラッシュ メモリ
sup-bootdisk:	アクティブ スイッチ プロセッサ（SP）の内部フラッシュ メモリ
slavebootdisk:	冗長ルート プロセッサ（RP）の内部フラッシュ メモリ
slavesup-bootdisk:	冗長スイッチ プロセッサ（SP）の内部フラッシュ メモリ
disk0:	アクティブ RSP（フロント パネルのディスク 0）の外部フラッシュ メモリ
disk1:	アクティブ RSP（フロント パネルのディスク 1）の外部フラッシュ メモリ
slavedisk0:	冗長 RSP（フロント パネルのディスク 0）の外部フラッシュ メモリ
slavedisk1:	冗長 RSP（フロント パネルのディスク 1）の外部フラッシュ メモリ

ルート スイッチ プロセッサ 720 ポートの設定

ルート スイッチ プロセッサ　720 のポート 1 には、Small Form-Factor Pluggable（SFP）コネクタが 1 つ装備されています（ほかに特別な設定オプションはありません）。

ルート スイッチ プロセッサ　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）が装備されています。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。

ルート スイッチ プロセッサ 720 のポート 2 が RJ-45 コネクタまたは SFP コネクタのいずれか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 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}`
	または
	`Router(config-if)# no media-type`
		使用するコネクタを選択します。
		
		デフォルト設定（SFP モジュール）に戻します。

次に、RJ-45 コネクタを使用するように、スロット 5 に搭載された RSP720 のポート 2 を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とモニタリング

ここでは、スイッチング モードの設定手順、および ルート スイッチ プロセッサ 720 に組み込まれたスイッチ ファブリック機能のモニタ手順について説明します。

- 「スイッチ ファブリック機能の機能概要」（P.4-7）
- 「スイッチ ファブリック機能の設定」（P.4-8）
- 「スイッチ ファブリック機能のモニタ」（P.4-9）

スイッチ ファブリック機能の機能概要

ここでは、スイッチ ファブリック機能の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.4-7）
- 「レイヤ 3 スイッチド トラフィックの転送の決定」（P.4-7）
- 「スイッチング モード」（P.4-8）

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 ルート スイッチ プロセッサ 720 に内蔵された機能です。ファブリック対応モジュール間の専用接続を作成し、これらのモジュール間で連続的なフレーム伝送を行います。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に加えて、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備えています。

レイヤ 3 スイッチド トラフィックの転送の決定

PFC3 または分散型フォワーディング カード 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 を搭載していないモジュールを介してルータに着信する各パケットの転送先をすべて決定します。
- DFC3 は、次の場合に、DFC3 対応モジュールを介してルータに着信する各パケットの転送先をすべて決定します。
  - 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 ルート スイッチ プロセッサ 720 に送信します。ルート スイッチ プロセッサ 720 のファブリック インターフェイスが 32 Gbps スイッチング バスにパケットを転送し、パケットは出力モジュールで受信されたあと、出力ポートから送信されます。

スイッチング モード

ルート スイッチ プロセッサ 720 が搭載されている場合、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：ルータに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は、すべてのトラフィックに対してこのモードが使用されます。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（32 バイト）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：ルータに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が両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して、このモードが使用されます。このモードでは、ルータはスイッチ 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（フレームの最初の 64 バイト）を送信します。
- bus モード：ルータは、ファブリック非対応モジュール間のトラフィックや、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対して、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 バスまたは RSP バスとの間で送受信されます。

表 4-2 に、搭載されているファブリック対応モジュール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 4-2　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 モードの使用を防止するには、**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、ルータ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 モードのしきい値に戻すには、**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」（P.4-9）
- 「ファブリック チャネルのスイッチング モードの表示」（P.4-9）
- 「ファブリック ステータスの表示」（P.4-10）
- 「ファブリック使用率の表示」（P.4-10）
- 「ファブリック エラーの表示」（P.4-11）

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。

次に、スイッチ ファブリック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
%Truncated mode is allowed
%System is allowed to operate in legacy mode

Module Slot     Switching Mode     Bus Mode
    5                     DCEF     Compact
    9                Crossbar      Compact
```

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      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
```

ファブリック使用率の表示

特定のモジュールまたは全モジュールのファブリック使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**]	ファブリック使用率を表示します。

次に、全モジュールのファブリック使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
```

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 all

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
```

CHAPTER 5

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、Cisco Nonstop Forwarding（NSF）with Stateful Switchover（SSO）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 7600 Series Routers Command References』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- NSF with SSO では、IPv6 マルチキャスト トラフィックがサポートされません。Route Processor Redundancy（RPR）および RPR+（IPv6 マルチキャスト トラフィックをサポート）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は、第 7 章「RPR および RPR+ スーパーバイザ エンジンの冗長設定」を参照してください。
- Release 12.2SR では、Single Router Mode（SRM）with SSO がサポートされません。

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について」（P.5-1）
- 「スーパーバイザ エンジンの設定の同期化」（P.5-9）
- 「NSF の設定作業」（P.5-11）
- 「冗長スーパーバイザ エンジンへのファイルのコピー」（P.5-19）

NSF with SSO スーパーバイザ エンジンの冗長構成について

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を説明します。

- 「NSF with SSO スーパーバイザ エンジンの冗長構成の概要」（P.5-2）
- 「SSO の動作」（P.5-2）
- 「NSF の動作」（P.5-3）
- 「シスコ エクスプレス フォワーディング」（P.5-3）
- 「マルチキャスト MLS NSF with SSO」（P.5-4）

- 「ルーティング プロトコル」（P.5-4）
- 「NSF の利点および制約事項」（P.5-8）

NSF with SSO スーパーバイザ エンジンの冗長構成の概要

（注） Supervisor Engine 720 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 が含まれている場合、**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てください。これにより、すべてのモジュールが dCEF モードで動作し、冗長スーパーバイザ エンジンへの切り替えが簡単になります（CSCec05612）。SRE リリース以降は、RSP720-10G スーパーバイザ エンジンの dcef モードでアップリンク ポートもイネーブルになります。他のスーパーバイザ エンジンでは、アップリンク ポートがディセーブルのままです。

Cisco 7600 シリーズ ルータは、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 エンジンが処理を引き継ぐようにすることによって、耐障害性を強化できます。Cisco NSF は SSO と連動し、切り替え後にユーザがネットワークを使用できない時間を最低限に抑えて、IP パケットの転送を続けます。Cisco 7600 シリーズ ルータは、Route Processor Redundancy（RPR）、Route Processor Redundancy plus（RPR+）もサポートします。冗長モードの詳細については、第 7 章「RPR および RPR+ スーパーバイザ エンジンの冗長設定」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 つがスタンバイとして指定されている場合に、残りのスーパーバイザ エンジンをアクティブとして確立します。それから 2 つのスーパーバイザ エンジンの間の情報を同期化します。アクティブ スーパーバイザ エンジンに障害が発生するか、アクティブ スーパーバイザ エンジンがルータから削除、あるいはメンテナンスのため手動でシャットダウンされると、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。このスイッチオーバーにより、レイヤ 2 トラフィックは中断されません。

SSO を実行するネットワーキング デバイスでは、冗長スーパーバイザ エンジンがアクティブ スーパーバイザ エンジンに障害が発生したあとに制御を引き継ぐように、両方のスーパーバイザ エンジンは同じ設定で稼働している必要があります。また、SSO スイッチオーバーは FIB と隣接エントリを保護し、スイッチオーバーのあとにレイヤ 3 トラフィックを転送できます。設定情報およびデータ構造は、起動時およびアクティブ スーパーバイザ エンジン コンフィギュレーションが変更されたときに、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 エンジンに同期化されます。2 つのスーパーバイザ エンジンの間で初期同期化が行われたあと、SSO は両者の間のステート情報（転送情報を含む）を維持します。

スイッチオーバー中、システム制御およびルーティング プロトコルの実行はアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに転送されます。スイッチでは、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に 0 ～ 3 秒が必要です。

NSF の動作

Cisco NSF は常に SSO と連動し、レイヤ 3 トラフィックに冗長性を提供します。NSF は SSO と連動して、スイッチオーバー後にネットワークが利用できなくなる時間を最小限にします。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、IP パケットを転送し続けることです。

Cisco NSF は、ルーティング用に BGP、OSPF、および IS-IS プロトコルによって、転送用に Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）によってサポートされます。ルーティング プロトコルでは NSF 機能および認識機能が拡張されました。これは、プロトコルを稼働するルータがスイッチオーバーを検出でき、ネットワーク トラフィックを転送し続け、ピア デバイスからのルート情報を回復するのに必要なアクションを実行できることを意味します。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 エンジンの間で同期化されたステート情報を使用してピア デバイスから受信した情報ではなく、スイッチオーバー後のルート情報を回復するように、IS-IS プロトコルを設定できます。

ネットワーキング デバイスが NSF 互換ソフトウェアを実行している場合、このデバイスは NSF 認識です。デバイスが NSF をサポートするように設定されている場合、デバイスは NSF 対応で、NSF 認識または NSF 対応ネイバーからルーティング情報を再構築します。

各プロトコルは、ルーティング プロトコルが Routing Information Base（RIB）テーブルを再構築する間に、スイッチオーバー中にパケットを転送し続ける CEF に依存します。ルーティング プロトコルが収束したあと、CEF は FIB テーブルを更新し、失効したルート エントリを削除します。それから CEF はラインカードに新しい FIB 情報を更新します。

シスコ エクスプレス フォワーディング

NSF の重要な要素はパケット転送です。シスコ製のネットワーキング デバイスでは、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）によって実行されます。CEF は FIB を維持し、スイッチオーバー時の FIB 情報を使用してスイッチオーバー中にパケットを転送し続けます。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短くします。

通常の NSF 動作中、アクティブ スーパーバイザ エンジンの CEF は現在の 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化します。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が発生すると、冗長スーパーバイザ エンジンはまず、アクティブ スーパーバイザ エンジンに存在するミラーリング イメージである FIB および隣接データベースを持ちます。プラットフォームにインテリジェント ラインカードが搭載されている場合、ラインカードはスイッチ上に現在の転送情報を維持します。プラットフォームに転送エンジンが搭載されている場合、CEF は冗長スーパーバイザ エンジンの転送エンジンに、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維持します。ラインカードまたは転送エンジンは、インターフェイスおよびデータ パスが利用できるようになるとすぐに、スイッチオーバー後も転送し続けることができます。

ルーティング プロトコルがプレフィックス単位ベースに RIB を追加すると、アップデートにより CEF に対するプレフィックス単位アップデートが発生します。これは、FIB および隣接データベースをアップデートするのに使用します。既存または新規エントリは、リフレッシュされた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。転送情報はラインカードまたは収束中の転送エンジンで更新されます。RIB が収束されると、スーパーバイザ エンジンは信号を出します。ソフトウェアは、現在のスイッチオーバー エポックよりも前のエポックを持った FIB および隣接エントリをすべて削除します。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

マルチキャスト MLS NSF with SSO

（注）　NSF with SSO では、IPv6 マルチキャスト トラフィックがサポートされません。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は、RPR または RPR+ の冗長性を設定してください。

ルータによって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中にドロップされないようにするには、マルチキャスト マルチレイヤ スイッチング（MMLS）NSF with SSO が必要です。MMLS NSF with SSO を使用しない場合、マルチキャスト プロトコルが収束するまで、レイヤ 3 マルチキャスト トラフィックがドロップされます。

スイッチオーバー プロセス中、（前のアクティブ スーパーバイザ エンジンからの）古いデータベースを使用してトラフィックが転送されます。マルチキャスト ルーティング プロトコルのコンバージェンスが発生したあと、MSFC 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組み合わされ、新しいショートカットとして表示されます。失効したエントリは徐々にデータベースから削除され、NSF はスイッチオーバー中も機能し、新しいキャッシュへスムーズに移行できます。

Protocol Independent Multicast（PIM）スパース モードおよび PIM デンス モードなどのマルチキャスト ルーティング プロトコルはデータ駆動型なので、プロトコルが収束できるように、マルチキャスト パケットは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用にソフトウェアによって転送される必要がないので、ルータ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をリークし続けます。ルータは mroute キャッシュを構築し、ハードウェアにショートカットを導入します。新しいルートが学習されると、データベースを通過し、古いフローを削除するタイマーが起動します。

（注）　マルチキャスト MLS NSF with SSO は、ユニキャスト プロトコルでの NSF サポートを必要とします。

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 MSFC だけで稼働し、隣接ルータからルーティング アップデートを受信します。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 では稼働しません。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 を認識する隣接デバイスに、ステート情報を送信するように要求します。代わりに、IS-IS プロトコルは、ネイバー デバイスが NSF 認識ではない環境の NSF 対応デバイス上でルーティング テーブルを再構築するため、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 エンジンに同期化するよう設定できます。Cisco NSF は、BGP、OSPF、IS-IS、および 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 プロトコルは、ルーティング情報を再構築している間にパケットを転送し続ける CEF によって異なります。

BGP の動作

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。メッセージに含まれるものは、NSF 対応デバイスに「グレースフル」リスタート機能があるステートメントです。グレースフル リスタートは、BGP ルーティング ピアがスイッチオーバーのあとにルーティング フラップが発生するのを防ぐメカニズムです。BGP ピアがこの機能を受信した場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応ルータ ピアおよび

BGP ピアは両方ともセッションの確立時に、OPEN メッセージ内でグレースフル 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、セッションはグレースフル リスタート対応になりません。

BGP セッションがスーパーバイザ エンジンのスイッチオーバー中に中断された場合、NSF 認識 BGP ピアが NSF 対応ルータに関連するルートすべてを失効としてマーキングしますが、一定期間の転送先を決定するためにこれらのルートを使用し続けます。この機能は、新しいアクティブ スーパーバイザ エンジンが BGP ピアでルーティング情報のコンバージェンスを待っている間に、パケットが失われないようにします。

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 対応ルータが BGP ピアでセッションを再確立します。新しいセッションの確立時に、NSF 対応ルータが再起動したこと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 ピアの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して新しい転送情報を持った RIB および FIB で更新されます。NSF 認識デバイスはネットワーク情報を使用して、失効ルートを BGP テーブルから削除します。その後 BGP プロトコルが完全に収束されます。

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 対応デバイスを使用して BGP セッションを確立します。この機能により、非 NSF 認識 BGP ピアとの相互運用性（および NSF 機能がない相互運用性）を可能にしますが、非 NSF 認識 BGP ピアでの BGP セッションはグレースフル リスタート対応になりません。

（注） NSF の BGP サポートでは、ネイバー ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージ内でこ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 ネイバーにグレースフル リスタート機能がないことを検出した場合、そのネイバーとの NSF 対応セッションを確立しません。グレースフル リスタート機能のある他のネイバーはすべて、NSF 対応ネットワーキング デバイスとの NSF 対応セッションを維持し続けます。

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する場合、ルータは OSPF ネイバーとリンク ステート データベースを再同期化するため、次の作業を行う必要があります。

- ネイバー関係をリセットしないで、ネットワーク上で利用できる OSPF ネイバーを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

スーパーバイザ エンジン スイッチオーバーのあと、NSF 対応ルータはできるだけ迅速に OSPF NSF 信号をネイバー NSF 認識デバイスに送信します。ネイバー ネットワーキング デバイスは、このルータとのネイバー関係をリセットしてはならないインジケータとしてこの信号を認識します。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、ネイバー リストの再構築を始めます。

ネイバー関係が再構築されると、NSF 対応ルータはすべての NSF 認識ネイバーとデータベースの再同期化を始めます。この時点でルーティング情報は OSPF ネイバーの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、失効ルートを削除し、RIB を更新して、新しい転送情報で FIB を更新します。その後、OSPF プロトコルは完全に収束されます。

（注） OSPF NSF では、すべてのネイバー ネットワーク デバイスが NSF 認識である必要があります。NSF 対応ルータが特定のネットワーク セグメント上に NSF 認識ネイバーがないことを検出した場合、ルータはそのセグメントの NSF 機能をディセーブルにします。全体が NSF 対応または NSF 認識ルータで構成された他のネットワーク セグメントは、NSF 機能を提供し続けます。

IS-IS の動作

IS-IS 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する場合、ルータは IS-IS ネイバーとリンク ステート データベースを再同期化するため、次の作業を行う必要があります。

- ネイバー関係をリセットしないで、ネットワーク上で利用できる IS-IS ネイバーを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

NSF を設定する場合、IS-IS NSF 機能は次のオプションを提供します。

- 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

ネットワーク セグメントの隣接ルータで、ルータの再起動機能用に 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 バージョンが稼働している場合、ルータは再起動する IETF NSF ルータを支援します。IETF を使用する場合、隣接ルータはスイッチオーバー後のルーティング情報を再構築する隣接情報およびリンク ステート情報を提供します。IETF IS-IS コンフィギュレーションの利点は、提案された標準に基づいたピア デバイスの間の動作であることです。

（注） ネットワーキング デバイスに IETF を設定する場合で隣接ルータが IETF と互換性がないとき、NSF はスイッチオーバー後に中断します。

ネットワーク セグメント上の隣接ルータが NSF 認識でない場合、シスコのコンフィギュレーション オプションを使用する必要があります。Cisco IS-IS コンフィギュレーションは、プロトコル隣接情報とリンクステート情報両方をアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに送信します。シスコのコンフィギュレーションの利点は、NSF 認識ネイバーに依存しないことです。

IETF IS-IS コンフィギュレーション

スーパーバイザ エンジン スイッチオーバー後できるだけ迅速に、NSF 対応ルータは IETF IS-IS コンフィギュレーションを使用して、IS-IS NSF 再起動要求をネイバー NSF 認識デバイスに送信します。隣接ネットワーキング デバイスは、この再起動要求をこのルータとのネイバー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。再起動するルータがネットワーク上のルータから再起動要求を受信すると、ネイバー リストの再構築を始めます。

交換が完了すると、NSF 対応デバイスはリンクステート情報を使用して失効ルートを削除し、RIB を更新して、新しい転送情報で FIB を更新します。その後 IS-IS が完全に収束されます。

一方のスーパーバイザ エンジンからもう一方のスーパーバイザ エンジンへのスイッチオーバーは数秒以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された時間の間、待機します。この間、新しい冗長スーパーバイザ エンジンが起動し、この設定をアクティブ スーパーバイザ エンジンと同期化します。IS-IS NSF を再起動しようとする前に接続を安定させるため、IS-IS NSF 動作は指定された時間の間、待機します。この機能は、IS-IS が失効情報でバックツーバック NSF を再起動しないようにします。

Cisco IS-IS コンフィギュレーション

シスコのコンフィギュレーション オプションを使用すると、冗長スーパーバイザ エンジンに十分な隣接情報および LSP 情報が保存されるか、または*チェックポイント*されます。スイッチオーバー後、新しいアクティブ スーパーバイザ エンジンがチェックポイントされたデータを使用して、隣接関係を維持し、ルーティング テーブルを迅速に再構築できます。

（注）　スイッチオーバー後、Cisco IS-IS NSF には十分なネイバー隣接情報および LSP 情報が設定されていますが、スイッチオーバーの前に隣接していたインターフェイスがすべて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、ネイバー デバイスから学習されたルートはルーティング テーブルの再計算で考慮されません。IS-IS NSF ではあらゆる理由でタイミング良くオンラインになることができないインターフェイスの待機時間を延長するコマンドが用意されています。

一方のスーパーバイザ エンジンからもう一方のスーパーバイザ エンジンへのスイッチオーバーは数秒以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された時間の間、待機します。この間、新しい冗長スーパーバイザ エンジンが起動し、この設定をアクティブ スーパーバイザ エンジンと同期化します。同期化が終了すると、IS-IS 隣接および LSP データは冗長スーパーバイザ エンジンにチェックポイントされますが、インターバル時間が満了するまで IS-IS は新しい NSF を再起動しようとしません。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 再起動からアップに戻る場合、ネイバーがなく、そのトポロジ テーブルは空です。ルータがインターフェイスを起動し、ネイバーを再取得し、トポロジおよびルーティング テーブルを再構築する必要がある場合、ルータは冗長スーパーバイザ エンジン（現在はアクティブ）によって通知されます。再起動ルータおよびピアは、再起動ルータへのデータ トラフィック転送を中断することなく、次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 再起動プロセスを介してトラフィックを転送し続けます。

ネイバーによる隣接のリセットを防ぐには、再起動ルータは EIGRP パケット ヘッダーの新しい Restart（RS）ビットを使用して、再起動を指示します。RS ビットは NSF 再起動中、Hello パケットおよび初期 INIT アップデート パケットに設定されます。hello パケットの RS ビットにより、ネイバーに迅速に NSF 再起動を通知できます。RS ビットを参照しない場合、ネイバーは INIT アップデートの受信、または Hello ホールド タイマーの期限切れによって隣接リセットを検出します。RS ビットを使用しない場合、ネイバーは、隣接リセットを NSF または通常の起動方法を使用して処理する必要があるかどうか認識できません。

ネイバーが Hello パケットまたは INIT パケットのいずれかを受信することにより再起動表示を受信すると、ネイバーはピア リストの再起動ピアを認識し、再起動ルータとの隣接関係を維持します。ネイバーはトポロジ テーブルを、最初のアップデート パケットに設定された RS ビットのある再起動ルータに送信します。このパケットは NSF 認識であり、再起動ルータに役立つことを示しています。ネイバーは NSF 再起動ネイバーでない場合、Hello パケットに RS ビットを設定しません。

（注）　ルータは NSF 認識ですが、コールド スタートから起動するのでネイバーを再起動する NSF を支援しない可能性があります。

1 つ以上のピア ルータが NSF 認識の場合、再起動ルータはアップデートを受信してからデータベースを再構築します。再起動ルータは Routing Information Base（RIB）に通知できるように収束したかどうかを認識する必要があります。各 NSF 認識ルータは、テーブル内容の終わりを示すために、最新アップデート パケットの End Of Table（EOT）マーカーを送信する必要があります。再起動ルータは EOT マーカーを受信すると、収束したことを認識します。再起動ルータはアップデートの送信を開始できます。

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再起動ルータが収束した時間を認識します。その後ピアはトポロジ テーブルをスキャンして、送信元として再起動されたネイバーを持ったルートを検索します。ピアはルート 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、ルートがまだ利用できるかどうかを判断します。ピアはアクティブになり、再起動したルータを介して利用できなくなったルート用に代替パスを検索します。

再起動ルータがネイバーから EOT 表示すべてを受信したとき、または NSF 収束タイマーが失効したとき、EIGRP が 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ってから、トポロジ テーブルを待機中の NSF 認識ピアすべてにフラッディングします。

NSF の利点および制約事項

Cisco NSF には次の利点があります。

- 向上したネットワーク アベイラビリティ。

  スイッチオーバー後にユーザ セッション情報を維持するよう、NSF はネットワーク トラフィックおよびアプリケーション ステート情報の転送を続けます。

- ネットワーク全体の安定性。

  ネットワークの安定性は、ネットワークのルータに障害が発生し、ルーティング テーブルを失った場合に作成されたルート フラップ数を削除することで向上します。

- 隣接ルータはリンク フラップを検出しない。

  インターフェイスはスイッチオーバーの間アップ状態のままなので、隣接ルータはリンク フラップを検出しません（リンクは停止せず、アップに戻ります）。

- ルーティング フラップの回避。

  SSO はスイッチオーバー時にネットワーク トラフィックの転送を続けるので、ルーティング フラップは回避されます。

- ユーザ セッションの損失なし。

  スイッチオーバーの前に確立されたユーザ セッションは維持されます。

Cisco NSF with SSO には次の制約事項があります。

- NSF が動作するには、SSO をデバイス上に設定する必要があります。
- NSF with SSO は IP Version 4 のトラフィックとプロトコルだけをサポートします。
- Enhanced Object Tracking は SSO を認識しないため、SSO モードの Hot Standby Routing Protocol（HSRP）、仮想ルータ冗長プロトコル（VRRP）、および Gateway Load Balancing Protocol（GLBP）と同時に使用することができません。
- 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 および SSO は共存できますが、それぞれの機能は独立して動作します。VRRP に依存するトラフィックは、スーパーバイザ 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。
- BGP NSF に参加しているネイバー デバイスはすべて NSF 対応で、BGP 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。
- 仮想リンク用 OSPF NSF はサポートされません。
- 同じネットワーク セグメント上のすべての OSPF ネットワーキング デバイスは、NSF 認識（NSF ソフトウェア イメージを稼働）である必要があります。
- IETF IS-IS の場合、ネイバー デバイスはすべて NSF 認識ソフトウェア イメージを稼働する必要があります。

- IPv4 マルチキャスト NSF with SSO は PFC3 だけでサポートされます。
- 基本的なユニキャスト プロトコルは、マルチキャスト NSF with SSO を使用するため NSF 認識である必要があります。
- Release 12.2(33)SRE 以降では、Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）は、SSO を認識し、また NSF with SSO によりサポートされています。

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.5-9）
- 「冗長構成設定時の注意事項および制約事項」（P.5-9）

（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 を介してルータを設定すると、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 ファイルの同期を開始します。

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。

- 「冗長構成設定時の注意事項および制約事項」（P.5-9）
- 「ハードウェア設定時の注意事項および制約事項」（P.5-10）
- 「コンフィギュレーション モードに関する制約事項」（P.5-10）

冗長構成設定時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。

- Supervisor Engine 720 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

  SRE リリース以降は、RSP720-10G スーパーバイザ エンジンの dcef モードでアップリンク ポートもイネーブルになります。他のスーパーバイザ エンジンは引き続きアップリンク ポートがディセーブルになります。
- 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スは行われません。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 を介してルータを設定すると、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 ファイルの同期を開始します。

- 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 の場合、ファブリック同期エラーが発生した場合のデフォルト動作は、冗長スーパーバイザ エンジンへの切り替えです。場合によっては、冗長スーパーバイザ エンジンへの切り替えは、ファブリック同期エラーの原因となったモジュールの電源を切ることよりも破壊的です。**no fabric error-recovery fabric-switchover** コマンドを入力してスイッチオーバーをディセーブルにし、ファブリック同期エラーが発生したモジュールの電源を切ってください。

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 ソフトウェアは、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 エンジンが単独でルータを稼働させるためのリソースを備えている必要があります。つまりスーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ デバイスを含む）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.5-19）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 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ルータを起動します。最新のリリース ノートの手順に従って、Catalyst オペレーティング システム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 レジスタは自動起動に設定されていなければなりません。

（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 の設定作業

ここでは NSF 機能の設定作業について説明します。

- 「SSO の設定」（P.5-11）
- 「マルチキャスト MLS NSF with SSO の設定」（P.5-12）
- 「マルチキャスト NSF with SSO の確認」（P.5-12）
- 「CEF NSF の設定」（P.5-13）
- 「CEF NSF の確認」（P.5-13）
- 「BGP NSF の設定」（P.5-13）
- 「BGP NSF の確認」（P.5-14）
- 「OSPF NSF の設定」（P.5-15）
- 「OSPF NSF の確認」（P.5-15）
- 「IS-IS NSF の設定」（P.5-16）
- 「IS-IS NSF の確認」（P.5-17）

SSO の設定

あらゆるサポート対象プロトコルを持った 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、次の作業を行います。

	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。このコマンドが入力されると、冗長スーパーバイザ エンジンがリロードされ、SSO モードで動作を開始します。
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。

次に、SSO 対応としてシステムを設定し、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） ここで示すコマンドは任意で、設定をカスタマイズするのに使用できます。大半のユーザにとってデフォルト設定が適切です。

冗長モードとして SSO が選択されている場合、マルチキャスト MLS NSF with SSO はデフォルトでオンになります。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 コンバージェンスの最大待機時間を指定します。有効値は 0 ～ 3600 秒です。
ステップ 3	`Router(config)# mls ip multicast sso leak` *interval*	パケット リークのインターバルを指定します。有効値は、0 ～ 3600 秒です。PIM スパース モードおよび PIM デンス モードの場合、これは既存の PIM スパース モードおよび PIM デンス 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。有効値は 1 ～ 100% です。この値は、パケット リーク用にフラグ付けされる既存の PIM スパース モードおよび PIM デンス モード マルチキャスト フローの総数の割合を表示します。

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 デバイスが SSO モードで稼働している間、CEF NSF 機能はデフォルトで動作します。したがって設定作業は不要です。

CEF NSF の確認

CEF が NSF 対応であ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 に参加しているピア デバイスすべてに BGP グレースフル リスタートを設定する必要があります。

NSF 用に BGP を設定するには、各 BGP NSF ピア デバイス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。

	コマンド	目的
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、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 グレースフル リスタート機能をイネーブルにし、BGP NSF を開始します。 BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバーと交換する機能のセッションを再開する必要があります。 再起動ルータおよびそのピアすべてで、このコマンドを使用します。

BGP NSF の確認

BGP 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 デバイスおよびネイバー デバイス上で設定されているか確認する必要があります。確認する手順は、次のとおりです。

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 コンフィギュレーションに表示されているか確認します。

```
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 ネイバーでステップ 1 を繰り返します。

ステップ 3　SSO デバイスおよびネイバー デバイスで、グレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを確認し、グレースフル リスタート機能を備えたアドレス ファミリであることを確認します。アドレス ファミリが表示されない場合、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 family 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 に参加するピア デバイスすべては OSPF NSF 認識である必要があります。これは、デバイス上の NSF ソフトウェア イメージをインストールすると自動的に設定されます。

OSPF NSF 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)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにし、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 用に NSF 動作をイネーブルにします。

OSPF NSF の確認

OSPF NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。OSPF NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応デバイスの OSPF コンフィギュレーションに表示されているか確認します。

```
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　NSF がデバイス上でイネーブルであるか確認するには、**show ip ospf** コマンドを入力します。

```
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 の設定

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、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` [**cisco** | **ietf**]	IS-IS 用 NSF をイネーブルにします。 IETF ドラフトベースの再起動をサポートするネットワーキング デバイスとの隣接関係が保証される同種ネットワークで IS-IS をイネーブルにするには、**ietf** キーワードを入力します。 NSF 認識ネットワーキング デバイスとの隣接関係がない異種ネットワークで IS-IS を稼働するには、**cisco** キーワードを入力します。
ステップ 4	`Router(config-router)# nsf interval` [*minutes*]	（任意）NSF 再起動試行までの最小時間を指定します。*連続した* NSF 再起動試行間のデフォルト時間は、5 分です。
ステップ 5	`Router(config-router)# nsf t3` {**manual** [*seconds*] | **adjacency**}	（任意）過負荷になったリンクステート情報を生成し、情報をネイバーにフラッディングする前に、IS-IS データベースが同期化するまで IS-IS が待機する時間を指定します。 IETF 動作を選択した場合に限り、**t3** キーワードが適用されます。**adjacency** を指定すると、再起動ルータが、ネイバー デバイス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）IS-IS NSF 再起動が、IS-IS の隣接関係を持つすべてのインターフェイスが起動するのを待機してから、再起動を完了する時間を指定します。デフォルトは 10 秒です。

IS-IS NSF の確認

IS-IS NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。IS-IS NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応デバイスの IS-IS コンフィギュレーションに表示されていることを確認します。Cisco IS-IS または IETF IS-IS コンフィギュレーションのいずれかを表示します。次の例は、デバイスが IS-IS NSF のシスコ実装を使用していることを示します。

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

ステップ 2　NSF コンフィギュレーションが **cisco** に設定されている場合、NSF がデバイス上でイネーブルかを確認するには **show isis nsf** コマンドを入力します。シスコのコンフィギュレーションを使用すると、コマンドの出力はアクティブ RP および冗長 RP で異なります。次の表示では、アクティブ RP 上のシスコ コンフィギュレーションの出力例を示します。この例では、「NSF restart enabled」の存在に注意してください。

```
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
```

次に、スタンバイ RP 上のシスコ コンフィギュレーションの出力例を示します。この例では、「NSF restart enabled」の存在に注意してください。

```
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 コンフィギュレーションが **ietf** に設定されている場合、NSF がデバイス上でイネーブルかを確認するには **show isis nsf** コマンドを入力します。次の表示では、ネットワーキング デバイス上の IETF IS-IS コンフィギュレーションの出力例を示します。

```
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)# router eigrp` *as-number*	EIGRP ルーティング プロセスをイネーブルにし、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。 再起動ルータおよびそのピアすべてで、このコマンドを使用します。

EIGRP NSF の確認

EIGRP NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。EIGRP NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、「nsf」が SSO 対応デバイスの EIGRP コンフィギュレーションに表示されていることを確認します。

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

ステップ 2　NSF がデバイス上でイネーブルであるか確認するには、**show ip protocols** コマンドを入力します。

```
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

次のコマンドを入力して、冗長スーパーバイザ エンジン上の **disk0:** デバイスにファイルをコピーします。

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

次のコマンドを入力して、冗長スーパーバイザ エンジン上の **bootflash:** デバイスにファイルをコピーします。

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

次のコマンドを入力して、冗長 MSFC 上の **bootflash:** デバイスにファイルをコピーします。

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

CHAPTER 6

Cisco 7600 シリーズ ルータでの ISSU および eFSU

この章では、Cisco 7600 シリーズ ルータで In Service Software Upgrade 機能を実行する方法について説明します。

この章の内容は、次のとおりです。

- 「ISSU および eFSU の概要」（P.6-1）
- 「Cisco 7600ISSU および eFSU のサポート」（P.6-5）
- 「Cisco 7600ISSU および eFSU の注意事項および制約事項」（P.6-7）
- 「稼働中ソフトウェア アップグレードの実行」（P.6-9）
- 「非 eFSU イメージの eFSU イメージへのアップグレード」（P.6-21）
- 「コマンド リファレンス」（P.6-21）

ISSU および eFSU の概要

大部分のネットワークでは、ソフトウェア アップグレードにはシステム ダウンタイムを要しますが、In Service Software Upgrade（ISSU）機能を使用することで、ルータ ソフトウェアのアップグレード時でも、ルータによるトラフィックの転送を続行できます。したがって、ISSU によりネットワークの可用性が向上し、ソフトウェア アップグレードによるダウンタイムが短縮されます。

Cisco 7600 シリーズ ルータは、次のタイプのアップグレード手順をサポートします。どちらのタイプのアップグレードにも、同じ ISSU コマンドとアップグレード手順が使用されます。

- ISSU：システムのダウンタイムを最小限に抑えてシステム アップグレードを行います。この機能は、ラインカード ソフトウェアが同じ Cisco IOS ソフトウェア リリース間のソフトウェア アップグレードに使用できます
（Cisco IOS Release 12.2SRB1 以降のリリースで使用可能）。
- enhanced Fast Software Upgrade（eFSU）：ISSU のサブセットである eFSU により、サポートされているラインカードに新しいラインカード ソフトウェアのイメージをプリロードすることにより、ソフトウェア アップグレード中の停止時間を最小限に抑えられます。この機能は、ラインカード ソフトウェアが異なるリリース間のアップグレードに使用できます
（Cisco IOS Release 12.2SRB 以降のリリースで使用可能）。

ISSU では、NonStop Forwarding（NSF）の既存の機能を Stateful SwitchOver（SSO）と併用して、ソフトウェア アップグレードを実行します。2 つのスーパーバイザ エンジンまたは Route Switch Processor（RSP; ルート スイッチ プロセッサ）を備えた冗長システムでは、プロセッサのどちらか一方がアクティブになり、その間もう一方のプロセッサはスタンバイ モードで動作し、アクティブなプロセッサがダウンした場合に処理を引き継ぐ準備をしています。

稼働中ソフトウェア アップグレード（ISSU または eFSU）時は、新しいソフトウェアがスタンバイ プロセッサにロードされ、アクティブなプロセッサは古いソフトウェアを使用して動作を続行します。アップグレードの一部として、アクティブなプロセッサとスタンバイ プロセッサとの間でスイッチオーバーが行われ、スタンバイ プロセッサがアクティブになり、新しいソフトウェアの実行を開始します。アップグレードを続行して新しいソフトウェアを別のプロセッサにロードすることも、アップグレードを中断して古いソフトウェアで動作を再開することもできます。

新しいソフトウェア リリースに新しいラインカード ソフトウェアが含まれており、ルータのラインカードが eFSU をサポートしている場合、アップグレード プロセスにより新しいラインカード ソフトウェアがラインカードにプリロードされます。スイッチオーバー発生時（アクティブなプロセッサとスタンバイ プロセッサ間）に、ラインカードは新しいソフトウェア イメージを使用して再起動されます。eFSU は、新しいソフトウェア イメージをラインカードにプリロードすることで、ソフトウェア アップグレード時の停止時間を最小限に抑えます。

ISSU の詳細については、次の URL の『*Cisco IOS In Service Software Upgrade Process*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sbisefsu.htm

ISSU の概要

Cisco IOS Releases 12.2SRB1 以降のリリースでは Cisco 7600 シリーズ ルータで ISSU がサポートされます。ISSU のアップグレード中、ルータはトラフィックのルーティングと転送を続行するため、あるソフトウェア リリースから別のソフトウェア リリースへのアップグレードを最小限のシステム ダウンタイム（0 ～ 3 秒）で実行できます。

ISSU は、ルータの NSF/SSO 準拠プロトコルおよびソフトウェア機能に使用できます。ISSU をサポートする Cisco 7600 プロトコルと機能の一覧については、「ISSU のサポート」（P.6-5）を参照してください。

（注）　ISSU アップグレードを実行するには、新旧の Cisco IOS ソフトウェア リリースが共に同じラインカード ソフトウェアを備えている必要があります。リリースに異なるラインカード ソフトウェアが含まれる場合、ルータは eFSU アップグレードを実行します。

eFSU の概要

eFSU は、この機能をサポートするラインカードに新しいソフトウェア イメージをプリロードすることで、稼働中ソフトウェア アップグレード時の停止時間を最小限に抑えます。ソフトウェア アップグレード プロセス時に、アクティブなスーパーバイザ エンジンまたは RSP とスタンバイ中のスーパーバイザ エンジンまたは RSP 間でスイッチオーバーが発生します。スイッチオーバーが発生すると、ラインカードは再起動されます。eFSU をサポートするラインカードは、プリロードされた新しいソフトウェア イメージを使用して再起動されます。

eFSU をサポートする Cisco 7600 ラインカードを次に示します。

- SIP-400 および SIP-600
- ESM-2x10GE および ESM-20x1GE-3C
- 67*xx* ラインカード

その他すべての Cisco 7600 ラインカードはスイッチオーバー時にハード リセットされ、ラインカードの再起動後、ソフトウェア イメージがロードされます。

（注）　eFSU をサポートするには、ラインカードには 512 MB のメモリと、新しいソフトウェア イメージを格納するための十分な空きメモリが必要です。使用可能なメモリが十分にない場合、ソフトウェアのプリロードは失敗し、ラインカードはスイッチオーバー時にリセットされます。

停止時間とサポートに関する考慮事項

eFSU アップグレード時に、ラインカードは、プロセッサ間で発生するスイッチオーバー後に再起動またはリセットされます。ラインカードは再起動またはリセットされるため、プロトコルおよびソフトウェア機能がオンラインに復帰するまで、ラインカードへのリンクは切断され、トラフィック処理は中断されます。ラインカードによる処理が中断される時間（停止時間）は、eFSU プロセスが新しいソフトウェア イメージをラインカードにプリロード可能かどうかにより異なります。

- eFSU をサポートするラインカードの場合、停止時間は RPR+ モードの場合の停止時間と同じです。
- eFSU をサポートしないラインカードの場合、停止時間は RPR モードの場合の停止時間と同じです。

新しいソフトウェアのダウンロード後（**issu loadversion**）は、**show issu outage slot all** コマンドを使用して、インストールしたラインカードの最大停止時間を表示できます。コマンドの例については、「インストールされているラインカードの最大停止時間の表示（任意）」（P.6-15）を参照してください。

旧バージョンのソフトウェアをルータにロードしようとし、そのバージョンが現在インストールされているラインカードをサポートしていない場合、次のいずれかの状況が発生します。

- **issu loadversion** コマンドで **force** オプションを使用した場合、ルータは RPR モードになります。
- **force** オプションを省略すると、eFSU プロセスが中断され、ラインカードでの問題発生を通知するエラー メッセージが表示されます。

ラインカード メモリの予約

eFSU をサポートするラインカードでは、ルータは新しいソフトウェア イメージ（解凍フォーマット）を格納するためのメモリをラインカード上で自動的に予約します。必要なメモリの量は、ラインカードのタイプにより異なります。

次のコマンドを実行して、ルータがソフトウェアのプリロード用にメモリを予約しないようにできます（ラインカードをインストールするスロットを *slot-num* で指定）。ただし、推奨はできません。

no mdr download reserve memory image slot *slot-num*

（注）　新しいソフトウェア イメージを保持するのに十分な空きメモリがラインカードにない場合、ソフトウェアのプリロードは失敗し、ラインカードはスイッチオーバー時にリセットされます。停止時間は、RPR を使用した場合の停止時間と同じです（ラインカードの再起動後、新しいラインカード イメージをロードする必要があるため）。

ラインカードで予約されるメモリ量を判断するには、次の例に示すとおり **show mdr download image** コマンドを使用します（Cisco 7600 SIP-600 の場合）。

```
SIP-600# show mdr download image
Pre-download information
Slot CPU In-Progress Complete LC Mem Resv (bytes)
 1   0      N           N         0
 1   1      N           N         0
 2   0      N           N         0
 2   1      N           N         0
```

```
 3   0     N          N         0
 3   1     N          N         0
 4   0     N          N         0
 4   1     N          N         0
 5   0     N          N         0
 5   1     N          N         0
 6   0     N          Y         36175872
 6   1     N          N         0
 7   0     N          N         0
 7   1     N          N         0
 8   0     N          N         0
 8   1     N          N         0
 9   0     N          Y         35127296
 9   1     N          N         0
10   0     N          Y         31195136
10   1     N          N         0
11   0     N          N         0
11   1     N          N         0
12   0     N          N         0
12   1     N          N         0
13   0     N          Y         31195136
13   1     N          N         0

SIP-600#
```

eFSU の動作

ソフトウェア アップグレード時に、eFSU をサポートするラインカード上でルータは次の手順を実行します。これらの手順は、アップグレード プロセス中に自動的に実行されるので、ユーザの操作は必要ありません。

- インストールされている各ラインカードに新しい Cisco IOS ソフトウェア イメージに必要なメモリを予約する（ラインカードがソフトウェアのプリロードをサポートする場合）。
- **issu loadversion** コマンドの一部として、サポートされているラインカードに新しいソフトウェア イメージをプリロードする。
- スイッチオーバーの発生時に、新しいソフトウェア イメージを使用してラインカードを再起動する（**issu runversion**）。
- ロールバックまたは中断が発生した場合、ルータはラインカード ソフトウェアを元のバージョンに戻す。中断時間をできるだけ短くするため、ルータはラインカードに元のソフトウェア バージョンをプリロードします。ロールバックまたは中断の完了後、ラインカードは元のソフトウェア バージョンを使用して再起動されます。

ラインカード ソフトウェア プリロードのエラー処理

ラインカード ソフトウェアのプリロード中に問題が発生した場合、ルータは次の対処方法を実行します。

- バージョンをロードする際のラインカードのクラッシュ：スイッチオーバー発生時にラインカードがリセットされます。
- eFSU 起動時にラインカードをアクティブにしない：ソフトウェア アップグレード時にラインカードに電源が供給されないため、ラインカードはプロセス終了時にリセットされます。ソフトウェア アップグレード プロセスの開始後、ルータに挿入されるラインカードに同じ対処方法が適用されます。

- バージョン実行時またはロールバック時のラインカードのクラッシュ：アクティブなスーパーバイザ エンジンまたは RSP に存在するソフトウェア イメージに対応するソフトウェア イメージのバージョンを使用して、ラインカードが起動します。

Cisco 7600ISSU および eFSU のサポート

ISSU アップグレード時に、NSF/SSO 準拠プロトコルおよびソフトウェア機能は動作を続行し、最小限のシステム ダウンタイムが生じます。NSF/SSO 準拠でないルーティング プロトコルおよびソフトウェア機能は、アップグレード時に再起動されます。これは、再起動後にこれらがオンラインに復帰するまで、しばらくの間動作が停止することを意味します。

ISSU アップグレードを実行するには、新旧の Cisco IOS ソフトウェア リリースが共に同じラインカード ソフトウェアを備えている必要があります。リリースに異なるラインカード ソフトウェアが含まれる場合、ルータは eFSU アップグレードを実行します。

ISSU のサポート

ISSU は次の Cisco 7600 ハードウェアおよびソフトウェアでサポートされます。

提供状況

- Cisco IOS Release 12.2SRB1 以降

ハードウェア

- サポートされるすべての Cisco 7600 シャーシ（拡張（-S）シャーシを含む）
- RSP720-3C、RSP720-3CXL、Sup720-3B、Sup720-3BXL、Sup32
- すべての Cisco 7600 ラインカード、DFC、およびその他のモジュール

ソフトウェア

- 802.1q
- 802.1x
- ARP
- ATM
- BGP
- Etherchannel（PagP および LACP）
- GLBP
- HDLC
- HSRP
- IPv4
- L2 マルチキャスト
- MLP（マルチリンク PPP）
- MPLS（LDP、TE、および VPN を含む）：アップグレード時に実行が必要な手順の詳細については、*ISSU MPLS Client* のマニュアルを参照してください。
  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_issu_clients_ps6922_TSD_Products_Configuration_Guide_Chapter.html#wp1054109

- NetFlow
- PPP
- QoS
- Routing Information Base（RIB）
- SNMP
- SPAN および Remote SPAN
- STP
- Virtual Routing and Forwarding（VRF）

Cisco IOS ソフトウェア リリースに関する ISSU 互換性マトリクス

次の表に、C7600 用のさまざまな Cisco IOS リリースに関する ISSU 互換性マトリクスを示します。2 つのリリース間で ISSU がサポートされている場合は、その列に Yes と表示され、2 つのリリース間で ISSU がサポートされていない場合は、対応する列に No と表示されています。

表 6-1　ISSU 互換性マトリクス

Cisco IOS リリース	12.2 (33) SRB	12.2 (33) SRC	12.2 (33) SRD	12.2 (33) SRE	15.0 (1) S 以降のリリース
12.2 (33) SRB	Yes	Yes	No	No	No
12.2 (33) SRC	Yes	Yes	No	No	No
12.2 (33) SRD	No	No	Yes	Yes	No
12.2 (33) SRE	No	No	Yes	Yes	No
15.0(1) S 以降のリリース	No	No	No	No	Yes

eFSU のサポート

eFSU は次の Cisco 7600 ハードウェアおよびソフトウェアでサポートされます。

提供状況

- Cisco IOS Release 12.2SRB 以降
- Release 12.2(33)SRB1 で導入された RSP720 および Sup32 のサポート

ハードウェア

- すべての Cisco 7600 シャーシ（3 スロット シャーシ、CISCO7603 を除く）
- RSP720-3C、RSP720-3CXL、Sup720-3B、Sup720-3BXL、Sup32
- DFC3B、DFC3BXL、DFC3C、DFC3CXL
- SM-2x10GE、ESM-20x1GE-3C
- SIP-400、SIP-600、67*xx* ラインカード

サポートされないハードウェア

- 拡張 FlexWAN、OSM-GE-WAN
- 68*xx*、65*xx*、64*xx*、63*xx*、および 61*xx* ラインカード

ソフトウェアのサポート

eFSU 実行時に、Cisco 7600 ラインカードが再起動されます。再起動中、ソフトウェア機能とルーティング プロトコルは使用できません。停止時間は、ラインカードが eFSU をサポートしているかどうかにより異なります（「eFSU の概要」（P.6-2）を参照）。

Cisco 7600ISSU および eFSU の注意事項および制約事項

Cisco 7600 シリーズ ルータで稼働中ソフトウェア アップグレードを実行する際の注意事項と制約事項を次に示します。特に指定がない限り、注意事項は ISSU および eFSU の両方に適用されます。

- サポートされていない Cisco 7600 ハードウェアおよびソフトウェアは、ISSU または eFSU と共存できます（つまり、どちらもルータに含めることができます）。さらにルータは、サポートされていないプロトコルがあれば通常の手順で再起動し、「ブラック ホール」状態を防止します。
- 稼働中ソフトウェア アップグレードを実行するには、ルータでは 2 つのルート プロセッサ（RP）、つまりアクティブな RP とスタンバイ RP が 1 つずつ必要です。Cisco 7600 ルータ では、2 つのスーパーバイザ エンジンまたは Route Switch Processors（RSP; ルート スイッチ プロセッサ）が必要です。これらにはルータ用のルート プロセッサが含まれているためです。
- アクティブなスーパーバイザ エンジンまたは RSP およびスタンバイ スーパーバイザ エンジンまたは RSP では、アップグレード プロセス実行前に新旧のソフトウェア イメージの両方を保存するため、少なくとも 256 MB のフラッシュ メモリが必要です。
- ISSU および eFSU のどちらでも、同じ ISSU コマンドとアップグレード手順が使用されます。唯一の相違点は、ラインカードが ISSU によるアップグレード時には起動されず、eFSU では起動されることです。
- ルータは、新旧のソフトウェア イメージを調べて、適切なプロセス（ISSU または eFSU）を自動実行し、ソフトウェア イメージをアップグレードします。
  - 新旧のソフトウェア イメージでラインカード ソフトウェアが同じ場合、ルータは ISSU を実行してソフトウェアをアップグレードします。システムのダウンタイムは 0 ～ 3 秒です。
  - 新旧両イメージでラインカード ソフトウェアが異なる場合、ラインカードはアップグレード プロセス中に再起動またはリセットされます。システム ダウンタイムは、ラインカードが eFSU をサポートしているかどうかにより異なります（詳細については「停止時間とサポートに関する考慮事項」（P.6-3）を参照してください）。
- ISSU アップグレード機能は、NSF/SSO をサポートするすべてのソフトウェア機能でサポートされます。NSF/SSO をサポートしないソフトウェア機能は、ソフトウェア アップグレード時に発生するスイッチオーバー後、これらの機能がオンラインに復帰するまで、しばらくの間動作を中止します。
- ソフトウェアのプリロードを正常に実行するには、eFSU をサポートするすべてのラインカードに最低 512 MB のメモリが必要です。そうでない場合、これらのラインカードでプリロードは失敗します。
- eFSU をサポートするラインカードは、新しいソフトウェア イメージを保持するための十分なメモリを備えている必要があります。使用可能なメモリが十分でない場合、ソフトウェアのプリロードは失敗し、カードはスイッチオーバー時にリセットされます（スイッチオーバーはアクティブなスーパーバイザ エンジンまたは RSP とスタンバイ スーパーバイザ エンジンまたは RSP 間で発生）。
- ISSU および eFSU は SSO モードだけでサポートされます。RPR および RPR+ モードではサポートされません。
- 稼働中ソフトウェア アップグレード中は、Online Insertion and Removal（OIR; ホットスワップ）はサポートされません。アップグレードがアクティブな間にルータに新しいラインカードを挿入しようとしても、カードにルータから電源供給されません。アップグレードが終了すると、ルータは新しく挿入されたラインカードをリセットします。
- アップグレード中は、スーパーバイザ エンジンまたは RSP 間で手動スイッチオーバーを実行しないでください。手動スイッチオーバーはルータでは許可されますが、当社では使用しないことを強く推奨します。
- ISSU コマンド（eFSU でも使用）をコマンドライン インターフェイス（CLI）で使用できるのは、サポートされているプロセッサがルータにインストールされている場合だけです。それ以外のタイプのスーパーバイザ エンジンまたは RSP がインストールされている場合、コマンドは使用できません。
  - Release 12.2SRB1 以降では、コマンドは RSP720、Sup720、または Sup32 で使用できます。

  - Release 12.2SRB では、Sup720 がインストールされている場合に限り、コマンドを使用できます。
- コンフィギュレーション レジスタが自動起動できるよう設定されていることを確認します（レジスタの最低バイトは 2 に設定する必要があります）。
- **issu abortversion** コマンドを実行（してソフトウェア アップグレードを中断）する前に、スタンバイ スーパーバイザ エンジンまたは RSP が起動（STANDBY HOT（SSO の場合）または COLD（RPR の場合））していることを確認します。
- 旧ソフトウェア バージョンから Cisco IOS Release 12.2SRB 以降にアップグレードするには、Fast Software Upgrade（FSU）プロセスを使用します。このプロセス中に、eFSU をサポートするラインカード上で、ラインカード ソフトウェア イメージもアップグレードされます。
- eFSU をサポートしないモジュールでは、Route Processor Redundancy（RPR）モードでソフトウェア イメージをアップグレードできます。
- 異なるファイル システムから同じイメージを使用してアクティブ スーパーバイザとスタンバイ スーパーバイザを起動すると、ISSU が失敗します。

稼働中ソフトウェア アップグレードの実行

ここでは、Cisco 7600 ルータで稼働中ソフトウェア アップグレード（ISSU または eFSU）を実行するプロセスについて説明します。説明する手順は次のとおりです。

- 「ソフトウェア アップグレード プロセスの概要」（P.6-9）
- 「アップグレードの準備」（P.6-11）
- 「新しいソフトウェア イメージのコピー」（P.6-13）
- 「スタンバイ RP への新しいソフトウェアのロード」（P.6-13）
- 「スイッチオーバーのアクティブからスタンバイへの強制切り替え」（P.6-16）
- 「新しいソフトウェア バージョンの許可とロールバック プロセスの停止（任意）」（P.6-18）
- 「スタンバイに対する新しいソフトウェアの認定」（P.6-19）
- 「ソフトウェア インストレーションの確認」（P.6-20）
- 「アップグレード プロセスの中断」（P.6-21）

各セクションでは、アップグレード プロセスでの特定の手順を簡単に説明し、コマンドの例を示します。コマンドの例では、コマンド出力で重要なフィールドを太字で示しています。これらのフィールドをチェックして、コマンドのステータスを確認します。

コマンドの詳細については、次の URL にある 12.2SRB の新しい機能に関するマニュアル サイトで、『*Cisco IOS In Service Software Upgrade Process*』（機能ガイド）を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sbisefsu.htm

ソフトウェア アップグレード プロセスの概要

ここでは、Cisco 7600 ルータでソフトウェア イメージをアップグレード（またはダウングレード）する際に必要な作業の概要を示します。次のセクションでは、ルータでのソフトウェア アップグレード プロセスの例を示します。

ISSU および eFSU のどちらでも、同じ ISSU コマンド セットとアップグレード手順が使用されます。

（注）　ISSU アップグレード プロセスは、同じラインカード ソフトウェアを共有する Cisco IOS リリースに対してだけ実行できます。リリースに含まれるラインカード ソフトウェアが異なる場合、ルータは eFSU アップグレードを実行します。

	コマンドまたはアクション	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	`Router# copy tftp disk_name`	TFTP を使用して、アクティブ RP およびスタンバイ RP（disk0: および slavedisk0:）上のフラッシュ メモリに新しいソフトウェア イメージをコピーします。プロンプトで、新しいソフトウェア イメージの名前と場所を指定します。
ステップ 3	`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 4	`Router(config)# no service image-version efsu` `Router(config)# end`	Cisco 7600 ルータでソフトウェア アップグレードを実行する際に必要な互換性マトリクス チェックをディセーブルにします。**end** コマンドを実行すると、特権 EXEC モードに戻ります。

ステップ 5	`Router# show version | in image`
	`Router# show bootvar`
	
	`Router# show redundancy`
	`Router# show issu state [detail]`
		show コマンドでは、ルータが ISSU または eFSU の実行準備ができていることを確認します。**show version** および **show bootvar** コマンドでは、ブート イメージの設定を確認します。
		show redundancy および **show issu state** コマンドでは、冗長モードがイネーブルになっていることと、SSO と NSF が設定されていることを確認します。
		（注）　**show redundancy** および **show issu state** は、アップグレードのステータスを確認するため（次の例に示すとおり）アップグレード全体で使用します。

ステップ 6	`Router# issu loadversion active-slot active-image standby-slot standby-image [force]`	アップグレード プロセスを開始して、新しいソフトウェア イメージをスタンバイ RP にロードします。新しいイメージがロードされ、スタンバイ RP が SSO モードに移行するのに数秒かかる場合があります。
ステップ 7	`Router# remote command switch show issu outage slot all`	（任意）インストールされているラインカードの最大停止時間を表示します。スーパーバイザ エンジンのスイッチ プロセッサ（SP）または RSP に対してコマンドを実行します。 （注）　コマンドの **show issu outage slot all** は SP 上でしかサポートされません。
ステップ 8	`Router# issu runversion slot image`	スイッチオーバーを強制実行して、スタンバイ スーパーバイザ エンジンまたは RSP をアクティブにし、新しいソフトウェアの実行を開始させます。それまでアクティブだったプロセッサはスタンバイ状態となり、古いイメージを使用して起動します。

	コマンドまたはアクション	目的
ステップ 9	`Router# issu acceptversion {active slot-number | active slot-name slot-name}`	（任意）ロールバック タイマーを停止して、アップグレード プロセス中に新しいソフトウェア イメージが自動的に中断されないようにします。
ステップ 10	`Router# issu commitversion slot active-image`	新しいソフトウェア イメージを、指定されたスロットのスタンバイ スーパーバイザ エンジンまたは RSP にロードします。
ステップ 11	`Router# show redundancy` `Router# show issu state [detail]`	アップグレード プロセスのステータスを確認します。アップグレードが正常に実行された場合は、アクティブなスーパーバイザ エンジンまたは RSP とスタンバイ スーパーバイザ エンジンまたは RSP が共に新しいソフトウェア バージョンを実行します。

アップグレードの準備

ソフトウェア アップグレードを実行する前に、必ず「Cisco 7600ISSU および eFSU の注意事項および制約事項」（P.6-7）を確認してください。

ISSU または eFSU の準備をする前に、次に示す作業を実行します。

- 「互換性マトリクス チェックのディセーブル化」（P.6-11）
- 「ブート イメージのバージョンとブート変数の確認」（P.6-11）
- 「冗長モードの確認」（P.6-12）
- 「ISSU ステートの確認」（P.6-12）

互換性マトリクス チェックのディセーブル化

Cisco 7600 ルータでソフトウェア アップグレードを実行するには、グローバル コンフィギュレーション モードで次のコマンドを実行することで、まず互換性マトリクス チェックをディセーブルにする必要があります。

```
Router(config)# no service image-version efsu
```

ブート イメージのバージョンとブート変数の確認

アップグレードを開始する前に、次の例に示すとおり **show version** および **show bootvar** コマンドを実行して、ルータのブート イメージ バージョンと BOOT 環境変数を確認することを推奨します。

```
Router# show version | in image
System image file is "disk0:oct22"

Router# show bootvar
BOOT variable = disk0:oct22,1;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2102

Standby BOOT variable = disk0:oct22,1;
Standby CONFIG_FILE variable =
Standby BOOTLDR variable =
Standby Configuration register is 0x2102
```

冗長モードの確認

冗長モードがイネーブルになっており、NSF および SSO が設定されていることを確認することも推奨します。次のコマンド例に冗長性の確認方法を示します。

```
Router# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 9 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 8 minutes
                 Image Version = Cisco IOS Software, s72033_rp Software
(s72033_rp-ADVENTERPRISEK9_WAN_DBG-M), Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 23-Oct-06 02:43 by
                         BOOT = disk0:oct22,1;
                    CONFIG_FILE =
                        BOOTLDR =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 8 minutes
                 Image Version = Cisco IOS Software, s72033_rp Software
(s72033_rp-ADVENTERPRISEK9_WAN_DBG-M), Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 23-Oct-06 02:43 by
                         BOOT = disk0:oct22,1;
                    CONFIG_FILE =
                        BOOTLDR =
        Configuration register = 0x2102
```

ISSU ステートの確認

次に示すとおり、ISSU ステートも確認する必要があります。

```
Router# show issu state

                         Slot = 5
                    RP State = Active
                   ISSU State = Init
                  Boot Variable = disk0:oct22,1;

                         Slot = 6
                    RP State = Standby
                   ISSU State = Init
```

```
Boot Variable = disk0:oct22,1;
```

新しいソフトウェア イメージのコピー

ISSU または eFSU プロセスを開始する前に、新しいソフトウェア イメージをアクティブなルート プロセッサおよびスタンバイ ルート プロセッサ上のフラッシュ メモリ（disk0: および slavedisk0:）にコピーする必要があります。これらのルート プロセッサは Cisco 7600 スーパーバイザ エンジンまたはルート スイッチ プロセッサ上にあります。

```
Router# copy tftp disk0:

Address or name of remote host []? sys1
Source filename []? /auto/tftpboot/image/c7600s72033-adventerprisek9_wan-mz
Destination filename [c7600s72033-adventerprisek9_wan-mz]? c7600s72033
Accessing tftp://sys1//auto/tftpboot/image/c7600s72033-adventerprisek9_wan-mz
Loading /auto/tftpboot/image/c7600s72033-adventerprisek9_wan-mz from 192.0.2.245 (via
GigabitEthernet5/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

（コマンド出力は省略）

```
[OK - 124978660 bytes]

124978660 bytes copied in 259.868 secs (480931 bytes/sec)

Router# copy disk0:c7600s72033 slavedisk0:

Destination filename [c7600s72033]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

（コマンド出力は省略）

```
124978660 bytes copied in 308.488 secs (405133 bytes/sec)
```

スタンバイ RP への新しいソフトウェアのロード

issu loadversion コマンドを実行して、アップグレード プロセスを開始します。この手順により、スタンバイ スーパーバイザ エンジンまたは RSP が再起動され、スタンバイ ルート プロセッサに新しいソフトウェア イメージがロードされます。
ダウンロードが完了すると、**runversion** コマンドを実行するようプロンプトが表示されます。

```
Router# issu loadversion 5 disk0:c7600s72033 6 slavedisk0:c7600s72033
Router#
*Oct 27 21:26:20.119: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF
request)
```

（上記の例では、スロット 6 のスタンバイ スーパーバイザ エンジンが再起動していることを示しています。再起動が完了すると、ルータは新しいイメージをスタンバイにロードします）

```
*Oct 27 21:26:20.775: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
changing to Simplex mode
*Oct 27 21:29:46.123: SP: pf_redun_check_img_compatibility: MATRIX result is compatible!!!
Of course...
*Oct 27 21:29:47.135: %PFREDUN-SP-6-ACTIVE: Standby initializing for SSO mode
*Oct 27 21:29:47.431: %SYS-SP-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure
console debugging output.
*Oct 27 21:29:50.647: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the
standby Router.
```

```
*Oct 27 21:30:29.687: %FABRIC-SP-5-CLEAR_BLOCK: Clear block option is off for the fabric
in slot 6.
*Oct 27 21:30:29.783: %FABRIC-SP-5-FABRIC_MODULE_BACKUP: The Switch Fabric Module in slot
6 became standby
*Oct 27 21:30:30.523: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
*Oct 27 21:30:32.459: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
*Oct 27 21:30:32.675: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now
online
*Oct 27 21:29:46.071: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.
*Oct 27 21:30:14.123: %SPANTREE-SP-STDBY-5-EXTENDED_SYSID: Extended SysId enabled for type
vlan
*Oct 27 21:30:14.539: SP-STDBY: SP: Currently running ROMMON from S (Gold) region
*Oct 27 21:30:17.067: %DIAG-SP-STDBY-6-RUN_MINIMUM: Module 6: Running Minimal
Diagnostics...
*Oct 27 21:30:29.331: %DIAG-SP-STDBY-6-DIAG_OK: Module 6: Passed Online Diagnostics
*Oct 27 21:31:30.431: %SYS-SP-STDBY-5-RESTART: System restarted --
Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ), Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:49 by
*Oct 27 21:33:14.231: %ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please
issue the runversion command
*Oct 27 21:33:13.471: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode
*Oct 27 21:33:14.239: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Oct 27 21:33:13.655: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.
```

（注）　この時点で、**show redundancy** および **show issu state detail** コマンドを使用してアップグレード ステータスをチェックすることを推奨します（次の例を参照）。**issu loadversion** が完了したら、スタンバイ RP が新しいソフトウェア イメージを使用してロードされ、RP が SSO モードになっているはずです。**issu loadversion** が完了するのに数秒かかる場合があるため、**show** コマンドを入力するタイミングが早すぎた場合、必要な情報が表示されないことがあります。

```
Router# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 38 minutes
Switchovers system experienced = 0
              Standby failures = 1
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 37 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 23-Oct-06 02:43 by
                         BOOT = disk0:oct22,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102
```

```
Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 13 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:21 by
                         BOOT = disk0:c7600s72033,12;disk0:oct22,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102


Router# show issu state detail

                         Slot = 5
                     RP State = Active
                   ISSU State = Load Version
                  Boot Variable = disk0:oct22,12
                 Operating Mode = sso
                Primary Version = disk0:oct22
              Secondary Version = disk0:c7600s72033
                Current Version = disk0:oct22
                 Variable Store = PrstVbl
                      ROMMON CV = [disk0:oct22]

                         Slot = 6
                     RP State = Standby
                   ISSU State = Load Version
                  Boot Variable = disk0:c7600s72033,12;disk0:oct22,12
                 Operating Mode = sso
                Primary Version = disk0:oct22
              Secondary Version = disk0:c7600s72033
                Current Version = disk0:c7600s72033
```

インストールされているラインカードの最大停止時間の表示（任意）

新しいソフトウェアのダウンロード後は、Switch Processor（SP; スイッチ プロセッサ）上で **show issu outage slot all** コマンドを実行して、インストールされているラインカードの最大停止時間を表示できます。

```
Router# remote command switch show issu outage slot all

Slot # Card Type                                    MDR Mode          Max Outage Time
------ -------------------------------------      -----------       ---------------
     1 CEF720 24 port 1000mb SFP                   WARM_RELOAD        300 secs
     2 1-subslot SPA Interface Processor-600       WARM_RELOAD        300 secs
     3 4-subslot SPA Interface Processor-400       WARM_RELOAD        300 secs
     4 2+4 port GE-WAN                             RELOAD             360 secs

Router#
```

（注）　ISSU アップグレードの場合、MDR Mode ではコマンド出力に NSF_RELOAD と表示されます。これは、ラインカードが再起動またはリロードされず、最大停止時間が 0 ～ 3 秒であることを示しています。

スイッチオーバーのアクティブからスタンバイへの強制切り替え

アクティブなスーパーバイザ エンジンまたは RSP およびスタンバイ スーパーバイザ エンジンまたは RSP 間で強制的にスイッチオーバーを実行するには、**issu runversion** コマンドを実行します。新しいソフトウェア イメージがロードされているスタンバイ スーパーバイザ エンジンまたは RSP がアクティブになります。それまでアクティブだったスーパーバイザ エンジンまたは RSP はスタンバイとなり、古いソフトウェア イメージを使用して起動します（ソフトウェア アップグレードを中断して古いイメージを復元することが必要になった場合）。

```
Router# issu runversion 6

This command will reload the Active unit.  Proceed ? [confirm]
*Oct 27 21:43:18.901: %SYS-SP-3-LOGGER_FLUSHING: System pausing to ensure console
debugging output.

*Oct 27 21:43:18.901: %OIR-SP-6-CONSOLE: Changing console ownership to switch processor
```

（この時点でスーパーバイザ間のスイッチオーバーが発生します。それまでスタンバイだったスーパーバイザ エンジンまたは RSP はアクティブになり、新しいソフトウェア バージョン（c7600s72033）を実行します。それまでアクティブだったスーパーバイザ エンジンまたは RSP はスタンバイとなり、古いソフトウェア（oct22）を使用して起動します）

```
*Oct 27 21:43:19.105: %SYS-SP-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure
console debugging output.

*Oct 27 21:43:21.702: %SYS-SP-3-LOGGER_FLUSHING: System pausing to ensure console
debugging output.

***
*** --- SHUTDOWN NOW ---
***

*Oct 27 21:43:21.702: %SYS-SP-5-RELOAD: Reload requested by Delayed Reload. Reload Reason:
Reason unspecified.
*Oct 27 21:43:21.702: %OIR-SP-6-CONSOLE: Changing console ownership to switch processor

*Oct 27 21:43:22.067: %SYS-SP-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure
console debugging output.

System Bootstrap, Version 8.1(3)
Copyright (c) 1994-2004 by cisco Systems, Inc.
Cat6k-Sup720/SP processor with 1048576 Kbytes of main memory

Autoboot executing command: "boot disk0:oct22"
Loading image, please wait ...

Initializing ATA monitor library...
```

（コマンド出力は省略、新しいアクティブ ログ）

```
Press RETURN to get started!

*Oct 27 21:30:06.611: STDBY: RP: Currently running ROMMON from S (Gold) region
*Oct 27 21:31:07.923: %SPANTREE-STDBY-5-EXTENDED_SYSID: Extended SysId enabled for type
vlan
*Oct 27 21:31:30.183: %SYS-STDBY-5-RESTART: System restarted --
Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ), Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:21 by
```

```
*Oct 27 21:31:30.307: %SYS-STDBY-6-LOGGINGHOST_STARTSTOP: Logging to host 172.19.126.3
Port 514 started - CLI initiated
*Oct 27 21:43:22.067: %PFREDUN-SP-STDBY-6-ACTIVE: Initializing as ACTIVE processor
*Oct 27 21:43:22.071: %FABRIC-SP-STDBY-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in
slot 6 became active.
*Oct 27 21:43:22.715: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.
*Oct 27 21:43:24.363: %ISSU_PROCESS-SP-7-DEBUG: Initializing timers
*Oct 27 21:43:24.363: %ISSU_PROCESS-SP-7-DEBUG: rollback timer process has been started
*Oct 27 21:43:24.554: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
*Oct 27 21:43:24.650: %OIR-SP-3-SOFT_RESET: Module 1 is being soft reset as a part of
swichover error recovery
*Oct 27 21:43:24.674: %LINK-SP-3-UPDOWN: Interface TenGigabitEthernet2/1, changed state to
down
*Oct 27 21:43:24.754: %OIR-SP-3-SOFT_RESET: Module 2 is being soft reset as a part of
swichover error recovery
*Oct 27 21:43:24.854: %OIR-SP-3-SOFT_RESET: Module 3 is being soft reset as a part of
swichover error recovery
*Oct 27 21:43:24.906: %OIR-SP-3-SOFT_RESET: Module 4 is being soft reset as a part of
swichover error recovery
*Oct 27 21:43:24.962: %OIR-SP-3-SOFT_RESET: Module 7 is being soft reset as a part of
swichover error recovery
```

（コマンド出力は省略）

```
*Oct 27 21:48:34.787: %SYS-SP-STDBY-6-BOOTTIME: Time taken to reboot after reload =  314
seconds
*Oct 27 21:50:31.059: %ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please
issue the acceptversion command
*Oct 27 21:50:31.067: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode
*Oct 27 21:50:31.067: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Oct 27 21:50:31.251: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.

Router# enable
```

（注） この時点で、新しくアクティブになったスーパーバイザ エンジンまたは RSP は新しいソフトウェア イメージを実行しており、スタンバイ スーパーバイザ エンジンまたは RSP は古いソフトウェア イメージを実行しています。次の例に示すとおり、アクティブなスーパーバイザ エンジンまたは RSP とスタンバイ スーパーバイザ エンジンまたは RSP のステートを確認する必要があります（**show redundancy** および **show issu state detail**）。

```
Router# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 57 minutes
Switchovers system experienced = 1
              Standby failures = 0
        Last switchover reason = user initiated

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
```

```
       Uptime in current state = 17 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:21 by
                         BOOT = disk0:c7600s72033,12;disk0:oct22,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 5
        Current Software state = STANDBY HOT
       Uptime in current state = 15 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 23-Oct-06 02:43 by
                         BOOT = disk0:oct22,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102

router# show issu state detail

                         Slot = 6
                    RP State = Active
                   ISSU State = Run Version
                 Boot Variable = disk0:c7600s72033,12;disk0:oct22,12
                Operating Mode = sso
              Primary Version = disk0:c7600s72033
            Secondary Version = disk0:oct22
              Current Version = disk0:c7600s72033
               Variable Store = PrstVbl
                    ROMMON CV = [disk0:c7600s72033]

                         Slot = 5
                    RP State = Standby
                   ISSU State = Run Version
                 Boot Variable = disk0:oct22,12
                Operating Mode = sso
              Primary Version = disk0:c7600s72033
            Secondary Version = disk0:oct22
              Current Version = disk0:oct22
```

（注） アップグレード プロセスを完了するには、**issu acceptversion**（任意）および **issu commitversion** コマンドを実行します（次の項を参照）。

新しいソフトウェア バージョンの許可とロールバック プロセスの停止（任意）

新しいソフトウェア イメージは、許可または認定する必要があります。そうでなければ、ロールバック タイマーが期限切れになり、アップグレード プロセスが停止されます。この状況が発生した場合、ソフトウェア イメージは前回のソフトウェア バージョンに戻ります。ロールバック タイマーは、アップグレード プロセスによってルータの動作が停止しないようにするためのセーフガードとして機能します。

次のコマンド シーケンスでは、**issu acceptversion** がロールバック タイマーを停止して、新しいソフトウェア イメージの機能を調べられるようにします。新しいイメージが許可できることを確認した場合、**issu commitversion** コマンドを実行してアップグレード プロセスを終了します。

```
Router# show issu rollback-timer
        Rollback Process State = In progress
      Configured Rollback Time = 45:00
       Automatic Rollback Time = 27:08

Router# issu acceptversion 6
% Rollback timer stopped. Please issue the commitversion command.
```

この時点で、ロールバック タイマーを表示して、ロールバック プロセスが停止されていることを確認します。

```
Router# show issu rollback-timer
        Rollback Process State = Not in progress
      Configured Rollback Time = 45:00
```

スタンバイに対する新しいソフトウェアの認定

新しいソフトウェア イメージをスタンバイ スーパーバイザ エンジンまたは RSP にロードして、ソフトウェア アップグレード プロセスを完了するには、**issu commitversion** コマンドを実行します。次の例では、新しいイメージ（c7600s72033）を、スロット 5 のスタンバイ スーパーバイザ エンジンにロードします。

```
Router# issu commitversion 5

Building configuration...

*Oct 27 22:09:57.239: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the
standby Router. [OK]
feeder#
*Oct 27 22:10:15.613: %OIR-SP-3-PWRCYCLE: Card in module 5, is being power-cycled (RF
request)
```

（スロット 5 のスタンバイ スーパーバイザ エンジンが再起動を開始し、続いて、新しいイメージをロードします。）

```
*Oct 27 22:10:15.639: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
changing to Simplex mode
*Oct 27 22:13:40.723: SP: pf_redun_check_img_compatibility: MATRIX result is compatible!!!
Of course...
*Oct 27 22:13:41.731: %PFREDUN-SP-6-ACTIVE: Standby initializing for SSO mode
*Oct 27 22:13:42.027: %SYS-SP-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure
console debugging output.
*Oct 27 22:13:44.999: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the
standby Router.
*Oct 27 22:14:24.019: %FABRIC-SP-5-CLEAR_BLOCK: Clear block option is off for the fabric
in slot 5.
*Oct 27 22:14:24.115: %FABRIC-SP-5-FABRIC_MODULE_BACKUP: The Switch Fabric Module in slot
5 became standby
```

（コマンド出力は省略）

```
*Oct 27 22:15:23.310: %SYS-SP-STDBY-5-RESTART: System restarted --
Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ), Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:49 by
```

```
*Oct 27 22:15:44.751: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode
*Oct 27 22:15:45.135: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Oct 27 22:15:44.935: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.
```

（注）　以上で、ソフトウェア アップグレード プロセスが完了しました。アクティブなスーパーバイザ エンジンまたは RSP とスタンバイ スーパーバイザ エンジンまたは RSP は共に新しいソフトウェア バージョンを実行しています。

ソフトウェア インストレーションの確認

ソフトウェア アップグレードのステータスを確認する必要があります。アップグレードが正常に実行された場合は、アクティブなスーパーバイザ エンジンまたは RSP とスタンバイ スーパーバイザ エンジンまたは RSP が共に新しいソフトウェア バージョンを実行します。

```
Router# show redundancy

Redundant System Information :
------------------------------
       Available system uptime = 1 hour, 13 minutes
Switchovers system experienced = 1
              Standby failures = 1
        Last switchover reason = user initiated

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 6
        Current Software state = ACTIVE
       Uptime in current state = 33 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:21 by
                          BOOT = disk0:c7600s72033,12;disk0:oct22,1;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 5
        Current Software state = STANDBY HOT
       Uptime in current state = 4 minutes
                 Image Version = Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ),
Version 12.2
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 26-Oct-06 03:21 by
                          BOOT = disk0:c7600s72033,12;disk0:oct22,1;
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102


router# show issu state detail
```

```
                Slot = 6
          RP State = Active
        ISSU State = Init
     Boot Variable = disk0:c7600s72033,12;disk0:oct22,12
   Operating Mode = sso
  Primary Version = N/A
Secondary Version = N/A
  Current Version = disk0:c7600s72033
   Variable Store = PrstVbl
        ROMMON CV = [disk0:c7600s72033]

                Slot = 5
          RP State = Standby
        ISSU State = Init
     Boot Variable = disk0:c7600s72033,12;disk0:oct22,12
   Operating Mode = sso
  Primary Version = N/A
Secondary Version = N/A
  Current Version = disk0:c7600s72033
```

アップグレード プロセスの中断

ソフトウェア アップグレードは、**issu abortversion** コマンドを実行することでどの段階ででも手動で中断できます。またソフトウェアが障害を検出した場合、アップグレード プロセス自体が中断します。

issu loadversion コマンドの実行後プロセスを中断した場合、スタンバイ スーパーバイザ エンジンまたは RSP がリセットされ、元のソフトウェアを使用してリロードされます。

次に、**issu abortversion** *slot image* コマンドを使用して、ソフトウェア アップグレード プロセスを中断する例を示します。

```
Router# issu abortversion 6 c7600s72033
```

（注）　**issu abortversion** コマンドを実行する前に、スタンバイ スーパーバイザ エンジンまたは RSP が起動（STANDBY HOT（SSO の場合）または COLD（RPR の場合））していることを確認します。

非 eFSU イメージの eFSU イメージへのアップグレード

新しい Cisco IOS ソフトウェア イメージが eFSU をサポートしていない場合、ソフトウェア イメージを手動でアップグレードする必要があります。それには、スタンバイ スーパーバイザ エンジン または RSP 上でソフトウェア イメージをアップグレードした後、手動スイッチオーバーを実行して、スタンバイが新しいイメージによる処理を引き継ぐようにする必要があります。これにより、それまでアクティブで現在はスタンバイとなっているスーパーバイザ エンジンまたは RSP 上でソフトウェア イメージをアップグレードできます。手順については、「Fast Software Upgrade の実行」（P.7-8）を参照してください。

コマンド リファレンス

Cisco 7600 シリーズ ルータでは、すべての標準 ISSU コマンドがサポートされています。これらのコマンドの詳細については、次の URL にある『*Cisco IOS In Service Software Upgrade Process*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/sbisefsu.htm

CHAPTER 7

RPR および RPR+ スーパーバイザ エンジンの冗長設定

この章では、Route Processor Redundancy（RPR）および RPR+ を使用して、スーパーバイザ エンジンの冗長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 7600 Series Routers Command References』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- RPR および RPR+ では IPv6 マルチキャスト トラフィックがサポートされます。
- Release 12.2SR では、Single Router Mode（SRM）with Stateful Switchover（SSO）がサポートされません。

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」（P.7-1）
- 「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.7-4）
- 「スーパーバイザ エンジンの冗長構成の設定」（P.7-6）
- 「Fast Software Upgrade の実行」（P.7-8）
- 「冗長スーパーバイザ エンジンへのファイルのコピー」（P.7-10）

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を説明します。

- 「スーパーバイザ エンジンの冗長構成の概要」（P.7-2）
- 「RPR の動作」（P.7-2）
- 「RPR+ の動作」（P.7-3）
- 「スーパーバイザ エンジンの設定の同期化」（P.7-3）

スーパーバイザ エンジンの冗長構成の概要

（注）　スーパーバイザ エンジンの冗長構成の重要事項については、「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」（P.7-4）を参照してください。

Cisco 7600 シリーズ ルータは、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 エンジンが処理を引き継ぐようにすることによって、耐障害性を強化できます。Cisco 7600 シリーズ ルータでは、次の冗長モードがサポートされます。

- RPR：2 分以上のスイッチオーバーをサポートします。
- 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働するわけではなく、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.7-8）を参照）。

ルータの電源投入時に、2 つのスーパーバイザ エンジン間で RPR が動作します。最初に起動するスーパーバイザ エンジンは、RPR 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 カードおよびポリシー フィーチャ カードは全面的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。

- すべてのスイッチング 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 コントロール 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。

ルータの電源投入時に、2 つのスーパーバイザ エンジン間で RPR+ が稼働します。最初に起動するスーパーバイザ エンジンは、アクティブ スーパーバイザ エンジンになります。MSFC および PFC は全面的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.7-4）
- 「RPR+ スーパーバイザ エンジンの設定の同期化」（P.7-4）

（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 を使用してルータを設定したら、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開始し、RPR+ を使用して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+ モードの場合は、次の動作が発生すると設定が同期化されます。

- 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、冗長構成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。冗長構成により、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 CLI 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。

- 「冗長構成に関する注意事項および制約事項」（P.7-4）
- 「RPR+ に関する注意事項および制約事項」（P.7-5）
- 「ハードウェア設定時の注意事項および制約事項」（P.7-6）
- 「コンフィギュレーション モードに関する制約事項」（P.7-6）

冗長構成に関する注意事項および制約事項

RPR および RPR+ 冗長モードに関する注意事項および制約事項は、次のとおりです。

- Supervisor Engine 720 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 が含まれている場合、**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てください。これにより、すべてのモジュールが dCEF モードで動作し、冗長スーパーバイザ エンジンへの切り替えが簡単になります（CSCec05612）。

  SRE リリース以降は、RSP720-10G スーパーバイザ エンジンの dcef モードでアップリンク ポートもイネーブルになります。他のスーパーバイザ エンジンでは、アップリンク ポートがディセーブルのままです。
- 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スは行われません。アクティブになるスーパーバイザ エンジンは常に 1 つだけです。

- 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 を使用してルータを設定したら、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開始し、RPR+ を使用して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ルータが回復するまで、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 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。

  - 終了したすべての PPP セッション
  - すべての ATM SVC 情報
  - 終了したすべての 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 ソフトウェアが稼働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 ソフトウェアが稼働していない場合は、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 エンジンが搭載されたルータ上で、**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るには **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「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 ソフトウェアは、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 エンジンが単独でルータを稼働させるためのリソースを備えている必要があります。つまりスーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ デバイスを含む）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.7-10）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 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ルータを起動します。最新のリリース ノートの手順に従って、Catalyst オペレーティング システム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（詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください）。

（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。

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。

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

冗長構成の設定

冗長構成を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# 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。このコマンドが入力されると、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+ モードで動作を開始します。
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）　デフォルトの自動同期設定を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 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 ソフトウェア 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、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **copy** *source_device*:*source_filename* {**disk0** | **disk1**}:*target_filename* または： Router# **copy** *source_device*:*source_filename* **sup-bootflash:***target_filename* または： Router# **copy** *source_device*:*source_filename* **slavedisk0:***target_filename* または： Router# **copy** *source_device*:*source_filename* **slavesup-bootflash:***target_filename*	新しい Cisco IOS ソフトウェア イメージを両方のスーパーバイザ エンジン上のブートフラッシュにコピーします。
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 イメージが稼働します。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#
```

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:** デバイス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:** デバイス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:** デバイスにファイルをコピーします。

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

CHAPTER 8

インターフェイスの設定

この章では、Cisco 7600 シリーズ ルータ 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。この章の内容は、次のとおりです。

- 「インターフェイス設定の概要」（P.8-1）
- 「interface コマンドの使用」（P.8-2）
- 「インターフェイス範囲の設定」（P.8-3）
- 「インターフェイス範囲マクロの定義および使用」（P.8-4）
- 「オプションのインターフェイス機能の設定」（P.8-5）
- 「活性挿抜の概要」（P.8-15）
- 「インターフェイスのモニタおよびメンテナンス」（P.8-15）
- 「TDR を使用したケーブル ステータスの確認」（P.8-16）

（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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

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イネーブルになります。各インターフェイスは、ルータの特定スロットに設置されたモジュールのポートに対応します。

- スロット番号：モジュールの搭載先スロットです。Cisco 7600 シリーズ ルータの各スロットには、上から下へ、または右から左へ、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。Cisco 7600 シリーズ ルータのポート番号は、常に 1 から始まります。ルータの背面から見て、左から右へ、または上から下へ通し番号が付けられています。

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。

いくつかの LAN プロトコルおよび WAN プロトコル（ATM やフレーム リレーなど）でサブインターフェイスがサポートされます。サブインターフェイスは仮想インターフェイスであり、物理ハードウェア インターフェイスと関連付けられます。各サブインターフェイスを設定し、別のネットワークをサポートできます。このためサブインターフェイスによって、1 つの物理インターフェイスが複数のネットワークをサポートできるようになります。

Cisco ルータでインターフェイスを設定する詳細情報については、次の URL にある『*Cisco IOS Interface Configuration Guide*』を参照してください。

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

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。**interface** コマンドを使用するには、次の手順を実行します。

ステップ 1　特権 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　**interface** コマンドを入力します。インターフェイス タイプ、スロット番号、ポート番号を指定し、設定するインターフェイスを特定します。たとえばスロット 5 に搭載されているファスト イーサネット カードのポート 5（ファスト イーサネット ポート 5/5）にインターフェイスを設定するには、次のように入力します。

```
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。たとえば、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 3　**interface** コマンドに続いて適切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、インターフェイスを設定します。このインターフェイス コンフィギュレーション コマンドでは、インターフェイスで実行するプロトコルおよびアプリケーションを定義します。**interface** コマンドを再度入力するか、Ctrl キーを押した状態で Z キーを押してインターフェイス コンフィギュレーション モードを終了するまで、これらのコマンドは収集されて **interface** コマンドに適用されます。

（注）　**show interfaces** EXEC コマンドを使用すると、ルータのインターフェイスの一覧を表示できます。

show hardware EXEC コマンドを使用すると、システム ソフトウェアおよびハードウェアの一覧を表示できます。

ステップ 4　インターフェイスを設定したあとで、「インターフェイスのモニタおよびメンテナンス」（P.8-15）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できます。

インターフェイス範囲の設定

インターフェイス範囲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。インターフェイス範囲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ときは、以下に注意してください。

- マクロの詳細については、「インターフェイス範囲マクロの定義および使用」（P.8-4）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を入力する必要はありません。
- **interface range** コマンドを使用する場合、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はありません。
- **no interface range** コマンドでは VLAN インターフェイスがサポートされます。

（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、対象となる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)#
```

インターフェイス範囲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（インターフェイス範囲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範囲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るのを待ってから、インターフェイス範囲コンフィギュレーション モードを終了してください。

インターフェイス範囲マクロの定義および使用

インターフェイス範囲マクロを定義して、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** コマンドで **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。

インターフェイス範囲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*}]	インターフェイス範囲マクロを定義して、NVRAM 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、インターフェイス範囲マクロ 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範囲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範囲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範囲マクロ 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範囲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範囲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、インターフェイス範囲マクロ enet_list を使用して、インターフェイス範囲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」（P.8-5）
- 「ジャンボ フレーム サポートの設定」（P.8-9）
- 「IEEE 802.3X フロー制御の設定」（P.8-12）
- 「ポート デバウンス タイマーの設定」（P.8-13）
- 「インターフェイスに関する記述の追加」（P.8-14）

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 モード設定上のガイドライン」（P.8-6）
- 「イーサネット インターフェイス速度の設定」（P.8-6）
- 「インターフェイスのデュプレックス モードの設定」（P.8-7）
- 「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」（P.8-7）
- 「速度およびデュプレックス モードの設定の表示」（P.8-8）

速度およびデュプレックス モード設定上のガイドライン

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、Cisco 7600 シリーズ ルータが、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、ルータ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、ルータは自動的に、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、1000 Mbps 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、ポートにデュプレックス モードを設定するように求めるルータプロンプトが表示されます。

（注） Cisco 7600 シリーズ ルータは、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、再設定時に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）。

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、以下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 8-1 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のリンク ステータスを示します。

表 8-1　リンク ネゴシエーションの設定および可能なリンク 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
Off	Off	アップ	アップ
On	On	アップ	アップ
Off	On	アップ	ダウン
On	Off	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 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 サポートの概要」（P.8-9）
- 「MTU サイズの設定」（P.8-11）

注意　次のスイッチング モジュールは、8092 バイトの最大入力フレーム サイズをサポートします。

- WS-X6516-GE-TX（100 Mbps で動作する場合）
- 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 サポートが設定されている場合、上記モジュールは 8092 バイトを超える入力フレームをドロップします。

（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 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 サポートの概要」（P.8-9）
- 「イーサネット ポート」（P.8-10）
- 「VLAN インターフェイス」（P.8-11）

ジャンボ フレーム 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も大きい最大伝送単位（MTU）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、MSFC 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、サイズを超えているトラフィックがドロップされます。グローバルな LAN ポートの MTU サイズを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.8-12）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 バイトよりも大きい場合に、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。

ポリシー フィーチャ カード（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、PFC 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 はトラフィックをドロップします。

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 バイトよりも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、サイズを超えているトラフィックがドロップされます。グローバルな LAN ポートの MTU サイズを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.8-12）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」（P.8-10）
- 「レイヤ 3 イーサネット ポート」（P.8-11）
- 「レイヤ 2 イーサネット ポート」（P.8-11）

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、入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 バイトよりも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 バイトよりも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.8-12）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 サイズだけを設定できます（「グローバルな出力 LAN ポート MTU サイズの設定」（P.8-12）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.8-11）
- 「グローバルな出力 LAN ポート MTU サイズの設定」（P.8-12）

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（1500 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 サイズを設定するときは、以下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 ～ 9216 バイトです。

- レイヤ 2 イーサネット ポートについては、グローバルな出力 LAN ポート MTU サイズだけ設定可能です（「グローバルな出力 LAN ポート MTU サイズの設定」（P.8-12）を参照）。

次に、ギガビット イーサネット ポート 1/2 に 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（9216 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

Cisco 7600 シリーズ ルータ上のギガビット 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、他のデバイスから 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ときは、以下に注意してください。

- 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。
- 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 ポートを設定します。
- **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ギガビット イーサネット 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ギガビット イーサネット ポートが設定されます。
- ポーズ フレームの送信を設定する場合は、次の情報に注意してください。
  - 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 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。ポート デバウンス タイマーは、各 LAN ポートに、個別に設定できます。

注意　ポート デバウンス タイマーをイネーブルにすると、リンクアップ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**

ポートにデバウンス タイマーを設定する場合、次の点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 ポートでだけサポートされています。
- 銅製メディア上で 1000Mpbs で動作するポートでは、ポート デバウンス タイマー値を 5000 ミリ秒まで 100 ミリ秒単位で増やすことができます。
- WS-X6502-10GE はサポートされません。
- ファイバ メディアと銅製メディアの両方が、10Gbps ポートでサポートされます。
- メディアだけの変更が検出されます。

表 8-2 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 8-2　ポート デバウンス タイマー遅延時間

ポートの種類	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 Mpbs または 100 Mbps で動作するポート	300 ミリ秒	3100 ミリ秒
銅製メディア上で 1000 Mpbs または 10 Gbps で動作するポート	300 ミリ秒	3100 ミリ秒
WS-X6502-10GE 以外の光ファイバ メディア上で 1000 Mpbs または 10 Gbps で動作するポート	10 ミリ秒	100 ミリ秒
WS-X6502-10GE 10 ギガビット ポート	1000 ミリ秒	3100 ミリ秒

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記述の追加

インターフェイスの機能に関する記述を追加できます。記述は、**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記述を追加するには、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記述を追加します。
`Router(config-if)# no description`	インターフェイスから記述を削除します。

次に、ファスト イーサネット ポート 5/5 に関する記述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"
```

活性挿抜の概要

Cisco 7600 シリーズ ルータでは活性挿抜（OIR）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、『*Cisco 7600 Series Router 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、Cisco 7600 シリーズ ルータ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。

ルータ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の設定は 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、ルータはこのモジュールをオンラインにしません。

レイヤ 2 MAC アドレスは EEPROM 上に保存され、システムでスイッチング 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、取り付けられた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

Cisco 7600 シリーズ ルータでインターフェイスのモニタおよびメンテナンスを行うコマンドは次のとおりです。

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**	現在のルーティング情報フィールド（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。

コマンド	目的
`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。
`Router(config)# interface type slot/port` `Router(config-if)# shutdown`	指定インターフェイスをシャットダウンします。インターフェイスのすべての機能はディセーブルになり、インターフェイスは使用不可として表示されます。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。
`Router(config)# interface type slot/port` `Router(config-if)# no shutdown`	シャットダウンされたインターフェイスをイネーブルにします。
`Router# clear counters [{type[1] slot/port} | {vlan vlan_ID} | {port-channel channel_ID}]`	インターフェイス カウンタをクリアします。任意のインターフェイス タイプを指定しない場合は、指定インターフェイスのすべての現行カウンタがクリアされます。 **（注）** このコマンドでは、SNMP 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。
`Router# clear interface type1 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**

（注）

- コマンド構文および使用法の詳細については、次の URL にある『*Cisco 7600 Series Cisco IOS Command Reference*』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- Cisco ルータでインターフェイスのモニタとメンテナンスを行う方法については、次の URL にある『*Cisco IOS Interface Configuration Guide*, Release 12.2』を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/finter_c.html

TDR を使用したケーブル ステータスの確認

タイム ドメイン リフレクトメータ（TDR）を使用して、銅製ケーブルのステータスを確認できます。TDR はケーブルを介して信号を送信し、反射され戻ってきた信号を読み取ることで、ケーブル障害を検出します。信号のすべてまたは一部は、ケーブル不良の数によって、またはケーブルの終端によって反射されて戻ってきます。

TDR を使用して、リンクを確立できない場合にケーブル配置に障害が発生しているかどうかを判断します。特に既存のルータを交換する、ギガビット イーサネットにアップグレードする、または新しいケーブルを敷く場合に、このテストは重要です。

TDR テストを実行する前に、ポートはアップである必要があります。ポートがダウンしている場合、**test cable-diagnostics tdr** コマンドを入力できず、次の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 では、最大で 115 m の長さ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中止するには、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中止します。

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 9

Supervisor Engine 32 の設定

この章では、Cisco 7600 シリーズ ルータに搭載された 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。

- 「Supervisor Engine 32 のフラッシュ メモリ」（P.9-1）
- 「Supervisor Engine 32 ポート」（P.9-2）

（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 7600 Series Routers Command References』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- Cisco IOS ソフトウェアを使用する場合、Supervisor Engine 32 メモリの最低要件は次のとおりです。
  - 512 MB DRAM（Supervisor Engine 32 上）
  - 512 MB DRAM（MSFC2A 上）
- Supervisor Engine 32 は、WS-6503 シャーシおよび WS-6503-E（3 スロット）シャーシでサポートされますが、Cisco 7603 シャーシではサポートされません。
- 4 スロットのシャーシの場合、Supervisor Engine 32 はスロット 1 またはスロット 2 のいずれかに搭載します。
- 6 スロットまたは 9 スロットのシャーシの場合、Supervisor Engine 32 はスロット 5 またはスロット 6 のいずれかに搭載します。
- 13 スロットのシャーシの場合、Supervisor Engine 32 はスロット 7 またはスロット 8 のいずれかに搭載します。
- Supervisor Engine 32 には PFC3B があり、PFC3B モードで動作します。
- Supervisor Engine 32 では、スイッチ ファブリック接続がサポートされません。
- Supervisor Engine 32 でサポートされているハードウェア機能とソフトウェア機能については、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/ios/12_2sr/release/notes/122SRrn.html#wp4769974

Supervisor Engine 32 のフラッシュ メモリ

Supervisor Engine 32 には以下が含まれます。

- **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:** : 256MB の内部 CompactFlash フラッシュ メモリ（ROMMON からは **bootdisk:**）

リリース 12.2SRB およびそれ以降を実行するには、両方の Sup32 モジュールにおいて、最小で 128 MB ブートフラッシュが必要です。512 MB のブートフラッシュが搭載された CompactFlash（CF）アダプタは、リリース 12.2(18)SXF およびそれ以降のリリースの Sup32 モジュールで使用できます。注文の場合は、Cisco Part Number CF-ADAPTER= を使用してください。

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 2 つの Universal Serial Bus（USB）2.0 ポートもあり、現在はイネーブルになっていません。

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 は 10/100/1000 Mbps RJ-45 ポートです。

WS-SUP32-10GE ポート 1 および 2 は XENPAK を受信する 10 ギガビット イーサネット ポートで、ポート 3 は 10/100/1000 Mbps RJ-45 ポートです。

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、コマンドライン インターフェイス（CLI）を使用して、Cisco 7600 シリーズ ルータ上でレイヤ 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 ポートを設定する方法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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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。

この章の内容は、次のとおりです。

- 「レイヤ 2 スイッチングの機能概要」（P.10-1）
- 「レイヤ 2 LAN インターフェイスのデフォルト設定」（P.10-5）
- 「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」（P.10-5）
- 「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.10-6）

レイヤ 2 スイッチングの機能概要

ここでは、Cisco 7600 シリーズ ルータにおけるレイヤ 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」（P.10-1）
- 「VLAN トランクの概要」（P.10-3）
- 「レイヤ 2 LAN ポート モード」（P.10-4）

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」（P.10-2）
- 「セグメント間のフレーム スイッチング」（P.10-2）

- 「アドレス テーブルの作成」（P.10-2）

レイヤ 2 イーサネット スイッチングの概要

Cisco 7600 シリーズ ルータは、レイヤ 2 イーサネット セグメント間での同時パラレル接続をサポートします。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。

Cisco 7600 シリーズ ルータは、高帯域のデバイスおよび多数のユーザに起因する輻輳問題を解決するために、デバイス（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 ネットワークに重大な輻輳を引き起こしていますが、有効な解決策の 1 つは全二重通信です。イーサネットは通常、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。パケットを双方向に同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。

セグメント間のフレーム スイッチング

Cisco 7600 シリーズ ルータ上の各 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デバイスが、ネットワークの帯域幅を共有します。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、ルータは各 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、ルータは、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、ルータはアドレス テーブルを維持します。フレームがルータに着信すると、ルータは送信元ネットワーク デバイスの MAC アドレスと、フレームを受信した LAN ポートを対応付けます。

アドレス テーブルの作成

Cisco 7600 シリーズ ルータは、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ルータが受信すると、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、ルータ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。ルータは以後、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。ルータ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、Cisco 7600 シリーズ ルータ上での 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.10-3）

トランキングの概要

（注）　VLAN の詳細については、第 14 章「VLAN の設定」を参照してください。

トランクとはルータとその他のネットワーキング デバイス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。

- スイッチ間リンク（ISL）：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.10-4）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 インターフェイスの設定はできません。

Dynamic Trunking Protocol（DTP）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、ISL および 802.1Q の両方のトランクで自動ネゴシエーションをサポートしています。

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「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）　一部のモジュールでは ISL カプセル化をサポートしません（「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 ポートがネイバー LAN ポートとネゴシエーションを行い、ネイバー 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。ネイバー 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。ネイバー 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。ネイバー 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。ネイバー 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、ネイバー 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 デバイスによっては、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 をサポートしないデバイスに接続されている 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 をサポートしないデバイス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
スパニングツリー プロトコル（STP）	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 • 1000 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 ポートの設定時には、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、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 Cisco 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 と反対側の端のネイティブ 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 Cisco 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 BPDU 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 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 トポロジーを定義するスパニングツリーのインスタンス（Mono Spanning Tree（MST））が 1 つしか維持されません。802.1Q トランクを介してシスコ製ルータを他社製のルータに接続すると、他社製ルータの MST とシスコ製ルータのネイティブ 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 トポロジーが形成されます。
  - Cisco 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 Cisco 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、Cisco 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 トポロジーを維持できます。Cisco 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。
  - Cisco 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 Cisco 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、Cisco スイッチを他社製の 802.1Q クラウドに接続できません。このように接続すると、ルータは ISL トランク ポートまたはアクセス ポートのスパニングツリー ポート ステートを「矛盾する」状態にし、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、Cisco 7600 シリーズ ルータにおけるレイヤ 2 スイッチングの設定手順について説明します。

- 「レイヤ 2 スイッチング用の LAN ポートの設定」（P.10-7）
- 「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.10-8）

- 「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.10-13）
- 「カスタム IEEE 802.1Q EtherType フィールド値の設定」（P.10-15）

（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。ネイバー 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。ネイバー 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）。

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」（P.10-8）
- 「DTP を使用するためのレイヤ 2 トランクの設定」（P.10-9）
- 「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.10-9）
- 「アクセス VLAN の設定」（P.10-10）
- 「802.1Q ネイティブ VLAN の設定」（P.10-10）
- 「トランク上で許容される VLAN のリストの設定」（P.10-11）
- 「プルーニング適格 VLAN のリストの設定」（P.10-11）
- 「トランクの設定の完了」（P.10-12）
- 「レイヤ 2 トランクの設定の確認」（P.10-12）
- 「設定および確認の例」（P.10-12）

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.10-7）の手順を実行します。
- キーワードを指定せずに **switchport** コマンドを入力する場合（前述のステップ 3）、デフォルト モードは **switchport mode dynamic desirable** および **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場合、次の点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.10-9）を参照）は、**switchport trunk encapsulation negotiate** コマンドと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、カプセル化または 802.1Q 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.10-12）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.10-7）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.10-4）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.10-12）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.10-7）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、次の点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.10-8）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.10-4）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.10-8）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.10-9）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.10-12）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.10-7）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.10-12）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.10-7）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、次の点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.10-12）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.10-7）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 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）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）、VLAN トランキング プロトコル（VTP）、ポート集約プロトコル（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.10-12）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.10-7）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.13-5）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（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 トランスペアレント モードのネットワーク デバイスは、VTP Join メッセージを送信しません。VTP トランスペアレント モードのネットワーク デバイスにトランク接続されている Cisco 7600 シリーズ ルータでは、トランスペアレント モードのネットワーク デバイス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スペアレント モードのネットワーク デバイス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.10-12）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、ネイバー 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

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 デバイス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 フィールド値の設定時には、以下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 デバイスすべてがカスタム 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 のメンバー 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では、カスタム EtherType フィールド値を設定できません。
- ポートごとに、EtherType フィールド値 1 つだけをサポートします。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。
- カスタム IEEE802.1Q EtherType フィールド値をサポートするモジュールの一覧については、『*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。

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。

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、Cisco 7600 シリーズ ルータに Flex Link 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「Flex Link の概要」（P.11-1）
- 「Flex Link の設定」（P.11-2）
- 「モニタリング :Flex Link」（P.11-4）

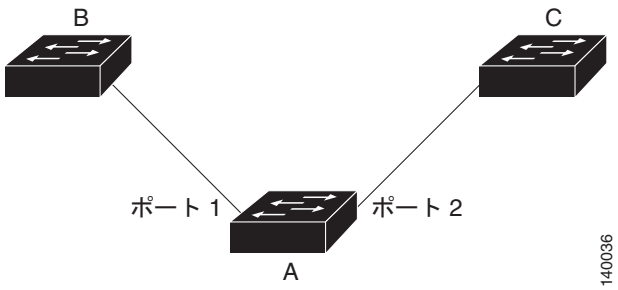
Flex Link の概要

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）のペアであり、片方のインターフェイスが他方のバックアップとして動作するように設定されています。Flex Link は、カスタマーが STP を実行しないサービス プロバイダー ネットワークまたは企業ネットワークで一般的に設定します。Flex Link では、スパニングツリー プロトコル（STP）の代替手段であるリンクレベルの冗長性が提供されます。Flex Link インターフェイスでは、STP が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、プライマリにするリンクのスタンバイ リンクとして、1 つのレイヤ 2 インターフェイスを設定します。インターフェイスのペアに Flex Link を設定すると、片方のインターフェイスだけがリンクアップ状態になり、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されると、スタンバイ リンクがトラフィックの転送を始めます。アクティブでないリンクがアップに戻ると、そのリンクはスタンバイ モードになります。

図 11-1 では、ルータ A のポート 1 およびポート 2 が、アップリンク ルータ B および C に接続されています。これは Flex Link として設定されているので、片方のインターフェイスだけがトラフィックを転送し、他方のインターフェイスはスタンバイ モードになります。ポート 1 がアクティブ リンクである場合は、ポート 1 がポート 1 とルータ B の間でトラフィックの転送を始めます。ポート 2（バックアップ リンク）とルータ C の間のリンクはトラフィックを転送しません。ポート 1 がダウンすると、ポート 2 がアップし、ルータ C へのトラフィックの転送を始めます。ポート 1 は、アップに戻るとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィックの転送を続けます。

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、トラップによってネットワーク管理ステーションが通知を受けます。スタンバイ リンクがダウンすると、トラップによってユーザが通知を受けます。

Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

Flex Link の設定

ここでは、次の設定について説明します。

- 「Flex Link のデフォルト設定」（P.11-2）
- 「Flex Link 設定時の注意事項および制約事項」（P.11-2）
- 「Flex Link の設定」（P.11-3）

Flex Link のデフォルト設定

Flex Link はデフォルトでは設定されていません。

Flex Link 設定時の注意事項および制約事項

Flex Link を設定する場合は、次の注意事項と制約事項に従ってください。

- アクティブ リンクには、Flex Link バックアップ リンクを 1 つだけ設定できます。バックアップ リンクは、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にする必要があります。
- インターフェイスは 1 つの Flex Link ペアだけに属します。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは、別の Flex Link ペアに属することができません。
- どちらのリンクも、EtherChannel に属するポートには設定できません。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、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。

- バックアップ リンクを、アクティブ リンクと同じタイプにする必要はありません（ファスト イーサネット、ギガビット イーサネット、ポート チャネルのいずれか）。ただし同様の特性で両方の Flex Link を設定し、スタンバイ リンクがアクティブになった場合に、操作のループや変更が発生しないようにする必要があります。
- Flex Link ポートでは STP がディセーブルになります。ルータで STP をディセーブルにする場合は、ネットワーク トポロジにレイヤ 2 ループがないことを確認してください。
- Flex Link ポート、またはそのリンクの接続先ポートでは、STP 機能（PortFast、BPDU ガードなど）を設定しないでください。

Flex Link の設定

Flex Link 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(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）ルータ スタートアップ コンフィギュレーション ファイルに設定を保存します。

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

（注）　**switchport backup interface** コマンドを使用してスイッチポート インターフェイスを設定し、バックアップ インターフェイスにトラフィックを渡す場合、入力カウンタはバックアップ インターフェイスで増加しますが、実際のトラフィックはそのインターフェイスを通過しません。

次に、バックアップ インターフェイスでインターフェイスを設定して、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
```

モニタリング :Flex Link

表 11-1 に、Flex Link 設定をモニタするための特権 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、ルータに設定されているすべての Flex Link、およびアクティブ インターフェイスとバックアップ インターフェイスのそれぞれの状態（アップ モードまたはスタンバイ 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、Cisco 7600 シリーズ ルータのレイヤ 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「EtherChannel の機能概要」（P.12-1）
- 「EtherChannel 機能の設定時の注意事項および制約事項」（P.12-6）
- 「EtherChannel の設定」（P.12-8）

EtherChannel の機能概要

ここでは、EtherChannel の機能概要について説明します。

- 「EtherChannel 機能の概要」（P.12-1）
- 「EtherChannel の設定方法の概要」（P.12-2）
- 「LACP 1:1 冗長性機能の概要」（P.12-5）
- 「ポートチャネル インターフェイスの概要」（P.12-5）
- 「ロード バランシングの概要」（P.12-6）

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。

Cisco 7600 シリーズ ルータは、最大 128 個の EtherChannel をサポートします。

Cisco 7600 シリーズ ルータ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）　Cisco 7600 シリーズ ルータに接続するネットワーク デバイスによって、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 機能はルータ、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 の設定方法の概要

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」（P.12-2）
- 「EtherChannel の手動設定の概要」（P.12-3）
- 「PAgP による EtherChannel 設定」（P.12-3）
- 「IEEE 802.3ad LACP EtherChannel 設定の概要」（P.12-4）

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）またはリンク集約制御プロトコル（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 デバイス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 で定義されています。

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。

表 12-1 に、ユーザ設定可能な 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だけ、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。
auto	（PAgP のデフォルト）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
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。

表 12-1　EtherChannel のモード （続き）

モード	説明
passive	（LACP のデフォルト）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
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 の手動設定の概要

手動で設定された 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、EtherChannel 内のすべてのポート設定に互換性がある場合だけです。

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 グループの機能を動的に「学習」して、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。その後、その EtherChannel が単一のブリッジ ポートとしてスパニングツリーに追加されます。

PAgP は、**auto** モードおよび **desirable** モードでの両方で LAN ポート間のネゴシエーションを行い、ポート速度、トランキング ステートなどの基準に基づいて LAN ポートが 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、モード間で互換性がある限り、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。

表 12-2 ではこれらの組み合わせの概要について説明しています。

表 12-2　PaGP EtherChannel モード

ルータ A	ルータ B	結果
auto モード	**auto** モード	EtherChannel グループは作成されません。
auto モード	**desirable** モード	EtherChannel グループが作成されます。

表 12-2　PaGP EtherChannel モード（続き）

ルータ A	ルータ B	結果
desirable モード	**auto** モード	EtherChannel グループが作成されます。
desirable モード	**desirable** モード	EtherChannel グループが作成されます。

IEEE 802.3ad LACP EtherChannel 設定の概要

LACP では、LAN ポート間で LACP パケットを交換することによって、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** 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 グループの機能を動的に「学習」して、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、それらのリンクを 1 つの EtherChannel としてまとめます。その後、その EtherChannel が単一のブリッジ 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、モード間で互換性がある限り、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。

表 12-3 ではこれらの組み合わせの概要について説明しています。

表 12-3　LACP EtherChannel モード

ルータ A	ルータ B	結果
passive モード	**passive** モード	EtherChannel グループは作成されません。
passive モード	**active** モード	EtherChannel グループが作成されます。
active モード	**passive** モード	EtherChannel グループが作成されます。
active モード	**active** モード	EtherChannel グループが作成されます。

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 が稼働するルータごとに、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、またはコマンドライン インターフェイス（CLI）から設定できます（「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 プライオリティとともにルータの MAC アドレスを使用して、システム ID を形成します。他のシステムとのネゴシエーション時も同様です。

（注）　LACP のシステム ID は、LACP システム プライオリティ値とルータの 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 から設定できます（「チャネル グループの設定」（P.12-9）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。

（注）　ポート プライオリティは、デバイス上でピアより高い LACP システム プライオリティで設定されている場合にだけ有効です。

- 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。管理用のキーは、ポートが他のポートと集約できる能力を定義します。他のポートとの集約を行うポートの能力は、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や共有メディアなどのポートの物理特性
  - ユーザによる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だけ使用されます。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）。

LACP 1:1 冗長性機能の概要

リリース 12.2(33)SRC 以降では、LACP 1:1 冗長性機能によって、ホットスタンバイ リンクへのファスト スイッチオーバーとアクティブ リンク 1 つによって EtherChannel が設定されます。

LACP 1:1 冗長性機能を使用するには、2 つのポート（アクティブ 1 つとスタンバイ 1 つ）を使用して LACP EtherChannel を設定します。アクティブ リンクがダウンしても、EtherChannel はアップしたままで、システムはホットスタンバイ リンクへのファスト スイッチオーバーを実行します。ダウンしたリンクが再度動作可能になると、EtherChannel がもう 1 度ファスト スイッチオーバーを実行して元のアクティブ リンクに戻します。

LACP 1:1 冗長性機能（特にファスト スイッチオーバー機能）が正しく機能するには、リンクの両端でこの機能がイネーブル化されている必要があります。

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。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、スパニングツリー プロトコル（STP）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といった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 のロードバランスには、MAC アドレスまたは IP アドレスを使用できます。EtherChannel のロードバランスにはレイヤ 4 ポート番号も使用できます。EtherChannel のロードバランスには、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、ルータ上で設定されているすべての EtherChannel に適用されます。EtherChannel のロードバランスは、MPLS レイヤ 2 情報を使用します。

使用する設定で最多の種類のバランス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 アドレスにだけ送信され、かつ EtherChannel ロードバランスの基準として宛先 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、ロードバランス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、Cisco 7600 シリーズ ルータのすべての LAN ポートに対して使用できます。
- 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。
- 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。
- Inter-Switch Link Protocol（ISL; スイッチ間リンク）トランキングをサポートしないメンバー ポートを EtherChannel に追加すると、Cisco IOS ソフトウェアは、**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自動的に追加し、EtherChannel が ISL トランクとして設定されないようにします。EtherChannel がトランクでない場合、**switchport trunk encapsulation dot1q** コマンドは非アクティブです。
- 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 プロトコルの実行はできません。
- 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 のすべての LAN ポートをイネーブルにしてください。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 つがスイッチド ポート アナライザ（SPAN）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。複数の STP ポート パス コストを設定した場合でも、LAN ポートは EtherChannel の形成との互換性があります。
  - 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。
- 1 ～ 256 の番号のポートチャネル インターフェイスを最大 256 個設定できます。
- 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）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、完全プライオリティ キューのあるポートと完全プライオリティ キューのないポートを持つ EtherChannel をサポートします。

（注）　**mls qos channel-consistency** コマンドがディセーブルの場合は、他のファミリに属するカードからポートを設定します。この条件は、ポートチャネルに設定されたターゲット、およびポートチャネルのメンバー リンクのいずれにも QoS 適用されていない場合のみ有効です。

- ES20 と ES+ の相互バンドルはサポートされていません。また、特定の LAN カードと ES20/ES+ の相互バンドルもサポートされていません。
- EtherChannel は、次ではサポートされません。
  - Cisco 7600 SIP-400
  - Cisco 7600 SIP-200 の FastEthernet SPA

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.12-8）
- 「チャネル グループの設定」（P.12-9）
- 「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）
- 「EtherChannel ロード バランシングの設定」（P.12-12）
- 「EtherChannel Min-Links 機能の設定」（P.12-12）
- 「ファスト スイッチオーバーでの LACP 1:1 冗長性機能の設定」（P.12-13）

（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 を設定する場合、ここで説明する作業は行わないでください（「チャネル グループの設定」（P.12-9）を参照）。
- レイヤ 3 EtherChannel を設定する場合、ここで説明する手順に従って、ポートチャネル論理インターフェイスを手動で作成し、さらにレイヤ 3 LAN ポートをチャネル グループに含める必要があります（「チャネル グループの設定」（P.12-9）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、インターフェイス 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 port-channel number`	ポートチャネル インターフェイスを作成します。
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。 *group_number* : 1 ～ 256 で、最大 128 個のインターフェイスを作成可能

次に、インターフェイス port-channel 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、インターフェイス Port-channel 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、先に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 EtherChannel のポートチャネル論理インターフェイスの設定」（P.12-8）を参照）、そのあとでレイヤ 3 LAN ポートをここで説明する手順に従ってチャネル グループに含める必要があります。
- 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、インターフェイス コンフィギュレーション モードで 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 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。
ステップ 4	`Router(config-if)# channel-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.12-2）を参照）。PAgP は、auto および desirable モードだけをサポートします。LACP は、active および passive モードだけをサポートします。
ステップ 5	`Router(config-if)# lacp port-priority priority_value`	（任意：LACP 用）有効な値は 1 ～ 65535 です。値が大きいほど、プライオリティは低くなります。デフォルトは 32768 です。

	コマンド	目的
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 slot/port* `Router# show interfaces` *type slot/port* **etherchannel**	設定を確認します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、**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、「インターフェイス範囲の設定」（P.8-3）を参照してください。

次に、インターフェイス Port-channel 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 Interface
Fa5/2     d     U1/S1           1s       0        128        Any      0 5/2

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、インターフェイス port-channel 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ルータの 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、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実行します。

	コマンド	目的
ステップ 1	`Router(config)# lacp system-priority` *priority_value*	（LACP で任意）有効な値は 1 ～ 65535 です。値が大きいほど、プライオリティは低くなります。デフォルトは 32768 です。
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、次にルータの 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 ロードバランスを設定するには、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)# 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 ロードバランスを設定します。ロードバランス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 • **src-dst-ip**：送信元および宛先の IP アドレス • **src-dst-mac**：送信元および宛先の MAC アドレス • **src-dst-port**：送信元および宛先のレイヤ 4 ポート • **src-ip**：送信元の IP アドレス • **src-mac**：送信元の MAC アドレス • **src-port**：送信元のレイヤ 4 ポート
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 etherchannel load-balance`	設定を確認します。

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

EtherChannel Min-Links 機能は LACP EtherChannel でサポートされます。この機能では、ポート チャネル インターフェイスがリンクアップ状態に移行するために、リンクアップ状態になって EtherChannel でバンドルされている必要があるメンバー ポートの最低数を設定できます。

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 LACP EtherChannel にアクティブ メンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

EtherChannel Min-Links 機能を設定するには、インターフェイス 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 port-channel 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`	ポート チャネル インターフェイスがリンクアップ状態に移行するために、リンクアップ状態になって EtherChannel でバンドルされている必要があるメンバー ポートの最低数を設定します。デフォルト値は 1 です。
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 slot/port` `Router# show interfaces type slot/port etherchannel`	設定を確認します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**

（注）　EtherChannel Min-Links 機能は、EtherChannel の一端だけで設定しても正しく動作しますが、結果を最適にするには、EtherChannel の両端で同じ数の最低リンクを設定してください。

次に、EtherChannel でアクティブなメンバー ポートが 2 個より少ない場合に、ポートチャネル インターフェイス 1 が非アクティブになるよう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
```

ファスト スイッチオーバーでの LACP 1:1 冗長性機能の設定

LACP 1:1 冗長性機能のためには、LACP EtherChannel に 2 つのリンクが必要です。アクティブになるのはそのうちの一方だけです。ポート プライオリティ値が小さい（つまり、プライオリティの高い）方のリンクがアクティブ リンクになり、もう一方のリンクはホット スタンバイ ステートになります。LACP の max-bundle は 1 に設定する必要があります。

LACP 1:1 冗長性機能を設定するには、インターフェイス 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 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)# lacp fast-switchover`	この EtherChannel のファスト スイッチオーバー機能をイネーブルにします。
ステップ 3	`Router(config-if)# lacp max-bundle 1`	アクティブなメンバー ポートの最大数を 1 に設定します。

	コマンド	目的
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-config interface port-channel group_number` `Router# show interfaces type slot/port etherchannel`	設定を確認します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**

（注） LACP 1:1 冗長性機能（特に高速スイッチオーバー機能）が正しく機能するためには、EtherChannel の両方の端で機能をイネーブルにしておく必要があります。

この例は、1:1 冗長性機能を備えた LACP EtherChannel を設定する方法を示しています。ファストイーサネット ポート 5/6 は、デフォルトの 32768 より大きいポート プライオリティ番号（つまり、低いプライオリティ）で設定されるため、スタンバイ ポートになります。

```
Router# configure terminal
Router(config)# lacp system-priority 33000
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group 1 mode active
Router(config)# interface fastethernet 5/6
Router(config-if)# lacp port-priority 33000
Router(config)# interface port-channel 1
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# end
```

CHAPTER 13

VTP の設定

この章では、Cisco 7600 シリーズ ルータに VLAN トランキング プロトコル（VTP）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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.13-1）
- 「VTP のデフォルト設定」（P.13-6）
- 「VTP 設定時の注意事項および制約事項」（P.13-7）
- 「VTP の設定」（P.13-8）

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 VLAN 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 デバイスで構成されます。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 デバイス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 デバイス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「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」（P.13-2）
- 「VTP モードの概要」（P.13-2）
- 「VTP アドバタイズの概要」（P.13-3）
- 「VTP バージョンの概要」（P.13-3）

- 「VTP プルーニングの概要」（P.13-5）

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 デバイスで構成されます。1 つのネットワーク デバイスが所属できる 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、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）を使用します。

デフォルトでは、Cisco 7600 シリーズ ルータは VTP サーバ モードであり、ルータでトランク 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。

ルータが、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。ルータは、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。

ルータを VTP トランスペアレントとして設定した場合、VLAN の作成および変更は可能ですが、その変更が作用するのは個々のルータに限られます。

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 デバイスに伝播されます。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デバイスを管理するための作業負担が大幅に軽減されます。

VTP 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 Cisco 7600 シリーズ ルータを設定できます。

- 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 デバイスに、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 デバイスと同期化します。VTP サーバがデフォルトのモードです。

（注）　VTP バージョン 3 では、VLAN の操作はプライマリ サーバ上でのみ行われます。

- 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。
- トランスペアレント：VTP バージョン 1 では、VTP トランスペアレント ネットワーク デバイスは、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 および VTP バージョン 3 では、トランスペアレント ネットワーク デバイスは、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。
- オフ：VTP オフ モードでは、ネットワーク デバイス機能は、VTP 透過デバイスと同じ方法で動作します。ただし、VTP アドバタイズは転送されません。

（注）　Cisco 7600 シリーズ ルータは、Nonvolatile RAM（NVRAM; 不揮発性 RAM）に設定を書き込むときにルータ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、ルータを 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 デバイスは、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ネイバー ネットワーク デバイスは、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（ISL（スイッチ間リンク）および 802.1Q）
- エミュレート LAN 名（ATM LAN Emulation（LANE; LAN エミュレーション）用）
- IEEE 802.10 SAID（Security Association Identifier）の値（FDDI）
- VTP ドメイン名
- VTP 設定のリビジョン番号
- 各 VLAN の最大伝送単位（MTU）サイズを含めた VLAN 設定
- フレーム形式

VTP バージョンの概要

ネットワークで VTP を使用する場合は、VTP バージョン 1、2、またはバージョン 3 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 またはバージョン 3 を使用する必要があります。

VTP バージョン 2

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。

- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント ネットワーク デバイスは、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 メッセージをトランスペアレント モードで転送します。
- 整合性検査：VTP バージョン 2 の場合、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を介して新しい情報が入力された場合に限り、VLAN 整合性検査（VLAN 名、値など）を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの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 バージョン 3

バージョン 1 およびバージョン 2 でサポートされない次の機能が、VTP バージョン 3 でサポートされます。

- Hidden Password Support：VTP バージョン 3 では、パスワードを **hidden** または **secret** として設定するオプションがサポートされます。

  ドメインで takeover コマンドが発行される場合、**hidden** キーワードが指定されるときに、パスワードを再入力する必要があります。パスワード文字列から生成される秘密キーが、const_nvram:vlan.dat ファイルに保存されます。このオプションを使用して設定する場合、パスワードは、設定内では普通の文字列としては表示されません。代わりに、パスワードに関連付けられている秘密キーが、実行中の設定で 16 進数の形式で保存されます。**hidden** キーワードが指定されていない場合、VTP バージョン 1 および VTP バージョン 2 のように、const_nvram:vlan.dat にクリア テキストとして保存されます。

  secret キーワードが指定される場合、パスワードの秘密キーは直接設定できます。
- 拡張 VLAN データベース情報の引き継ぎ：VTP バージョン 2 では、VLAN 設定情報は、VLAN 番号 1 から 1000 だけに引き継がれます。VTP バージョン 3 では、情報は、VLAN 拡張範囲（VLAN 番号 1006 から 4094）にも引き継がれます。
- VTP バージョン 1、VTP バージョン 2、または VTP バージョン 3 が実行されている Cisco 7600 シリーズ ルータでは、デフォルトの VLAN 1 および 1002 から 1005 は変更できません。

（注） VTP プルーニングは、VLAN 番号 1 から 1000 だけに、引き続き適用されます。

- ドメインでのデータベースの引き継ぎ：VLAN データベース情報の引き継ぎに加え、VTP では、Multiple Spanning Tree（MST）プロトコル データベース情報も引き継がれます。
- VTP のディセーブル化：トランキング ポートで VTP がディセーブルになっているときには、そのポート上のすべての VTP インスタンスに適用されます。VTP がグローバルにディセーブル化されているときには、システム上のすべてのトランキング ポートに設定が適用されます。
- VTP バージョン 1 および VTP バージョン 2 では、VTP サーバの役割は、データベースを NVRAM にバックアップしすることと、管理者がデータベース情報を変更できるようにすることです。VTP バージョン 3 では、VTP プライマリ サーバと VTP セカンダリ サーバの役割が導入されました。VTP プライマリ サーバは、データベース情報をアップデートするために使用されます。アップデートの送信は、システム上のすべてのデバイスで受け取られます。VTP セカンダリ サーバは、VTP プライマリ サーバからのアップデートを介して受け取った VTP 設定を、その NVRAM にバックアップできます。

プライマリ サーバとセカンダリ サーバのステータスは、実行時のステータスで、設定オプションではありません。デフォルトでは、すべてのデバイスがセカンダリ サーバに割り当てられます。プライマリ サーバのステータスが必要になるのは、データベースのアップデートが必要な場合だけです。また、プライマリ サーバのステータスは、管理者がドメインから takeover メッセージを発行したときに取得されます（「テイクオーバーの起動」（P.13-13）を参照）。

プライマリ サーバ ステータスは、デバイスのリロードのときか、スイッチオーバー パラメータまたはドメイン パラメータが変更されるときに、失われます。セカンダリ サーバでは、設定がバックアップされ、その引き継ぎが継続されます。このため、プライマリ サーバなしで動作する VTP ドメインを存在させることができます。

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 デバイス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デバイスが 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デバイスについては、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 デバイス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、Cisco 7600 シリーズ ルータ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.13-10）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（「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.10-6）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

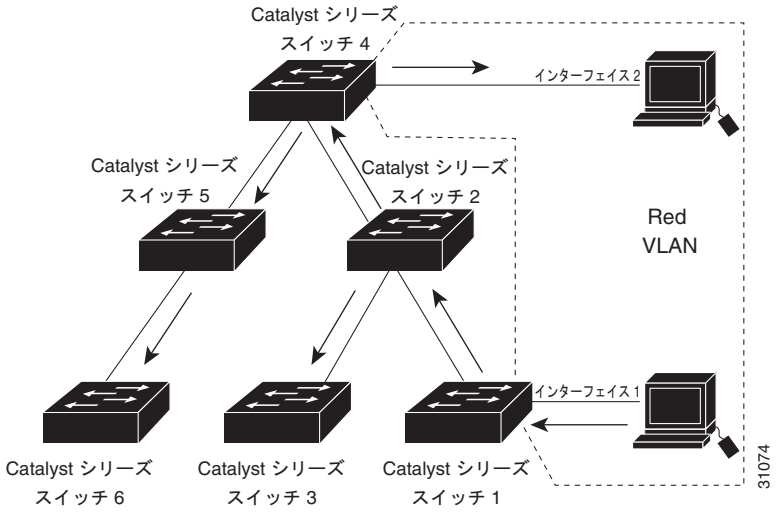
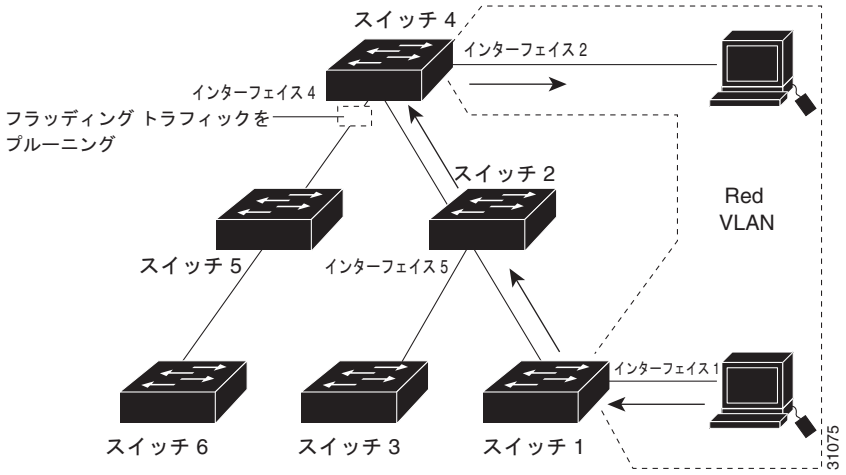


図 13-2 は、VTP プルーニングをイネーブルにした場合の同じスイッチド ネットワークを示しています。Red VLAN のトラフィックは指定されたリンク（スイッチ 2 のポート 5、スイッチ 4 のポート 4）でプルーニングされるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 3、5、6 には転送されません。

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イネーブルになります。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あり、VLAN 1 からのトラフィックをプルーニングできません。

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（「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.10-6）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作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブル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	（バージョン 1）
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

ネットワークで VTP を実装するときには、次の注意事項および制約事項に従ってください。

- 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 エンジンが搭載されたルータ上で、**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るには **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 デバイスで、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 デバイスにパスワードを設定する必要があります。

注意　VTP をセキュア モードで設定した場合、ドメイン内の各ネットワーク デバイスに管理ドメイン 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 デバイス上で 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 デバイスは、同一 VTP ドメイン内で VTP バージョン 1 が稼働しているネットワーク デバイス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 デバイスがバージョン 2 に対応する場合を除いて、ネットワーク デバイス上で 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 デバイス上で 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 デバイスで VTP バージョン 2 がイネーブルになります。
- トランク ポート上の VTP バージョン 3 デバイスで、VTP バージョン 2 デバイスからのメッセージを受信すると、その特定のトランク上の VLAN データベースのスケール ダウン バージョンを VTP バージョン 2 の形式で送信します。そのトランク上で VTP バージョン 2 パケットを最初に受信するときではない限り、VTP バージョン 3 デバイスでは、トランク ポート上で VTP バージョン 2 形式のパケットは送信されません。
- VTP バージョン 3 デバイスにより、トランク ポート上で VTP バージョン 2 デバイスが検出されると、VTP バージョン 3 パケットに加えて、さらに VTP バージョン 3 パケットが送信され続けます。これによって、トランク外に 2 種類のネイバーが混在できます。
- VTP バージョン 3 デバイスは、VPT バージョン 2 またはバージョン 1 のデバイスからは、設定情報を受け取りません。
- VPT バージョン 2 とは異なり、VTP をバージョン 3 に設定する場合、ドメインでは、VTP バージョン 3 システムとして動作を開始するために、すべてのデバイスがバージョン 3 として機能するよう設定されるわけではありません。
- バージョン 2 またはバージョン 3 の機能をサポートする VTP バージョン 1 デバイスで、VTP バージョン 3 パケットを受信するときには、VTP バージョン 2 の機能との矛盾が存在しない場合、デバイスは VTP バージョン 2 として設定されています。
- VTP バージョン 1 の機能だけをサポートするデバイスは、VTP バージョン 3 デバイスとは相互運用できません。
- 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 またはバージョン 3 をイネーブルにする必要があります。
- 2 つの VPT バージョン 3 の領域は、VTP バージョン 1 または VTP バージョン 2 の領域を介して、トランスペアレント モードでのみ通信が可能です。

- 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、ルータ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することはできません。
- 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、設定が有効なのは、そのルータ上の VLAN のプルーニングだけです。VTP ドメイン内のすべてのネットワーク デバイスに対して有効なわけではありません。
- VTP バージョン 1 とバージョン 2 では、VLAN 拡張範囲（VLAN 番号 1006 から 4094）の設定情報は引き継がれません。VLAN 拡張範囲は、各ネットワーク デバイスで手作業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 のモードはトランスペアレントに変わります。
- VTP トランスペアレント モードのネットワーク デバイスは、VTP Join メッセージを送信しません。VTP トランスペアレント モードのネットワーク デバイスにトランク接続されている Cisco 7600 シリーズ ルータでは、トランスペアレント モード ネットワーク デバイス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.10-11）を参照してください。
- VLAN データベースは、システム上で実行中の VTP バージョンに準拠する形式で、NVRAM ファイルに保存されます。VTP バージョン 2 だけをサポートする古いイメージでは、VTP バージョン 3 ファイル形式は認識されませんので、VTP がサポートされる新しいイメージからサポートされないイメージにシステムがダウングレードされた場合、NVRAM VLAN データベースの情報は失われます。

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」（P.13-8）
- 「VTP モードの設定」（P.13-11）
- 「テイクオーバーの起動」（P.13-13）
- 「VTP 統計情報の表示」（P.13-14）
- 「ドメインの VTP デバイスの表示」（P.13-14）

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。

- 「VTP パスワードの設定」（P.13-9）
- 「VTP プルーニングのイネーブル化」（P.13-10）
- 「VTP バージョン番号のイネーブル化」（P.13-10）

（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、次のコマンドを使用します。

コマンド	目的
Router(config)# **vtp password** *password_string* [**hidden** | **secret**]	VTP ドメインのパスワード（8 ～ 64 文字）を設定します。 VTP バージョン 3 では、**hidden** キーワードおよび **secret** キーワードを使用できます。 • **hidden** キーワードが使用される場合、パスワード文字列から生成される秘密キーが、const_nvram:vlan.dat ファイルに保存されます。takeover コマンドを使用された場合、パスワードを再入力する必要があります。 • **secret** キーワードが指定される場合、パスワードの秘密キーは直接設定できます。**secret** パスワードには、32 文字の 16 進数の文字列を含める必要があります。
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。

次に、**hidden** パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# vtp password WATER hidden
Generating the secret associated to the password.
Router(config)#
```

この例では、**hidden** キーワードを指定して設定したときに、パスワード WATER が表示される方法を示します。

```
Router# show vtp password
VTP Password: 89914640C8D90868B6A0D8103847A733
Router#
```

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、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)# 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。
ステップ 2	`Router# show vtp status | include pruning`	（任意）設定を確認します。

次に、VTP プルーニングを管理ドメイン内で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.10-11）を参照してください。

VTP バージョン番号のイネーブル化

VTP バージョン 2 対応のネットワーク デバイスでは、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。1 台のネットワーク デバイス上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべての VTP バージョン 2 対応ネットワーク デバイスでバージョン 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 デバイス上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのネットワーク デバイスで、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 デバイスがバージョン 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デバイス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 または VTP バージョン 3 をイネーブルにする必要があります。

VTP バージョン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** | **3**}	VTP バージョンをイネーブルにします。
ステップ 2	Router# **show vtp status** | **include** {**v1** | **v2** | **v3**}	（任意）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、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)# **vtp mode** {**client** | **server** | **transparent** | **off**}	VTP モードを設定します。
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。ルータが VTP ドメインにトランク接続されている場合、ルータはドメイン内の 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**	（任意）設定を確認します。

（注） VTP がディセーブルの場合は、VLAN データベース モードでなく、コンフィギュレーション モードで VLAN コンフィギュレーション コマンドを入力でき、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、ルータを VTP サーバとして設定する例を示します。

```
Router# configure 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、ルータを VTP クライアントとして設定する例を示します。

```
Router# configure terminal
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)# end
Router#
```

次に、ルータ上で VTP をディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Router(config)# end
Router#
```

次に、ルータ上で VTP と VTP アドバタイズメント転送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)# vtp mode off
Setting device to VTP OFF mode.
Router(config)# end
Router#
```

この例では、デバイスで VTP バージョン 1 を実行しているときの、VTP 設定パラメータの例を示しています。

```
Router# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : 0016.9c6d.5300
Configuration last modified by 127.0.0.12 at 10-18-07 10:12:42
Local updater ID is 127.00.12 at 10-18-07 10:2:42

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum number of existing VLANs : 5
Configuration Revision          : 1
MD5 digest                      : 0x92 0xF1 0xE8 0x52 0x2E ox5C 0x36 0x10 0x70 0x61 0xB8
                                0x24 0xB6 0x93 0x21 0x09
Router#
```

この例では、デバイスで VTP バージョン 2 を実行しているときの、VTP 設定パラメータの例を示しています。

```
Router# show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 2
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800
Configuration lst modified by 127.0.0.12 at 10-18-07 10:38:45
Local updater ID is 127.0.0.12 on interface EO 0/0 (first interface found)
```

```
Feature VLAN:
--------------
VTP Operating Mode           : Server
Maximum VLANs supported locally: 1005
Number of existing VLANs     : 1005
Configuration Revision       : 1
MD5 digest                   : 0x2E 0x6B 0x99 0x58 0xA2 0x4F 0xD5 0x150x70 0x61 0xB8
                             0x24 0xB6 0x93 0x21 0x09
Router#
```

この例では、デバイスで VTP バージョン 3 を実行しているときの、VTP 設定パラメータの例を示しています。

```
Router# show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 3
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800

Feature VLAN:
--------------
VTP Operating Mode              : Server
Number of existing VLANs        : 1005
Number of existing extended VLANs: 3074
Configuration Revision          : 18
Primary ID                      : 0012.4371.9ec0
Primary Description             :
Router#
```

テイクオーバーの起動

この手順は、VTP バージョン 3 だけに適用されます。テイクオーバーを起動するには、次の作業を行います。

コマンド	目的
`Router# vtp primary-server [vlan | mst]| [force]`	ルータの動作状態をセカンダリ サーバからプライマリ サーバに変更し、設定をドメイン全体にアドバタイズします （このデバイスのパスワードが **hidden** キーワードで設定された場合、ユーザに対し、再入力を促すプロンプトが表示されます)。 **（注）** **force** キーワードを使用すると、設定が矛盾するすべてのサーバで設定が上書きされます。**force** キーワードを使用する場合、テイクオーバーに進む前に確認を促すプロンプトが表示されます。 適切な機能（**vlan** または **mst**）を選択することによって、テイクオーバーの場所を指定します。機能が選択されていない場合、テイクオーバーは VLAN データベースに対して実行されます。

次に、テイクオーバーを起動し、**vlan** データベースに対して実行する例を示します。

```
Router# vtp primary-server vlan
Enter VTP password:password
```

```
This system is becoming primary for feature vlan

VTP Feature Conf Revision Primary Server Device ID      Description
----------- ------------      -------------- -------- --------------------
MST         Yes  4        0012.4371.9ec0=0012.4371.9ec0 R1
Do you want to continue? (confirm)
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
```

ドメインの VTP デバイスの表示

ドメイン内ですべての VTP デバイスを表示するには、特権 EXEC モードで次の作業を行います。

コマンド	目的
Router# **show vtp devices [conflicts]**	ドメイン内のすべての VTP デバイスで情報を収集し、表示します。 **（注）**　特定の機能に対して **vtp modes off** または **transparent** と設定されているルータからは、情報は収集または表示されません。 **conflicts** キーワード（任意）では、設定が矛盾するプライマリ サーバがあるデバイスの情報が表示されます。

次に、ドメイン内で VTP デバイスの情報を表示する例を示します。

```
Router# show vtp devices
Retrieving information from the VTP domain, please wait for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID         Device Description
----------- ---- -------- ------------------------------   ------------------
VLAN        No   18       0016.9c6d.5300 0012.011a.0d00    R2
VLAN        No   18       0016.9c6d.5300 0012.4371.9ec0    R1
MST         Yes  4        0012.4371.9ec0=0012.4371.9ec0    R1

Router#
```

CHAPTER 14

VLAN の設定

この章では、Cisco 7600 シリーズ ルータに 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.14-1）
- 「VLAN のデフォルト設定」（P.14-6）
- 「自動保護スイッチング グループ内の Bridged Routed Encapsulation と VLAN の相互作用」（P.14-8）
- 「VLAN の設定」（P.14-10）

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」（P.14-1）
- 「VLAN の範囲」（P.14-2）
- 「設定可能な VLAN パラメータ」（P.14-2）
- 「トークンリング VLAN の概要」（P.14-3）

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 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 メンバーシップは、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.20-2）を参照）。

Cisco 7600 シリーズ ルータは、IEEE 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 デバイス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	使用状況	VTP によって伝播される
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。この VLAN は使用できますが、削除できません。	Yes
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。	Yes
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。	Yes
1006 ～ 4094	拡張	イーサネット VLAN 専用です。	No

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。
- 昇順の内部 VLAN 割り当て（1006 から昇順）、または降順の内部 VLAN 割り当て（4094 から降順）を設定できます。
- Catalyst オペレーティングシステムが動作しているスイッチは、VLAN 1006 ～ 1024 の設定をサポートしていません。VLAN 1006 ～ 1024 を設定する場合、Catalyst ソフトウェアが動作するスイッチに VLAN が拡張されていないことを確認してください。
- 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.20-2）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、FDDI、FDDI Network Entity Title（NET）、TrBRF、または TrCRF）
- VLAN 状態（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 のスパニングツリー プロトコル（STP）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 が動作するネットワーク デバイスでサポートされる、2 つのトークンリング VLAN タイプについて説明します。

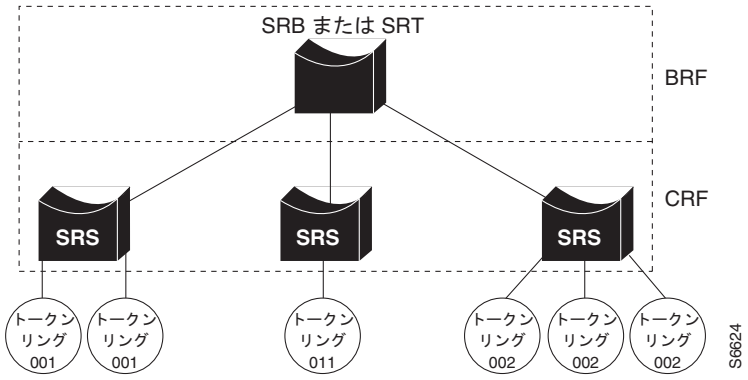
- 「トークンリング TrBRF VLAN」（P.14-3）
- 「トークンリング TrCRF VLAN」（P.14-4）

（注） Cisco 7600 シリーズ ルータは、スイッチ間リンク（ISL）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。Cisco 7600 シリーズ ルータが VTP サーバとして設定されている場合は、ルータからトークンリング VLAN を設定できます。

トークンリング TrBRF VLAN

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 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 デバイス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、Cisco 7600 シリーズ ルータ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 を実行するソースルート ブリッジ（SRB）またはソースルート トランスペアレント（SRT）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 MAC 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 トポロジー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、「自動保護スイッチング グループ内の Bridged Routed Encapsulation と VLAN の相互作用」（P.14-8）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。

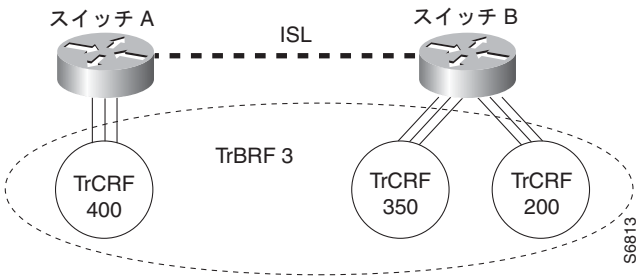
トークンリング TrCRF VLAN

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 デバイスのポートに限定されます。同一ネットワーク デバイスまたは異なるネットワーク デバイス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。

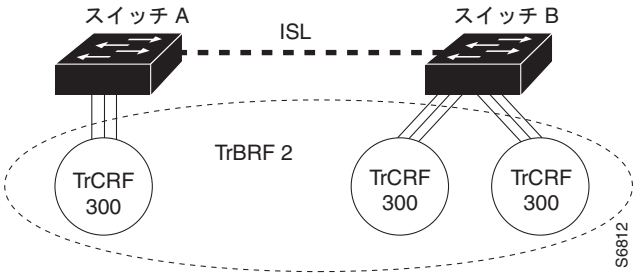
（注）　異なるネットワーク デバイス上に存在するリング間でデータを渡すには、リングを同じ TrBRF に対応付け、その TrBRF を SRB 用に設定します。

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 デバイスが 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 デバイス上のデフォルト TrCRF 間をトラフィックが通過します。

図 14-3　分散型 TrCRF



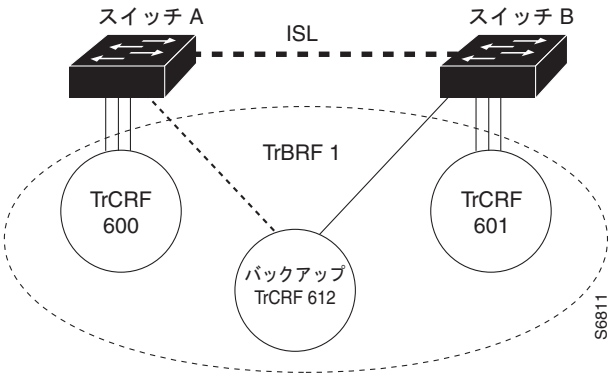
TrCRF 内では、ソースルート スイッチングを使用し、MAC アドレスまたはルート ディスクプリタに基づいてフレーム転送を行います。VLAN 全体を 1 つのリングとして動作させ、フレームを 1 つの TrCRF 内のポート間でスイッチングすることもできます。

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 デバイス間の 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 に属することができるのは、各ネットワーク デバイスで 1 つのポートに限られます。

ネットワーク デバイス間の 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 デバイス上のバックアップ 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	VLAN 1 の場合は「default」 その他のイーサネット VLAN の場合は「VLAN*vlan_ID*」	—
802.10 SAID	10*vlan_ID*	100001 ～ 104094
MTU サイズ	1500	1500 ～ 18190
トランスレーショナル ブリッジ 1	0	0 ～ 1005
トランスレーショナル ブリッジ 2	0	0 ～ 1005
VLAN ステート	active	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

表 14-3　FDDI VLAN のデフォルトおよび範囲 （続き）

パラメータ	デフォルト	範囲
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	active	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	active	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 CRF	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	active	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

自動保護スイッチング グループ内の Bridged Routed Encapsulation と VLAN の相互作用

Bridged Routed Encapsulation（BRE）シナリオでは、IP ルーテッド AAL5SNAP パケットがイーサネット側でブリッジされ、MAC ヘッダーに偽の SRC MAC と設定された Distributed STorage（DST）が追加されます。ATM PVC トラフィックは、イーサネットではなく、IP 経由でリレーされます。ただし、1 つの VLAN 上で複数の Virtual Connection（VC; 仮想接続）を設定することができません。複数の VC を設定するには、Automatic Protection Switching（APS; 自動保護スイッチング）グループの保護インターフェイスと現用インターフェイス上に 1 つずつ VLAN を設定します。この方法は、コンバージェンス時間が長いうえに、VLANS の使用効率が下がるため、あまり有効なソリューションではありません。これらの制限を解決するために、BRE+APS 機能を使用すれば、1 つの VLAN に対して 2 つの VC を設定することができます。ただし、これらの親インターフェイスも同じ APS グループに属している必要があります。

APS グループの設定方法については、次の URL にある『Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide』を参照してください。
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

サポートされるラインカード

この機能は、SIP-200 ラインカードと SIP-400 ラインカードでサポートされます。SIP 実装の詳細については、次の URL にある『Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide』を参照してください。
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw.html

要件および制限事項

BRE+APS 機能を設定する場合は、次の要件と制限事項に従ってください。

- 新しい VC が次の条件を満たしていれば、BRE-Connect VLANS を 2 つの VC に対して設定することができます。
  - 最初の VC と同じ APS グループに属している。
  - 最初の VC と同じ ATM インターフェイスに属していない。

- インターフェイスの APS パラメータを変更する（APS グループを変更する、または、APS 設定を削除する）前に、インターフェイス上の BRE 設定が削除されていることを確認してください。
- ATM インターフェイス上で BRE を設定する場合は、BRE エンドで L2 IP アドレスを設定できませんが、L3 非 BRE エンドで IP アドレスを設定できます。

表 14-7　ATM VLAN BRE 用の show コマンド

	コマンド	目的
ステップ 1	`Router(config)# show atm vlan bre`	設定を確認して、PVC のステータスを表示します。アクティブ VC は **UP** と表示され、非アクティブ VC は **DN**（ダウン）と表示されます。

次に、BRE ATM VLAN の設定を確認する例を示します。

```
Router# show atm vlan bre
Interface       Bre VCD            VPI/VCI   Vlan Learned MAC    Virtual MAC    State
ATM3/0/0.1      1                    0/11     100 0000.0000.0000 0000.0300.0001   UP
ATM3/0/0.2      2                    1/13     200 0000.0000.0000 0000.0300.0002   UP
ATM4/0/0.2      2                    1/13     300 0000.0000.0000 0000.0400.0002   DN
```

警告メッセージ

メイン インターフェイス上で APS を設定した場合と、メイン インターフェイスとサブインターフェイス内で BRE を設定した場合を検証します。BRE 設定を削除する前に、メイン インターフェイスで APS 設定を変更しようとすると、「%ATM2/0/0 - Remove BRE configs on this interface before changing APS configs」という警告メッセージが表示されます。

VLAN 設定時の注意事項および制約事項

ネットワークで VLAN の作成と変更を行う場合は、次の注意事項と制約事項に従ってください。

- 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 エンジンが搭載されたルータ上で、**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るには **no vtp file** コマンドを入力します。
- リリース 12.2(18)SXD 以前のリリースで使用可能だった VLAN データベース モードは、サポートされなくなりました。さらに 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。
- VLAN を作成する前に、Cisco 7600 シリーズ ルータを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。VTP の設定手順については、第 13 章「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 7600 Series Router Cisco IOS Command Reference*』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。

- Cisco 7600 シリーズ ルータは、トークンリングまたは FDDI メディアをサポートしません。ルータは 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。
- Cisco 7600 シリーズ ルータが VTP サーバとして設定されている場合は、ルータから FDDI およびトークンリング VLAN を設定できます。
- 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。

- 「VLAN 設定のバックグラウンド情報」（P.14-10）
- 「イーサネット VLAN の作成または変更」（P.14-11）
- 「VLAN へのレイヤ 2 LAN インターフェイスの割り当て」（P.14-13）
- 「内部 VLAN 割り当てポリシーの設定」（P.14-13）
- 「VLAN 変換の設定」（P.14-14）
- 「802.1Q VLAN から ISL VLAN へのマッピング」（P.14-17）

（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 7600 Series Router Cisco IOS Command Reference*』を参照してください。

VLAN 設定のバックグラウンド情報

ルータが VTP サーバ モードまたはトランスペアレント モードの場合は（「VTP の設定」（P.13-8）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。

ルータが VLAN トランスペアレント モードの場合に、**copy running-config startup-config** コマンドを使用すると、VLAN の設定が startup-config ファイルに保存されます。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）
- ルータの起動時に、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、ルータは vlan.dat ファイル内の設定を使用します。
- リリース 12.2(18)SXD 以前のリリースで使用可能だった VLAN データベース モードは、サポートされなくなりました。

- 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。

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リストで複数のイーサネット VLAN 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、特権 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 以降が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。
- 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。作成または変更対象の 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中の場合、ルータからメッセージが表示され、VLAN 設定は変更されません。

VLAN を削除する場合は、次の情報に注意してください。

- 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 の、メディア タイプ別のデフォルト VLAN は削除できません。

- 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）対応付けられています。

次に、イーサネット VLAN を作成して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
---- -------------------------------- --------- -------------------------------

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
```

次に、設定を確認する例を示します。

```
Router# show vlan name VLAN0003
VLAN Name                             Status    Ports
---- -------------------------------- --------- ---------------------

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
Router#
```

未使用 VLAN の全体数を一覧表示したり、システムでの VLAN の使用サマリ情報を表示するには、**sh vlan free** と **sh vlan free summary** コマンドを使用することもできます。

```
Router#show vlan free ?
  Summary  Total number of free vlans in the system
  |        Output modifiers
  <cr>

Router#show vlan free

Free VLANs
----------
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
```

```
20
21

Router#show vlan free ?
  Summary  Total number of free vlans in the system
  |        Output modifiers
Router#show vlan free summ
Router#show vlan free summary ?
  |  Output modifiers

Router#show vlan free summary

======= VLAN free/usage Summary =======

Total number of available vlans = 4094

Total number of free vlans = 4074

Total number of used vlans = 20

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.10-6）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。

	コマンド	目的
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 から昇順に内部 VLAN を割り当てるには、**ascending** キーワードを入力します。
- 4094 から降順に内部 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、降順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。

- 「VLAN 変換に関する注意事項および制約事項」（P.14-14）
- 「トランク ポート上の VLAN 変換の設定」（P.14-16）
- 「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」（P.14-16）

（注）　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 の変換時には、次の注意事項および制約事項に従ってください。

- VLAN 変換設定は、レイヤ 2 トランクではないポートに適用される場合、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。
- インターフェイス内で VALN 変換をイネーブルにすると、インターフェイスがリセットされます。
- 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）　OSM 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	ポートの数	ポート グループの数	ポート グループごとのポート範囲	ポート グループごとの変換数	VLAN 変換トランク タイプ サポート
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-X6704-10GE	4	4	各グループで 1 つのポート	128	ISL 802.1Q
WS-X6708-10GE	8	8	各グループで 1 つのポート	16	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 ～ 23 の奇数 25 ～ 47 の奇数 2 ～ 24 の偶数 26 ～ 48 の偶数	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）　WS-X6748-GE-TX カードの場合、ポートは ASIC ごとに奇数および偶数でグループ化され、ポート グループあたりの VLAN マッピング数は 128 です。VLAN マッピング設定はポート グループのすべてのポートに適用できるため、実行される VLAN マッピングの合計数は 22 です。

（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.10-8）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` `Router(config-if)# no switchport vlan mapping {all | 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。 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。

	コマンド	目的
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 デバイス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。

- Cisco 7600 シリーズ ルータ上で、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 Cisco 7600 シリーズ ルータ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 デバイスには、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
```

CHAPTER 15

プライベート VLAN の設定

この章では、Cisco 7600 シリーズ ルータ上でプライベート 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「プライベート VLAN の機能概要」（P.15-1）
- 「プライベート VLAN 設定時の注意事項および制約事項」（P.15-6）
- 「プライベート VLAN の設定」（P.15-11）
- 「プライベート VLAN のモニタ」（P.15-17）

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」（P.15-2）
- 「プライベート VLAN ポート」（P.15-3）
- 「プライマリ VLAN、独立 VLAN、コミュニティ VLAN」（P.15-3）
- 「プライベート VLAN ポートの分離」（P.15-4）
- 「プライベート VLAN による IP アドレス指定方式」（P.15-4）
- 「複数のルータにわたるプライベート VLAN」（P.15-5）
- 「プライベート VLAN とその他の機能の相互作用」（P.15-5）

プライベート VLAN ドメイン

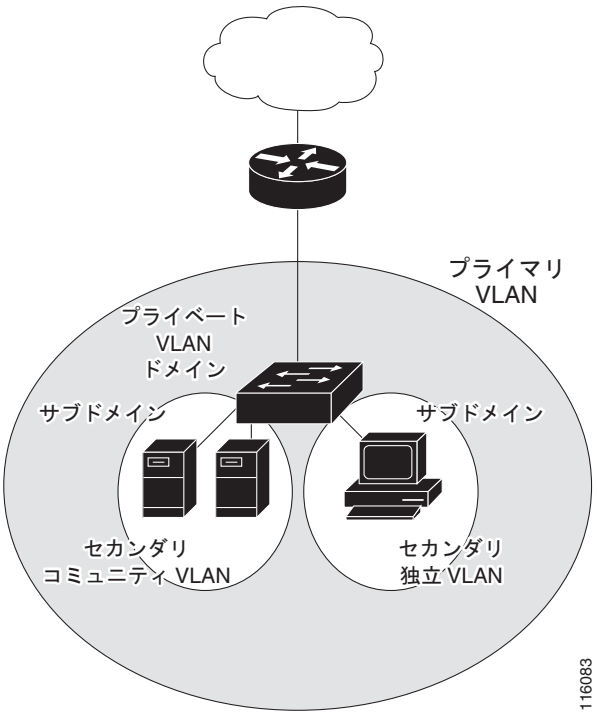
プライベート VLAN 機能では、サービス プロバイダーが VLAN の使用時に直面する、次の 2 つの問題に対処します。

- ルータは、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 とセカンダリ VLAN で構成されるプライベート VLAN のペアで表されます。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（サブドメインごとに 1 つずつのペア）を設定することができます。プライベート VLAN ドメイン内のすべての VLAN ペアが、同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、サブドメインを識別します（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 が 1 つしかありません。プライベート VLAN ドメイン内のすべてのポートが、プライマリ VLAN のメンバーです。つまり、プライマリ VLAN がプライベート VLAN ドメイン全体になります。

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 レベルでは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 レベルでその他のコミュニティ内のポートと通信できません。

プライベート VLAN ポート

プライベート VLAN ポートには 3 種類があります。

- 無差別：無差別ポートはプライマリ VLAN に属し、プライマリ VLAN に関連付けられたセカンダリ 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 ポートも含めて、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、無差別ポートを除く、同一プライベート VLAN ドメインのそ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、無差別ポートからのトラフィックを除き、独立ポート宛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、無差別ポートだけに転送されます。
- 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、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、レイヤ 2 で、他のコミュニティに属しているすべてのインターフェイスから、または、プライベート VLAN ドメイン内の独立ポートから分離されています。

（注） トランクは独立ポート、コミュニティ ポート、および無差別ポート間でトラフィックを伝送する 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ルータに送受信できます。

プライマリ VLAN、独立 VLAN、コミュニティ VLAN

プライマリ VLAN、および独立 VLAN とコミュニティ VLAN という 2 種類のセカンダリ VLAN には、次の特性があります。

- プライマリ VLAN：無差別ポートからホスト ポート（独立とコミュニティ）およびその他の無差別ポートへの単一方向トラフィック ダウンストリームを搬送します。
- 独立 VLAN：プライベート VLAN ドメインには独立 VLAN が 1 つだけあります。独立 VLAN はセカンダリ VLAN であり、ホストから無差別ポートおよびゲートウェイに向かう単一方向トラフィック アップストリームを搬送します。
- コミュニティ VLAN：コミュニティ VLAN はセカンダリ VLAN であり、コミュニティ ポートから同一コミュニティの無差別ポート ゲートウェイおよびその他のホスト ポートにアップストリーム トラフィックを搬送します。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。

無差別ポートは、1 つのみのプライマリ VLAN、1 つの独立 VLAN、複数のコミュニティ VLAN を処理できます。レイヤ 3 ゲートウェイは一般的に、無差別ポートを介してルータに接続されます。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセス ポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

スイッチド環境では、個々の VLAN および対応する IP サブネットを、個々のステーションまたはステーションの共通のグループに割り当てることができます。エンド ステーションは、プライベート VLAN の外部にアクセスするために、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 ポートの分離

プライベート VLAN を使用すると、次のようにエンド ステーションへのアクセスを制御できます。

- エンド ステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンド ステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルト ゲートウェイおよび選択エンド ステーション（バックアップ サーバなど）に接続されているインターフェイスを無差別ポートとして設定し、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るようにします。

複数のデバイス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デバイスにトランキングします。使用するプライベート VLAN 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 ポートがないデバイスを含めて、すべての中間デバイスでプライベート VLAN を設定します。

プライベート VLAN による IP アドレス指定方式

それぞれのカスタマーに別々の VLAN を割り当てると、次のように非効率的な IP アドレス指定方式が作成されます。

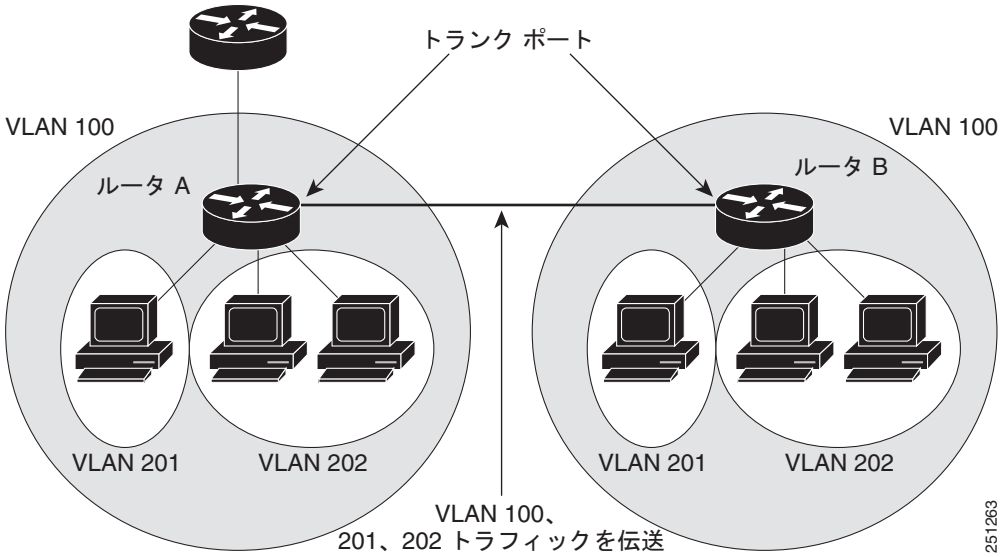
- カスタマー VLAN にアドレスのブロックを割り当てると、未使用 IP アドレスが発生することがあります。
- VLAN におけるデバイス数が増加する場合、割り当て済みアドレス数が増加に対応できるだけ十分に大きくないことがあります。

この問題は、プライベート VLAN を使用すると軽減します。プライベート VLAN では、プライベート VLAN のすべてのメンバーが、プライマリ VLAN に割り当てられている共通アドレス空間を共有するためです。ホストはセカンダリ VLAN に接続され、プライマリ VLAN に割り当てられているアドレスのブロックから IP アドレスが DHCP サーバによってホストに割り当てられますが、同一プライマリ VLAN 内のセカンダリ VLAN には割り当てられません。さまざまなセカンダリ VLAN のカスタマー デバイスには後続 IP アドレスが割り当てられます。新しいデバイスを追加すると、サブネット アドレスの巨大プールから次に使用できるアドレスが、DHCP サーバによって割り当てられます。

複数のルータにわたるプライベート VLAN

通常の VLAN と同じように、プライベート VLAN は複数のルータに広げることができます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN をネイバールータに伝送します。トランク ポートは、プライベート VLAN をその他の VLAN のように処理します。複数のルータに及ぶプライベート VLAN には、ルータ A の独立ポートからのトラフィックが、ルータ B の独立ポートに達しないという特徴があります（図 15-2 を参照）。

図 15-2　　複数のルータにわたるプライベート 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

VTP ではプライベート VLAN がサポートされないので、レイヤ 2 ネットワークのすべてのルータでは、プライベート VLAN を手動で設定する必要があります。ネットワークの一部のルータでプライマリ VLAN およびセカンダリ VLAN のアソシエーションを設定しない場合、これらのルータのレイヤ 2 データベースはマージされません。この状況では、それらのルータでプライベート VLAN トラフィックの不要なフラッディングが発生することがあります。

プライベート VLAN とその他の機能の相互作用

ここでは、プライベート VLAN がその他の機能と相互作用する方法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 と 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.15-6）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 の場合、同一 VLAN の各デバイスはレイヤ 2 レベルで相互に通信できますが、別々の VLAN のインターフェイスに接続しているデバイスはレイヤ 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、無差別ポートはプライマリ VLAN のメンバーであり、ホスト ポートはセカンダリ VLAN に属します。セカンダリ VLAN はプライマリ VLAN に関連付けられているので、これらの VLAN のメンバーはレイヤ 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 のすべてのポートに転送されます。プライベート VLAN ブロードキャスト転送は、次のようにブロードキャストを送信するポートに左右されます。

- 独立ポートは、無差別ポートまたはトランク ポートのみにブロードキャストを送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、同じコミュニティ VLAN のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックのルーティングとブリッジングは、プライベート VLAN 境界を横断して行われ、単一コミュニティ VLAN 内でも行われます。マルチキャスト トラフィックは、同じ独立 VLAN のポート間、または別々のセカンダリ VLAN のポート間では転送されません。

プライベート VLAN と SVI

ルータ 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 デバイスは、セカンダリ VLAN ではなく、プライマリ VLAN だけを介してプライベート 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 にはレイヤ 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間、セカンダリ VLAN の SVI は非アクティブになります。

- 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と、SVI をディセーブルにするまでは、設定が許可されません。
- セカンダリ VLAN として設定されている VLAN で SVI を作成し、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場合、SVI は作成されずに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、マッピングされている場合、プライマリ VLAN 上のすべての設定がセカンダリ VLAN SVI に伝播されます。たとえば、プライマリ VLAN SVI に IP サブネットを割り当てると、このサブネットはプライベート VLAN 全体の IP サブネット アドレスになります。

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 設定の注意事項について、次のセクションで説明します。

- 「セカンダリ VLAN およびプライマリ VLAN の設定」（P.15-7）
- 「プライベート VLAN ポートの設定」（P.15-9）
- 「その他の機能の制限事項」（P.15-9）

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 の設定時には、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 をトランスポート モードに設定したあとでは、VTP モードをクライアントまたはサーバに変更することはできません。VTP については、第 13 章「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、第 14 章「VLAN の設定」を参照してください。
- プライベート VLAN の設定後は、**copy running-config startup config** 特権 EXEC コマンドを使用して、VTP トランスペアレント モード設定およびプライベート VLAN 設定を startup-config ファイルに保存してください。ルータがリセットした場合、プライベート VLAN をサポートするためにデフォルトで VTP トランスペアレント モードになる必要があります。
- 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 ポートを使用するデバイスごとに、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。
- イーサネット VLAN だけをプライベート VLAN にすることができます。
- 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 VLAN 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 をプライマリ VLAN に関連付けられている場合、ブリッジ プライオリティなどのプライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。ただし、STP パラメータが必ずしもその他のデバイスに伝播されるとはかぎりません。STP 設定を手動でチェックして、プライマリ VLAN、独立 VLAN、コミュニティ VLAN のスパニングツリー トポロジが一致することを確認してください。これらの VLAN が同じ転送データベースを適切に共有できるようにするためです。
- ルータの 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 トポロジーが一致するように、ネットワーク内のすべてのデバイス上で MAC アドレス リダクション機能をイネーブルにする必要があります。
- プライベート VLAN が設定されているネットワーク内で、一部のデバイスの MAC アドレス リダクション機能をイネーブルにし、他のデバイス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 リダクションは個々のレベルにしか対応せず、範囲としてはすべての中間値を内部的に使用します。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 VLAN ACL（VACL）を適用できません （第 37 章「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と、DHCP スヌーピングはセカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、DHCP 設定は有効になりません。

- プライベート VLAN でトラフィックを伝送しないデバイスのトランクから、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）設定を適用できます（第 45 章「PFC QoS の設定」を参照）。
- プライベート VLAN を設定すると、スティッキ アドレス解決プロトコル（ARP）がデフォルトでイネーブルになり、レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリはスティッキ 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 ポートのスティッキ ARP エントリには期限切れがありません。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.40-43）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。
- スティッキ 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。スティッキ ARP はインターフェイスごとに設定できます。スティッキ ARP の設定については、「スティッキ ARP の設定」（P.40-43）を参照してください。次の注意事項および制約事項が、プライベート VLAN のスティッキ ARP に適用されます。
  - レイヤ 3 プライベート VLAN インターフェイスで学習した ARP エントリは、スティッキ ARP エントリです。
  - IP アドレスが同じでも、MAC アドレスが異なるデバイスを接続すると、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 ポートのスティッキ 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 VLAN マップを設定できます（「VLAN アクセス マップの適用」（P.37-7）を参照）。ただし、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN では、同一 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 内においてレイヤ 2 で転送されると、入力側と出力側で同じ VLAN マップが適用されます。プライベート VLAN 内部から外部ポートにフレームがルーティングされると、プライベート VLAN マップが入力側で適用されます。
  - フレームがホスト ポートから無差別ポートにアップストリームで送信される場合は、セカンダリ VLAN で設定された VLAN マップが適用されます。
  - フレームが無差別ポートからホスト ポートにダウンストリームで送信される場合は、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 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 およびセカンダリ 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 ACL 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 35 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 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ（SPAN）機能がサポートされます。
  - プライベート VLAN 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; VLAN ベースの SPAN）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監視することができます。
  - SPAN の詳細については、第 53 章「ローカル SPAN、RSPAN、および 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 ポートの設定時には、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、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。
- PAgP または 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 設定はいずれも非アクティブです。
- 設定ミスによって STP ループが発生しないようにして、STP コンバージェンスを高速化するには、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 BPDU ガードをイネーブルにします（第 21 章「オプションの STP 機能の設定」を参照）。イネーブルにすると、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。無差別ポートでは、PortFast および BPDU ガード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。
- ネットワーク デバイスをトランク接続し、プライマリ VLAN およびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートはさまざまなネットワーク デバイス上で使用できます。
- プライベート VLAN に関連するすべてのプライマリ VLAN、独立 VLAN、コミュニティ VLAN では、トランク間で同一トポロジーを維持する必要があります。すべての関連 VLAN で同じ STP ブリッジ パラメータとトランク ポート パラメータを設定し、同一トポロジーを維持することを強く推奨します。

その他の機能の制限事項

プライベート VLAN の設定時には、その他の機能で次の設定上の制限事項を考慮してください。

（注）　一部の状況では、エラー メッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

- プライベート VLAN が設定されているルータでは、フォールバック 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 モードになっており、ポートがプライマリ ポート、独立ポート、コミュニティ ポートのうちのいずれかであることをプライベート VLAN 設定が示している場合、ポートはプライベート VLAN 機能だけに影響されます。ダイナミック トランキング プロトコル（DTP）などのその他のモードにポートがなっている場合、ポートはプライベート ポートとして機能しません。
- 次のようなその他の機能用に設定したインターフェイスでは、プライベート VLAN ポートを設定しないでください。
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（LACP）
  - 音声 VLAN
- IEEE 802.1x ポートベース認証をプライベート VLAN ポートで設定できますが、ポート セキュリティ、音声 VLAN、またはユーザごとの ACL と一緒に 802.1x をプライベート VLAN ポートに設定しないでください。
- IEEE 802.1q マッピングは正常に動作します。トラフィックは、ISL VLAN から受信されたかのように、設定に従って dot1Q ポートに、または dot1Q ポートから再マッピングされます。
- 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、Remote SPAN（RSPAN）VLAN を設定しないでください。SPAN の詳細については、第 53 章「ローカル SPAN、RSPAN、および ERSPAN の設定」を参照してください。
- プライベート VLAN ホストまたは無差別ポートは、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 ポートとして設定すると、ポートは非アクティブになります。
- 宛先 SPAN ポートを独立ポートにしないでください。送信元 SPAN ポートを独立ポートにすることはできます。VSPAN を設定して、プライマリ VLAN およびセカンダリ VLAN の両方を拡張するか、入力トラフィックまたは出力トラフィックだけが重要な場合はそのどちらかを拡張できます。
- 各 VLAN 間でショートカットを使用する場合（このうちいずれかの VLAN がプライベート VLAN である場合）は、プライマリ VLAN、独立 VLAN、コミュニティ VLAN を考慮してください。プライマリ VLAN は、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。セカンダリ VLAN（真の送信元）が、レイヤ 2 FID テーブルでプライマリ VLAN に常に再マッピングされるからです。
- プライマリ VLAN の無差別ポートでスタティック MAC アドレスを設定する場合は、すべての関連セカンダリ VLAN に同じスタティック 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 ポートでスタティック MAC アドレスを設定する場合は、関連プライマリ VLAN に同じスタティック 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 アドレスを削除する場合は、設定した 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 で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、セカンダリ VLAN で学習した MAC アドレスは、プライマリ VLAN で複製されます。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ると、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。ポートはプライベート VLAN 設定の一部にすることができますが、ポートの EtherChannel 設定はいずれも非アクティブになります。

- 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の制約事項は次のとおりです。
  - すべてのリリースで、12 ポートの制約事項が次の 10Mb、10/100Mb、100Mb 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
  - 12 ポートの制約事項は、WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6524-100FX-MM（CSCea67876）の各イーサネット スイッチング モジュールには適用されません。

  12 ポート（1 ～ 12、13 ～ 24、25 ～ 36、37 ～ 48）のグループ内で、12 ポートのグループ内に次のいずれかのポートが含まれている場合は、独立ポートまたはコミュニティ VLAN ポートとしてポートを設定しないでください。
  - トランク ポート
  - SPAN 宛先ポート
  - 無差別プライベート VLAN ポート
  - **switchport mode dynamic auto** コマンドまたは **switchport mode dynamic desirable** コマンドで設定したポート

  12 ポートのグループ内に上記ポートのいずれかが含まれており、上記プロパティが設定されている場合は、12 ポート内の他のポートに関する独立 VLAN 設定またはコミュニティ VLAN 設定が非アクティブになります。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。
- 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の制約事項は次のとおりです。

  すべてのリリースで、この 24 ポートの制約事項が WS-X6548-GE-TX および WS-X6148-GE-TX 10/100/1000Mb 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 ポート（1 ～ 24、25 ～ 48）のグループ内では、24 ポートのグループのうち 1 つのポートが次のうちのいずれかになる場合、独立ポートまたはコミュニティ VLAN ポートとしてポートを設定しないでください。
  - トランク ポート
  - SPAN 宛先ポート
  - 無差別プライベート VLAN ポート
  - **switchport mode dynamic auto** コマンドまたは **switchport mode dynamic desirable** コマンドで設定したポート

  24 ポートのグループ内に上記ポートのいずれかが含まれており、上記プロパティが設定されている場合は、24 ポート内の他のポートに関する独立 VLAN 設定またはコミュニティ VLAN 設定が非アクティブになります。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、次の設定について説明します。

- 「プライベート VLAN としての VLAN の設定」（P.15-12）
- 「セカンダリ VLAN とプライマリ VLAN の関連付け」（P.15-13）

- 「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」（P.15-14）
- 「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」（P.15-15）
- 「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」（P.15-16）

（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}`	VLAN をプライベート VLAN として設定します。
	`Router(config-vlan)# no private-vlan {community | isolated | primary}`	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実行されません。
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、次の作業を実行します。

	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 と関連付ける際は、次の情報に注意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。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 を含めることができます。
- *secondary_vlan_list* パラメータには、独立 VLAN ID を 1 つだけ含めることができます。
- セカンダリ VLAN とプライマリ VLAN を関連付けるには、*secondary_vlan_list* を入力するか、*secondary_vlan_list* に **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 間の関連付けを消去するには、*secondary_vlan_list* に **remove** キーワードを使用します。
- このコマンドは、VLAN コンフィギュレーション サブモードを終了しない限り、有効になりません。

次の例は、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、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。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、*secondary_vlan_list* パラメータに **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 間のマッピングを消去するには、*secondary_vlan_list* パラメータに **remove** キーワードを使用します。

次の例は、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かぎり、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、インターフェイス FastEthernet 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 無差別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 無差別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** コマンドを一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かぎり、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 無差別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 無差別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 無差別ポートと、プライマリ VLAN および任意のセカンダリ VLAN 間のすべて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 無差別ポートとして設定する際は、次の情報に注意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。複数のカンマ区切りの項目を含めることができます。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 無差別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 無差別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、インターフェイス FastEthernet 5/2 をプライベート VLAN 無差別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 は、プライベート VLAN アクティビティをモニタするための特権 EXEC コマンドを示しています。

表 15-1　プライベート VLAN モニタリング コマンド

コマンド	目的
show interfaces status	インターフェイスが属している VLAN を含めて、インターフェイスのステータスを表示します。
show vlan private-vlan [**type**]	ルータのプライベート 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、Cisco 7600 シリーズ ルータに 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 7600 Series Routers Command References』を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.16-1）
- 「Cisco IP Phone サポートのデフォルト設定」（P.16-4）
- 「Cisco IP Phone サポートの設定時の注意事項と制約事項」（P.16-4）
- 「Cisco IP Phone サポートの設定」（P.16-5）

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」（P.16-1）
- 「Cisco IP Phone の音声トラフィック」（P.16-2）
- 「Cisco IP Phone のデータ トラフィック」（P.16-3）
- 「Cisco IP Phone の電源構成」（P.16-3）

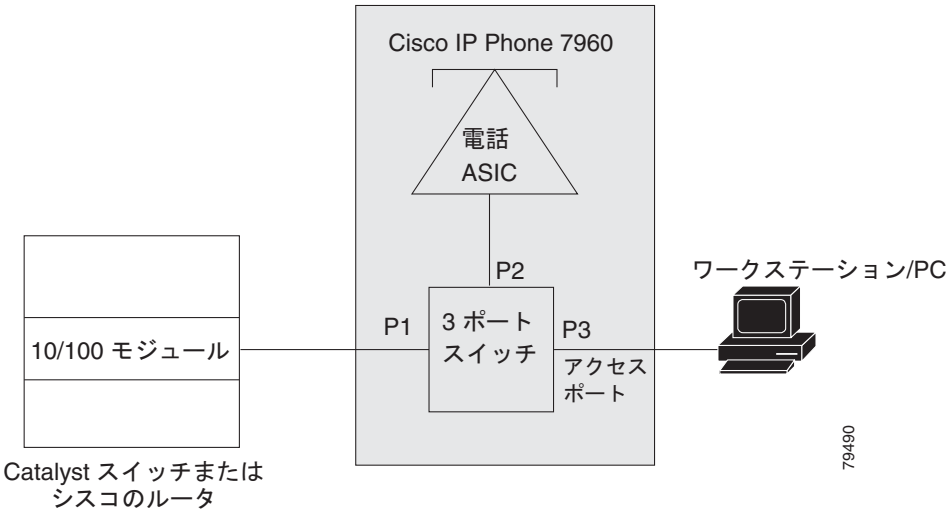
Cisco IP Phone の接続

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、次のデバイスとの接続専用です。

- ポート 1 は、ルータに接続します。
- 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 またはその他のデバイスに接続します。

図 16-1 に、ルータと PC の間に、Cisco IP Phone を接続する方法を示します。

図 16-1　スイッチに接続された Cisco IP Phone



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 CoS 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。音声トラフィックのフローを予測可能にするために、音声トラフィックのレイヤ 3 の IP precedence 値またはレイヤ 2 の CoS 値を信頼するように、QoS を設定できます（第 45 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 VLAN を音声トラフィック用、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。

ルータ上のレイヤ 2 アクセス ポートが、Cisco Discovery Protocol（CDP）パケットを送信するように設定できます。CDP は、接続された Cisco IP Phone が次のいずれかの方法で、ルータ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 ポートに接続するデバイス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 タイプを設定することはできません。

Cisco IP Phone のデータ トラフィック

（注）　Cisco IP Phone に接続されているデバイス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 上のアクセス ポートに接続するデバイス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（図 16-1 を参照）、ルータ上のレイヤ 2 アクセス ポートに CDP パケットの送信を設定して、接続された Cisco IP Phone が Cisco IP Phone 上のアクセス ポートを次のどちらかのモードに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.16-3）

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を供給されていると、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 ドーター 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 モジュールについては、マニュアル『*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。

スイッチング モジュール ポートは、電力を供給されていない 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、それがどこのモジュール、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 CLI または SNMP 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電力に戻されます。

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 デバイスを接続すると、そのネットワーク デバイスが損傷することがあります。ネットワーク デバイスを取り外し、別のネットワーク デバイスを接続する場合は、10 秒以上待機してから行うようにしてください。

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 サポートの設定時の注意事項と制約事項

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 Cisco 7600 シリーズ ルータポートで Cisco Discovery Protocol（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 ポートだけに設定できます。
- 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。

- QoS ポート アーキテクチャ 1p4t/2q2t を使用して、10/100 Mbps ポートが受信するレイヤ 2 CoS 値を信頼するように設定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 に接続されているデバイスは同じ 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、デバイス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、デバイスは 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 に接続されているデバイスは、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デバイス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デバイス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 MAC 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 50 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.16-5）
- 「データ トラフィックのサポートの設定」（P.16-7）
- 「インライン パワー サポートの設定」（P.16-8）

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。

	コマンド	目的
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。指定できる VLAN ID は 1 ～ 4094 です。ルータは、802.1Q 音声トラフィックを音声 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。ルータは、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。ルータは、タグなし音声トラフィックをアクセス VLAN に送ります。
- **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。ルータは、タグなし音声トラフィックをアクセス VLAN に送ります。
- 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 45 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.10-13）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デバイス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デバイスから受信したタグ付き入トラフィックを 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（有効な値は 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 ポートに接続するデバイス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デバイス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、Cisco 7600 シリーズ ルータに 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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- 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」（P.17-1）
- 「802.1Q トンネリングの設定時の注意事項および制約事項」（P.17-4）
- 「802.1Q トンネリングの設定」（P.17-6）
- 「IEEE 802.1ab LLDP」（P.17-7）

802.1Q トンネリングの機能概要

802.1Q トンネリングを使用すると、サービス プロバイダーは単一の VLAN を使用して、複数の VLAN を持つカスタマーをサポートできます。このときに、カスタマーの VLAN ID は保護され、各カスタマー VLAN のトラフィックは分離されます。

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を、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 VLAN に割り当てます。これがトンネル VLAN になります。カスタマーの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、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 のすべてのトンネル ポートが、トンネルの入口ポイントおよび出口ポイントになります。802.1Q トンネルには、カスタマー ルータへの接続に必要となる数のトンネル ポートをいくつでも含めることができます。

カスタマー ルータはトランク接続されますが、802.1Q トンネリングを使用した場合は、サービス プロバイダー ルータが、すべてのカスタマー VLAN を直接伝送する代わりに、1 つのサービス プロバイダー VLAN を使用してすべてのカスタマー VLAN を伝送します。

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 デバイス上の 802.1Q トランク ポートから着信し、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 ルータに着信します。カスタマー デバイス上の 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.17-3）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

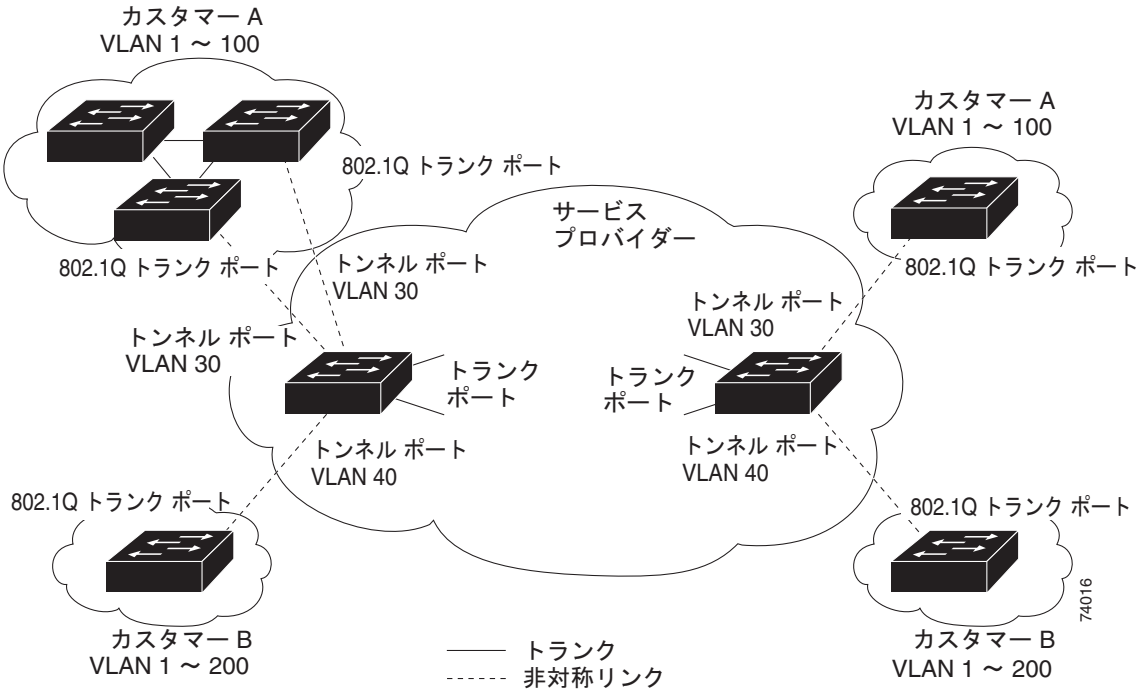
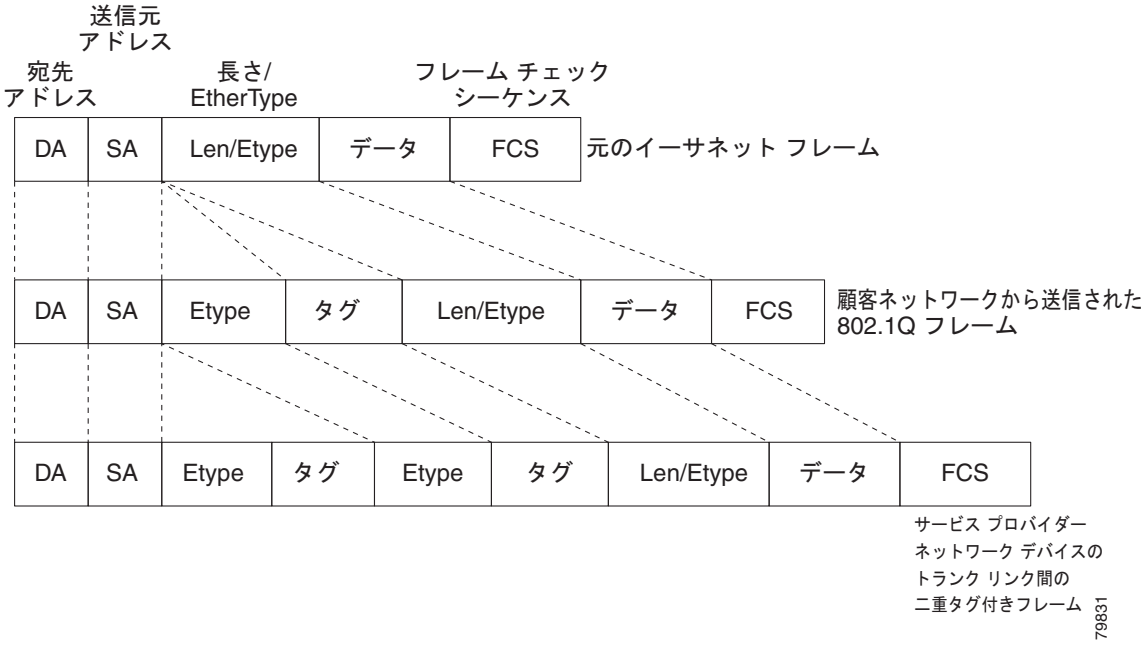


図 17-2　タグなし、802.1Q タグ付き、および二重タグ付きイーサネット フレーム



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（CoS）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ポイントになります。

トンネル ポートは異なるネットワーク デバイス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 デバイスを通過して、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 デバイスに対応するために、トンネルにはトンネル ポートを必要なだけ設定できます。

出口のトンネル ポートは、2 バイトの Ethertype フィールド（0x8100）と 2 バイトの length フィールドを取り除き、802.1Q タグは付けたまま、カスタマー デバイス上の 802.1Q トランク ポートにトラフィックを送ります。カスタマー デバイス上の 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 番めの 802.1Q タグがサービス プロバイダー ネットワーク デバイス間のトランク リンク上にある場合だけ、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 トンネリングをネットワークで設定するときは、次の注意事項および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は、トランキングを設定するコマンドはいずれも非アクティブです。
- トンネル ポートはカスタマー MAC 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デバイス間でトンネル トラフィックを伝送する場合は、ISL 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。
- 非対称リンク内の 802.1Q トランク ポートのネイティブ VLAN がトラフィックを伝送しないことを確認します。ネイティブ VLAN 内のトラフィックにはタグがないため、正しくトンネリングできません。また、グローバルな **vlan dot1q tag native** コマンドを入力して、ネイティブ VLAN 出力トラフィックにタグを付けたり、タグなしのネイティブ VLAN 入力トラフィックを廃棄することもできます。
- トンネル ポートでジャンボ フレームのサポートを次のように設定してください。
  - 「ジャンボ フレーム サポートの設定」（P.8-9）を参照してください。
  - 「ジャンボ フレーム サポートの設定」で指定されている、ジャンボ フレームをサポートしないモジュールをメモします。
- 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、ルータ内に 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。
  - ルータは、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）。
  - ルータはトンネル トラフィックに対して MAC レイヤ アクセス コントロールおよび QoS 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）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 が一致する必要のない設定の場合は、メッセージを無視してください。
- 非対称リンクでは、リンク上にトランク ポートが 1 つしかないため、ダイナミック トランキング プロトコル（DTP）はサポートされていません。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デバイス間で機能します。
  - CDP
  - 単一方向リンク検出（UDLD）
  - ポート集約プロトコル（PAgP）
  - リンク集約制御プロトコル（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 トランキング プロトコル（VTP）は、次のデバイス間で機能しません。
  - 非対称リンクで接続されたデバイス
  - トンネルを介して通信するデバイス

（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 はトンネリングされたデバイス間で機能します。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使用するように、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 ルータでは、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 ルータで、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ドロップするには、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 ルータで、グローバルな *vlan dot1q tag native* オプションを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）　このオプションがあるルータではイネーブル、別のルータではディセーブルになっていると、すべてのトラフィックがドロップされます。すべてのカスタマー ルータでは、各ルータのこのオプションは同じ設定になっていなければなりません。

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 がドロップされているため、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 プロバイダー側のルータ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。

- 「802.1Q トンネル ポートの設定」（P.17-6）
- 「ネイティブ VLAN トラフィックにタグを付けるためのルータ設定」（P.17-7）

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かぎり、必須です。

	コマンド	目的
ステップ 3	`Router(config-if)# 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。
	`Router(config-if)# no switchport mode dot1q-tunnel`	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ルータ設定

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 タグ付きフレームだけを許可するようにルータ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ドロップされます。

（注）　Release 15.1(2)S 以降では、ネイティブ VLAN タギングを **vlan dot1q tag native** コマンドを使用してグローバルにイネーブルにするか、または **switchport trunk native vlan** コマンドを使用してポートでローカルにイネーブルにすると、UDLD パケットが L2 ポートから VLAN 1 で送信されます。

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)# 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、ルータを設定します。
	`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ルータを設定し、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
```

IEEE 802.1ab LLDP

ここでは、IEEE 802.1ab Link Layer Discovery Protocol（LLDP; リンク層検出プロトコル）機能について説明します。

- 「LLDP の概要」（P.17-8）
- 「制限事項」（P.17-9）
- 「デフォルトの LLDP 設定」（P.17-10）
- 「Cisco 7600 シリーズ ルータでの LLDP の設定」（P.17-10）
- 「トラブルシューティングのヒント」（P.17-16）

LLDP の概要

Cisco Discovery Protocol（CDP）は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2 デバイス検出プロトコル（データ リンク レイヤ）です。CDP により、ネットワーク管理アプリケーションは、ネットワークに接続している他のシスコ デバイスを自動的に検出できます。

CDP コマンドの詳細については、次の URL にある『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_1/configfun/command/reference/frd3001b.html

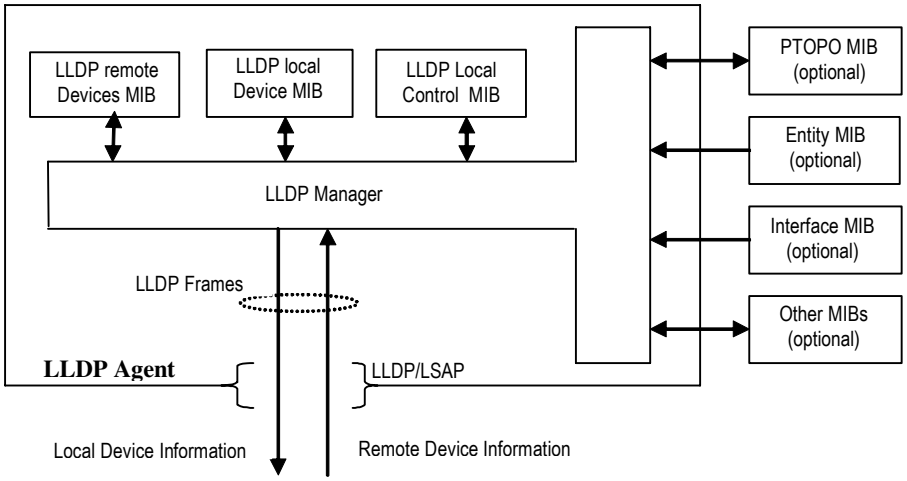
CDP は、ほとんどの場合、トポロジ ディスカバリに使用されます。非シスコ デバイスは、CDP を使用してシスコ デバイスと対話できません。非シスコ デバイスをサポートし、他のデバイスとの相互運用性を確保するために、IEEE 802.1AB LLDP が使用されます。

次に、一部の LLDP 機能を示します。

- このプロトコルは、2 つのシステム（別のネットワーク レイヤ プロトコルを実行）が互いに学習することを可能にします。
- LLDP は 802 LAN ステーションにおけるプロトコル スタックの省略可能な要素です。
- LLDP では、Logical Link Control（LLC; 論理リンク制御）サービスを使用して、他の LLDP エージェントとの間で情報を送受信します。LLC は、LLDP へのアクセス用に Link Service Access Point（LSAP; リンク サービス アクセス ポイント）を提供します。各 LLDP フレームは、単一の MAC サービス要求として送信されます。各着信 LLDP フレームは、LLC エンティティにより、MAC Service Access Point（MSAP; MAC サービス アクセス ポイント）で MAC サービス表示として受信されます。

図 17-3 に、ネットワークで動作する LLDP のハイレベルなビューを示します。

図 17-3　LLDP のブロック図



LLDP プロトコルは、LLDP エージェントを介して動作します。LLDP エージェントのタスクは次のとおりです。

- LLDP ローカル システム MIB から情報を収集して、その情報を定期的に送信する。
- ネイバーから LLDP フレームを受信して、LLDP リモート デバイス MIB およびその他のオプション MIB を読み込む。

LLDP は、ネイバー デバイスの検出に使用される属性セットをサポートします。これらの属性は、デバイスのタイプ、長さ、および値の記述であり、Type Length Value（TLV）とも呼ばれます。LLDP でサポートされるデバイスは、ネイバーとの情報の送受信に TLV を使用します。設定情報、デバイスの機能、デバイス ID などの詳細情報も、このプロトコルを使用してアドバタイズされます。

必須の LLDP TLV は次のとおりです。

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

制限事項

LLDP には、次の制約事項が適用されます。

- 所定のエンド ネットワーク デバイスで使用できるメモリによって、記録されるネイバー エントリの数が決定します。ただし、ほとんどの動作状況下では、プリンタ、IP 電話、ワークステーションなどのエンド デバイスは通常、受信モードのみで動作します。
- エンティティ MIB からのオブジェクトが、送信者 ID を作成するためなどで LLDP ブロードキャストに使用される場合、LLDP が正常に機能するには、それらの MIB が使用可能である必要があります。

デフォルトの LLDP 設定

表 17-1 に、デフォルトの LLDP 設定を示します。

表 17-1　デフォルトの LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	すべての TLV の送受信をイネーブルに
LLDP インターフェイス ステート	イネーブル
LLDP 受信	イネーブル
LLDP 転送	イネーブル

Cisco 7600 シリーズ ルータでの LLDP の設定

次に、c7600 プラットフォーム上での LLDP の設定方法について説明します。

- 「LLDP の設定」（P.17-10）
- 「LLDP のモニタリングと維持」（P.17-12）
- 「設定の確認」（P.17-13）

LLDP の設定

LLDP を設定するには、次の手順を実行します。

手順の概要

ステップ 1　**enable**

ステップ 2　**configure terminal**

ステップ 3　**lldp** {**run** | **holdtime** *seconds*| **reinit** | **timer** *rate*| **tlv-select**}

ステップ 4　**end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**lldp run**
	
	例：
	`Router(config)# lldp run`
	
	または
	lldp holdtime *seconds*
	
	例：
	`Router(config)# lldp holdtime 100`
	
	または
	lldp reinit
	
	例：
	`Router(config)# lldp reinit 2`
	
	または
	lldp timer ***rate***
	
	例：
	`Router(config)# lldp timer 75`
	
	または
	lldp tlv-select
	
	例：
	`Router(config-if)# lldp tlv-select system-description`
		ルータのすべてのインターフェイス上で LLDP をグローバルにイネーブルにします。
		保持時間を指定します。値の範囲は、0 ～ 65535 秒です。デフォルト値は 120 秒です。
		任意のインターフェイス上で LLDP を初期化する際の遅延時間を秒単位で指定します。
		値の範囲は、2 ～ 5 秒です。デフォルト値は 2 秒です。
		LLDP パケットが送信されるレートを指定します。値の範囲は、5 ～ 65534 秒です。デフォルト値は 30 秒です。
		サポートされるインターフェイスで特定の LLDP TLV をイネーブルにします。
		• **management-address**：管理アドレス TLV を指定します。
		• **port-description**：ポート記述 TLV を指定します。
		• **system-capabilities**：システム機能 TLV を指定します。
		• **system-description**：システム記述 TLV を指定します
		• **system-name**：システム名 TLV を指定します。

ステップ 4	**end** **例：** `Router(config-if)# end`	CLI を特権 EXEC モードに戻します。

設定例

これは、LLDP をグローバルにイネーブルにする例です。

```
Router> enable
Router# configure terminal
Router(config)# lldp run
Router(config)# end
```

次に、LLDP がイネーブルなデバイスに対して保持時間を定義する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# lldp holdtime 100
Router(config)# end
```

次に、LLDP が初期化する際の遅延時間を秒単位で指定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# lldp reinit 2
Router(config)# end
```

次に、Cisco IOS ソフトウェアが LLDP アップデートを隣接デバイスに送信する間隔を指定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# lldp timer 75
Router(config)# end
```

次に、LLDP TLV をサポートされているインターフェイスでイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# lldp tlv-select system-description
Router(config-if)# end
```

LLDP のモニタリングと維持

LLDP のモニタリングと維持を行うには、次の手順を実行します。

手順の概要

ステップ 1　**enable**

ステップ 2　**show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*] | **neighbors** [**ethernet** *number* | **detail**] | **traffic**]

ステップ 3　**clear lldp** {**counters** | **table**}

ステップ 4　**end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*] | **neighbors** [**ethernet** *number* | **detail**] | **traffic**] **例：** `Router# show lldp entry *`	LLDP 情報を表示します。 • **entry**：特定のネイバー エントリに関する情報を指定します。 • **error**：LLDP 計算エラーおよびオーバーフローを指定します • **interface**：LLDP インターフェイスのステータスおよび設定を指定します • **neighbors**：LLDP ネイバー エントリを指定します • **traffic**：LLDP 統計情報を指定します。 • **|**：出力修飾子を指定します （注）　**show lldp neighbors** コマンドを使用し、デバイス ID が 20 文字を超える場合、ID は表示制限によりコマンド出力で 20 文字に切り詰められます。
ステップ 3	**clear lldp {counters | table}** **例：** `Router# clear lldp counters`	LLDP トラフィック カウンタおよびテーブルをゼロにリセットします。
ステップ 4	**end** **例：** `Router# end`	CLI をユーザ EXEC モードに戻します。

設定例

次に、LLDP のモニタリングと維持を行う例を示します。

```
Router> enable
Router# show lldp entry *
Router# clear lldp counters
Router# end
```

設定の確認

ここでは、Cisco 7600 シリーズ ルータ上の LLDP の設定を確認するためのコマンドを示します。

```
Router# show lldp ?
      entry      Information for specific neighbor entry
      errors     LLDP computational errors and overflows
      interface  LLDP interface status and configuration
      neighbors  LLDP neighbor entries
      traffic    LLDP statistics
      |          Output modifiers
      <cr>
```

```
Router# show lldp entry *

    Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
    ----------------------------------------------
    Chassis id: 001b.0de4.9040
    Port id: Te5/4
    Port Description: TenGigabitEthernet5/4
    System Name: RSP

    System Description:
    Cisco IOS Software, rsp72043_rp Software (rsp72043_rp-ADVENTERPRISEK9_DBG-M),
    Experimental Version 15.1(20101020:182513) [mcp_dev-kalnaray-lldp-mcp-lds 202]
    Copyright (c) 1986-2010 by Cisco Systems, Inc.
    Compiled Sun 24-Oct-10 23:59 by kalnaray

    Time remaining: 113 seconds
    System Capabilities: B,R
    Enabled Capabilities: R
    Management Addresses:
        IP: 182.0.0.1
    Auto Negotiation - not supported
    Physical media capabilities - not advertised
    Media Attachment Unit type - not advertised
    Vlan ID: - not advertised
    Total entries displayed: 1

Router# show lldp errors

    LLDP errors/overflows:
        Total memory allocation failures: 0
        Total encapsulation failures: 0
        Total input queue overflows: 0
        Total table overflows: 0

Router# show lldp interface

    TenGigabitEthernet1/1:
        Tx: enabled
        Rx: enabled
        Tx state: IDLE
        Rx state: WAIT FOR FRAME

    TenGigabitEthernet1/2:
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

    TenGigabitEthernet1/3:
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

    TenGigabitEthernet1/4:
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

    GigabitEthernet5/1:
```

```
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

    GigabitEthernet5/2:
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

    Control Plane:
        Tx: enabled
        Rx: enabled
        Tx state: INIT
        Rx state: WAIT PORT OPER

Router# show lldp neighbors
    Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

    Device ID           Local Intf     Hold-time  Capability      Port ID
    RSP                 Te1/1          120        R               Te5/4

    Total entries displayed: 1

Router# show lldp traffic

    LLDP traffic statistics:
        Total frames out: 8
        Total entries aged: 0
        Total frames in: 4
        Total frames received in error: 0
        Total frames discarded: 0
        Total TLVs discarded: 0
        Total TLVs unrecognized: 0

Router# clear lldp ?
      counters  Clear LLDP counters
      table     Clear lldp table

Router# show lldp

    Global LLDP Information:
        Status: ACTIVE
        LLDP advertisements are sent every 30 seconds
        LLDP hold time advertised is 120 seconds
        LLDP interface reinitialisation delay is 2 seconds
```

トラブルシューティングのヒント

シナリオ / 問題	ソリューション

LLDP エラーに関するデバッグ情報を収集するには、どうしたらよいか。	**debug lldp errors** コマンドを使用します。次に、出力例を示します。
	`Router# debug lldp errors`
	`LLDP errors debugging is on`

LLDP で発生するすべてのイベントの詳細を収集するには、どうしたらよいか。	**debug lldp events** コマンドを使用します。次に、出力例を示します。
	`Router# debug lldp events`
	`LLDP events debugging is on`

LLDP のパケット関連のデバッグ情報を収集するには、どうしたらよいか。	**debug lldp packet** コマンドを使用します。次に、出力例を示します。
	`Router# debug lldp packet`
	`LLDP packet info debugging is on`

スイッチオーバーがあったときに、状態の変化に関するデバッグ情報を収集するには、どうしたらよいか。	**debug lldp state** コマンドを使用します。次に、出力例を示します。
	`Router# debug lldp state`
	`LLDP state debugging is on`

LLDP 設定のデバッグ コマンドを確認するには、どうしたらよいか。	**show debugging** コマンドを使用します。次に、出力例を示します。
	`Router# show debugging`
	`LLDP:`
	`  LLDP packet info debugging is on`
	`  LLDP events debugging is on`
	`  LLDP errors debugging is on`
	`  LLDP states debugging is on`

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、Cisco 7600 シリーズ ルータにレイヤ 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 7600 Series Routers Command References』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.18-1）
- 「レイヤ 2 プロトコル トンネリングのサポートの設定」（P.18-2）

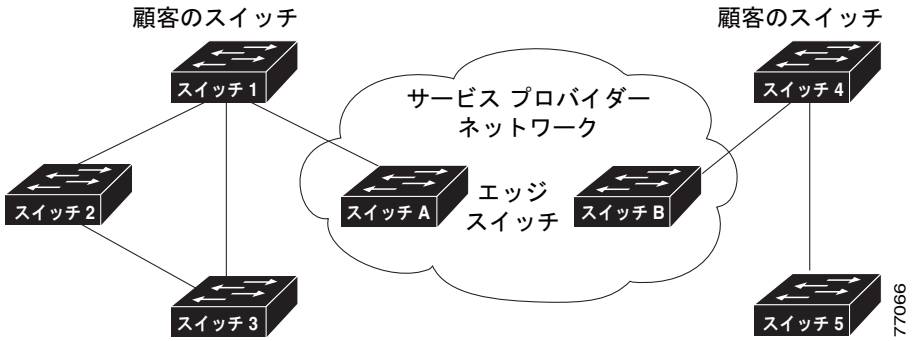
レイヤ 2 プロトコル トンネリングの機能概要

レイヤ 2 プロトコル トンネリングを使用すると、レイヤ 2 プロトコル データ ユニット（PDU）（CDP、STP、および VTP）をネットワーク経由でトンネリングできます。ここで使用する用語は、次のとおりです。

- エッジ ルータ：カスタマー ルータに接続されていて、サービス プロバイダー ネットワークの境界に配置されているルータ（図 18-1 を参照）
- レイヤ 2 プロトコル トンネル ポート：エッジ ルータ上の、特定のトンネリング プロトコルをカプセル化またはカプセル化解除できるポート。レイヤ 2 プロトコル トンネル ポートは CLI 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 パケットをドロップし、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 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、ルータ 1 上の VLAN 用の STP（図 18-1 を参照）によって、スイッチ 4 および 5 に基づくコンバージェンス パラメータを考慮せずに、スイッチ 1、2、3 上でスパニングツリー トポロジ が作成されます。顧客に単一のスパニング ツリー ドメインを提供できるようにするため、制御プロトコル PDU（CDP、STP、および VTP）用に BPDU をトンネリングする一般スキームが作成されます。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 ルータは、特殊なカプセル化フレームを待ち受けて、カプセル化を解除し、さらにトンネルから外へ転送します。

カプセル化では、PDU 内の宛先 Media Access Control（MAC; メディア アクセス コントロール）アドレスも書き換えられます。入力エッジ ルータは、レイヤ 2 トンネル ポートで受信した PDU の宛先 MAC アドレスをシスコ独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）に書き換えます。次に、PDU はレイヤ 2 トンネル ポートのネイティブ VLAN 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すると、ディセーブルになったプロトコルは、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様に動作します。

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、ルータ上の同じ VLAN にある別のトンネル ポートから伝送されます。
- 次のように、レイヤ 2 プロトコル トンネリング ポートでジャンボ フレーム サポートを設定してください。
  - 「ジャンボ フレーム サポートの設定」（P.8-9）を参照してください。
  - 「ジャンボ フレーム サポートの設定」で指定されている、ジャンボ フレームをサポートしないモジュールをメモします。

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かぎり、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**]	指定したプロトコル（複数可）用のレイヤ 2 プロトコル トンネル ポートとして、レイヤ 2 ポートを設定します。 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、以下に注意してください。

- 任意で、ポートにドロップしきい値を指定することもできます。1 ～ 4096 のドロップしきい値は、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。シャットダウンしきい値を指定しない場合、値は 0 です（シャットダウンしきい値はディセーブルです）。
- 任意で、ポートにシャットダウンしきい値を指定することもできます。1 ～ 4096 のシャットダウンしきい値によって、そのインターフェイス上で 1 秒間にそのプロトコルに関して処理されるパケット数が決まります。シャットダウンしきい値を超えると、ポートは errdisable ステートになります。シャットダウンしきい値を指定しない場合、値は 0 です（シャットダウンしきい値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 7600 Series Router Cisco IOS Command Reference*』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シャットダウンしきい値を設定し、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クリアする例を示します。

```
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

L2TPv3 の設定

この章では、Cisco IOS Software Release 15.1(3)S で L2TPv3 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 の『Cisco 7600 Series Router Cisco IOS Command Reference』を参照してください。
http://www.cisco.com/en/US/products/ps6922/prod_command_reference_list.html

この章の内容は次のとおりです。

- 「L2TPv3 の概要」（P.19-1）
- 「L2TPv3 の設定」（P.19-2）

L2TPv3 の概要

Layer 2 Tunneling Protocol version 3（L2TPv3; レイヤ 2 トンネリング プロトコル バージョン 3）機能は、L2TPv3 と疑似回線（PW）テクノロジーを使用してイーサネット トラフィックにトンネリング サービスを提供します。この機能は、RFC3985 Pseudowire Emulation Edge-to-Edge（PWE3）アーキテクチャで推奨されるネットワーク トポロジのプロバイダー エッジ（PE）ルータとして機能する SUP720-3B/3BXL および RSP720 ルータ用に開発されました。また、L2TPv3 は、Cisco 7600 ルータと、標準準拠のシスコ デバイスまたは非シスコ デバイスとの間の相互運用性をサポートします。

L2TPv3 トンネルは、2 台の PE ルータ間の制御接続です。1 つの L2TPv3 トンネルが複数のデータ接続を持つことができ、各データ接続は L2TPv3 セッションと呼ばれます。制御接続は、セッションの確立、維持、および解放に使用されます。各セッションは、ルータ全体で固有のセッション ID によって識別されます。

図 19-1　L2TPv3 対応のネットワーク トポロジ

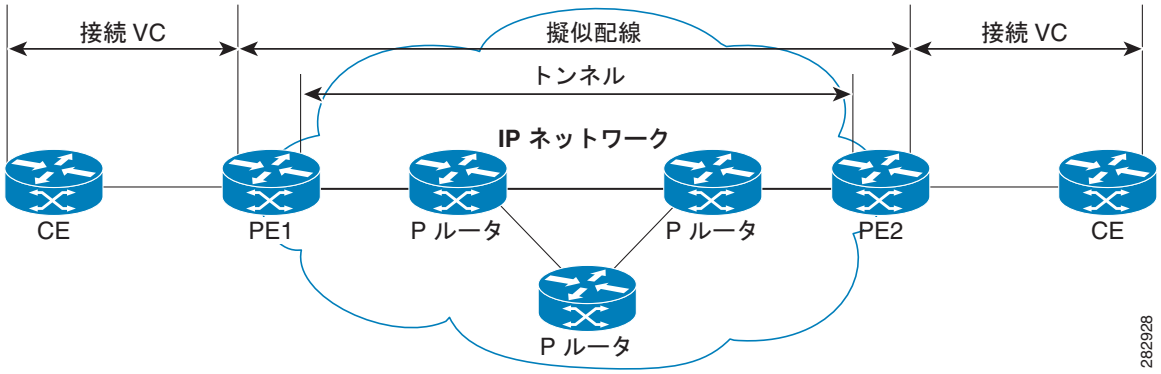


図 19-1 では、接続仮想回線（VC）が、カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイスを接続する物理または論理ポートを表しています。疑似回線は、2 つの接続 VC を接続する VC として定義され、各方向に 1 つずつ、計 2 つの L2TPv3 トンネル パスで構成されます。

L2TPv3 の制約事項

L2TPv3 には、次の制約事項が適用されます。

- レイヤ 2 相対ラインカードは L2TPv3 対応ラインカードにする必要があります。
- レイヤ 2 相対ラインカードごとに 1 つ以上の異なる L2TPv3 トンネルが必要です。
- Cisco 7600 ルータの L2TPv3 機能は、ES+ および SIP 400 ラインカードでサポートされます。
- Cisco 7600 ルータは、レイヤ 2 フレーム対応の IPv4 トンネリングのみサポートします。
- L2TPv3 機能は、カプセル化する PE での EoL2TPv3oMPLS などの設定はサポートしません。
- L2TPv3 機能は、最大 16,000 の疑似回線をサポートします。
- L2TPv3 は EVC 機能と同時にサポートされません。L2TPv3 は、EVC と同じポートに存在します。つまり、一方のサブインターフェイスが L2TP を介した dot1q タグ付きトラフィックのトンネリングに使用され、もう一方のサブインターフェイスは EVC 機能の実行に使用されます。
- Cisco IOS Release 15.1(3)S では、ES+ ラインカードで 4000 の IP トンネルがサポートされます。
- L2TPv3 機能は SSO をサポートしません。HA セットアップで L2TPv3 セッションに対するクッキーをイネーブルにする必要があります。

L2TPv3 の設定

L2TPv3 の設定については、
http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html を参照してください。

CHAPTER 20

STP および MST の設定

この章では、Cisco 7600 シリーズ ルータにスパニングツリー プロトコル（STP）および 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。

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章で説明する内容は、次のとおりです。

- 「STP の機能概要」（P.20-1）
- 「IEEE 802.1w RSTP の機能概要」（P.20-13）
- 「MST の概要」（P.20-18）
- 「STP の設定」（P.20-26）
- 「MST の設定」（P.20-37）
- 「MST の設定およびステータスの表示」（P.20-50）

（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 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 の機能概要について説明します。

- 「STP の概要」（P.20-2）
- 「ブリッジ ID の概要」（P.20-2）
- 「BPDU の概要」（P.20-3）
- 「ルート ブリッジの選定」（P.20-4）
- 「STP プロトコル タイマー」（P.20-4）
- 「スパニングツリー トポロジーの作成」（P.20-5）
- 「STP ポート ステート」（P.20-5）
- 「STP および IEEE 802.1Q トランク」（P.20-12）

STP の概要

STP は、ネットワークの不要なループを防止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ためには、任意の 2 つのステーション間にアクティブ パスを 1 つだけにする必要があります。STP の動作はエンド ステーションに対してトランスペアレントなので、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することはできません。

Cisco 7600 シリーズ ルータは、すべての VLAN 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 パスを構築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 デバイス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します。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 デバイスが複数のレイヤ 2 LAN ポート上でエンド ステーション MAC アドレスを学習したりする可能性があります。このような状況によって、ネットワークが不安定になります。

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 デバイスへのループフリー 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 トポロジーを再計算し、スタンバイ パスをアクティブにします。

ネットワーク デバイス上の 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 トポロジーにおけるポートの位置を表すとともに、その位置によってポートがどれだけ効率的にトラフィックを通過させることができるかを表します。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 デバイス上の各 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 アドレス割り当て」（P.20-3）

ブリッジ プライオリティ値

（注）　Cisco 7600 シリーズ ルータでは、拡張システム ID が常にイネーブルになっています。

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 20-1（P.20-3）および「VLAN のブリッジ プライオリティの設定」（P.20-34）を参照）。

拡張システム ID

12 ビットの拡張システム ID フィールドは、ブリッジ ID の一部です（表 20-1（P.20-3）を参照）。Cisco 7600 シリーズ ルータには、64 MAC アドレスがあり、12 ビットの拡張システム ID を常に使用します。

表 20-1　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 アドレス割り当て

Cisco 7600 シリーズ ルータでは、64 個のアドレスを使用して STP などのソフトウェア機能をサポートできます。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。

STP は、拡張システム ID および MAC アドレスを使用して、VLAN ごとにブリッジ ID を一意にします。

MAC アドレス リダクションを任意のデバイスでイネーブルにしている場合は、その他すべてのレイヤ 2 接続ネットワーク デバイスでも MAC アドレス リダクションをイネーブルにして、望ましくないルート ブリッジ選択およびスパニングツリー トポロジーの問題を避ける必要があります。

MAC アドレス リダクションをイネーブルにすると、ルート ブリッジ プライオリティは、4096 + VLAN ID の倍数となります。MAC アドレス リダクションがイネーブルの場合、ルータのブリッジ ID（スパニングツリー アルゴリズムで、ルート ブリッジのアイデンティティを判別するために使用され、最小のものが優先される）に指定できるのは、4096 の倍数だけです。使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 だけです。

同じスパニングツリー ドメイン内の別のブリッジが MAC アドレス リダクション機能を実行しない場合、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。

BPDU の概要

ブリッジ プロトコル データ ユニット（BPDU）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 デバイス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 デバイスがルート ブリッジになると見なしているネットワーク デバイスの固有のブリッジ 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 ID
- 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 デバイスが 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 デバイスが BPDU を受信します。ネットワーク デバイスが BPDU を受信すると、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、トポロジーが変更されると、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 つのネットワーク デバイスがルート 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 デバイスのルート 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 デバイスであり、このネットワーク デバイス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 デバイスがルート ブリッジとして選定されます。すべてのネットワーク デバイスがデフォルト 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 デバイスがルート 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、ルータがルート ブリッジとして選定される確率が変わります。大きな値を設定するとその確率が高くなり、小さな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 トポロジー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でも、ルート ブリッジに到達するために必要でないパスは、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 セグメントの指定ポートを判別します。

STP プロトコル タイマー

表 20-2 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。

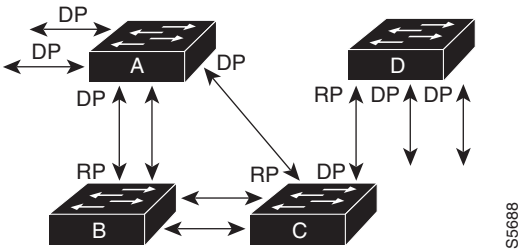
表 20-2　STP プロトコル タイマー

変数	説明
Hello タイマー	ネットワーク デバイスが他のネットワーク デバイスへ 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に、リスニング ステートおよびラーニング ステートが継続する必要があ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 デバイス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 トポロジーの作成

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 デバイスのブリッジ 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 デバイスがルート ブリッジになるように、デバイス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 デバイスを使用する、新しいスパニングツリー トポロジーを形成するように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 トポロジー



RP = ルート ポート
DP = 指定ポート

スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、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 ポートよりも高いプライオリティに変更すると（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」（P.20-6）

- 「ブロッキング ステート」（P.20-7）
- 「リスニング ステート」（P.20-8）
- 「ラーニング ステート」（P.20-9）
- 「フォワーディング ステート」（P.20-10）
- 「ディセーブル ステート」（P.20-11）

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 を通過する場合、伝播遅延が生じる可能性があります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーが変更される場合があります。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 ステートに直接遷移すると、一時的にデータ ループが発生する可能性があります。ポートは新しいトポロジー情報がスイッチド 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、古いトポロジーを使用して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 Cisco 7600 シリーズ ルータ上の各レイヤ 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。

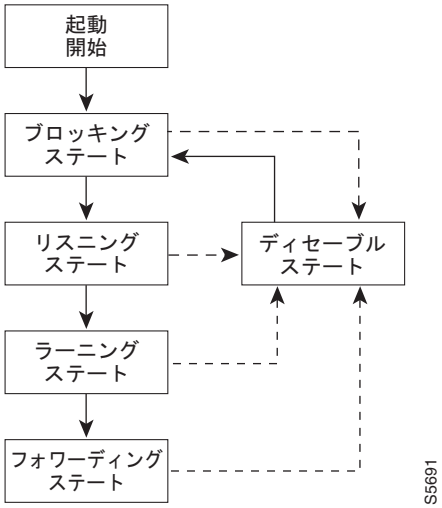
- ブロッキング：レイヤ 2 LAN ポートはフレーム転送に参加しません。
- リスニング：レイヤ 2 LAN ポートがフレーム転送に参加すべきであると STP が判断した場合に、ブロッキング ステートのあとで最初に開始する移行ステートです。
- ラーニング：レイヤ 2 LAN ポートがフレーム転送に参加する準備をしている状態です。
- フォワーディング：レイヤ 2 LAN ポートはフレームを転送します。
- ディセーブル：レイヤ 2 LAN ポートが STP に参加せず、フレームを転送しません。

レイヤ 2 LAN ポートは、次のように 5 種類のステートに移行します。

- 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、Cisco 7600 シリーズ ルータ、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。

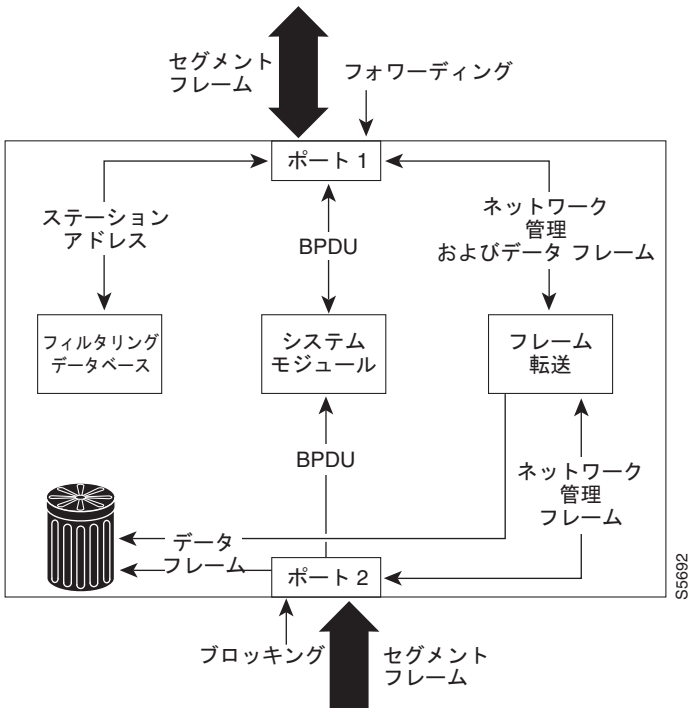
STP アルゴリズムによってレイヤ 2 LAN ポートがフォワーディング ステートになると、次の処理が行われます。

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、レイヤ 2 LAN ポートをラーニング ステートに移行し、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 ステーションが位置情報を学習します。
4. レイヤ 2 LAN ポートは、転送遅延タイマーがタイムアウトになるまで待機します。タイムアウトになったら、レイヤ 2 LAN ポートをフォワーディング ステートに移行します。フォワーディング ステートでは、ラーニング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 デバイスは、他のネットワーク デバイスと BPDU を交換するまで、そのネットワーク デバイス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 デバイス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 デバイスが 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失効し、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



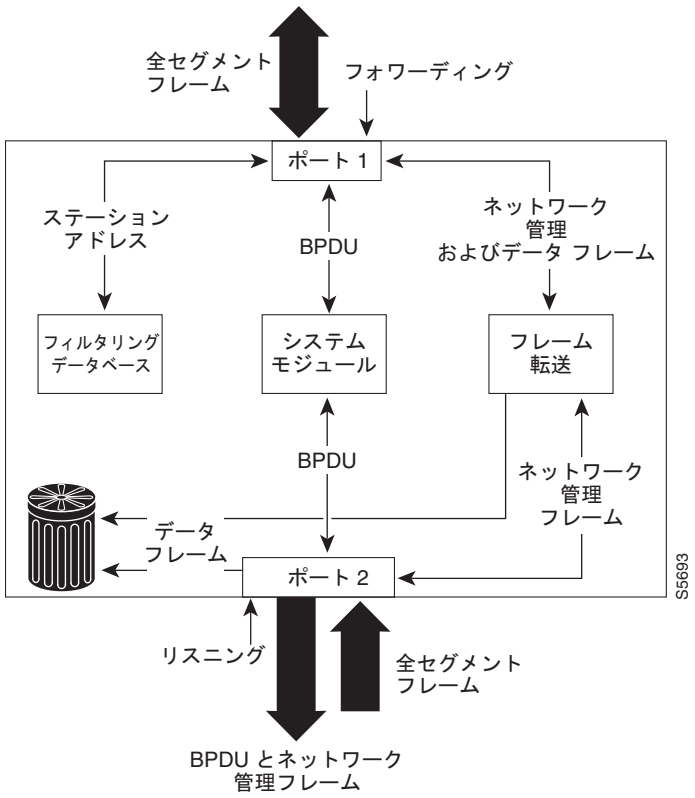
ブロッキング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 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 ステーションの位置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



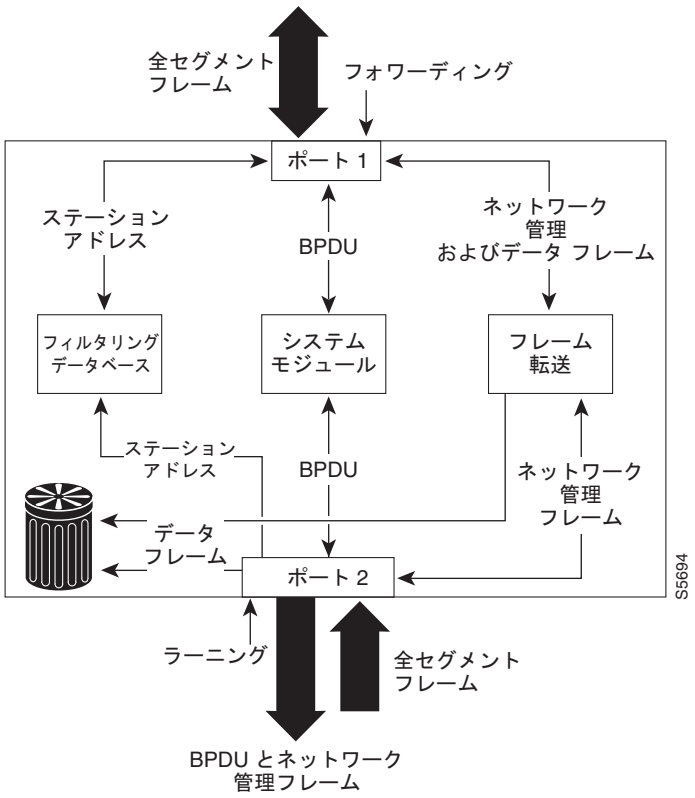
リスニング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 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 ステーションの位置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 モジュールから受信した BPDU を、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



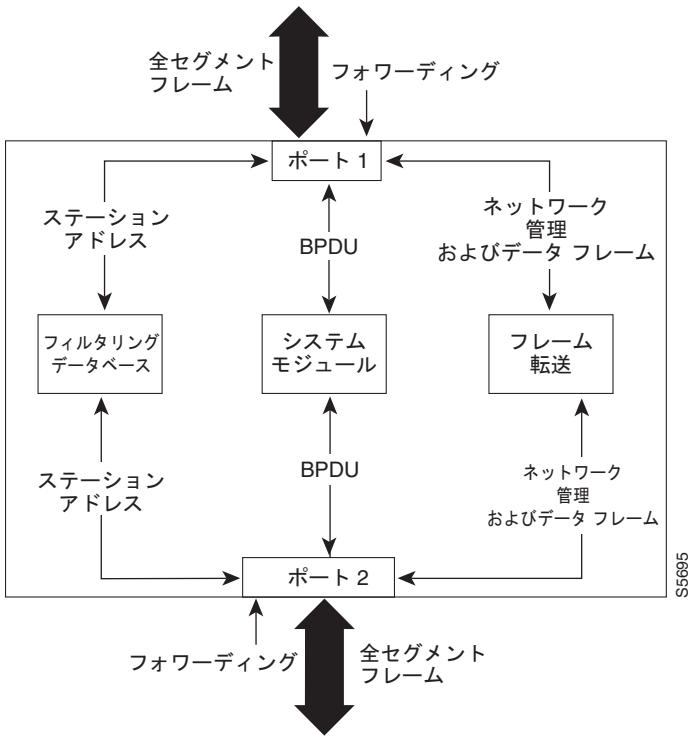
ラーニング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 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 ステーションの位置情報をアドレス 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



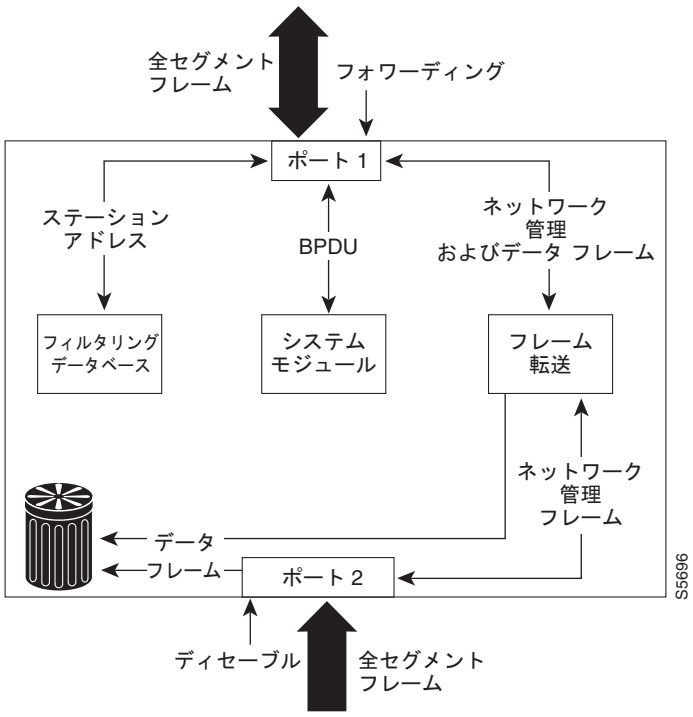
フォワーディング ステートのレイヤ 2 LAN ポートは、次の処理を実行します。

- 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 ステーションの位置情報をアドレス 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



ディセーブルになったレイヤ 2 LAN ポートは、次の処理を実行します。

- 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 ステーションの位置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 デバイスを使用したネットワークでは、ネットワーク デバイスがトランク上で許容される VLAN ごとに 1 つの STP インスタンスを維持します。しかし、他社製の 802.1Q ネットワーク デバイスでは、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 デバイスを他社製のネットワーク デバイスに接続する場合、シスコのネットワーク デバイスは、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 デバイス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 デバイスのクラウドと切り離されて、シスコのネットワーク デバイスによって維持されます。シスコのネットワーク デバイス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 デバイス間の単一トランク 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 RSTP の機能概要

RSTP ではポイントツーポイント配線が活用され、スパニングツリーの高速コンバージェンスが提供されます。スパニングツリーの再設定は 1 秒以内に発生します（802.1D スパニングツリーのデフォルト設定では 50 秒）。

ここでは、RSTP の機能概要について説明します。

- 「ポートの役割およびアクティブ トポロジー」（P.20-13）
- 「高速コンバージェンス」（P.20-14）
- 「ポートの役割の同期」（P.20-15）
- 「BPDU の形式および処理」（P.20-16）
- 「トポロジの変更」（P.20-18）
- 「Rapid PVST」（P.20-18）

ポートの役割およびアクティブ トポロジー

RSTP では、ポートの役割の割り当て、およびアクティブ トポロジーの学習により、スパニングツリーの高速コンバージェンスが可能になります。RSTP は 802.1D STP 上に構築され、スイッチ プライオリティが最も高い（プライオリティの数値が最も小さい）ルータが、「ルート ブリッジの選定」（P.20-4）で説明したようにルート ブリッジとして選択されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルート ポート：ルータがルート ブリッジにパケットを転送するとき、最適なパス（最低コスト）を提供します。
- DP：指定ルータに接続し、その LAN からルート ブリッジにパケットを転送するとき、パス コストを最低にします。DP は、指定ルータが LAN に接続されているポートです。
- 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：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートは、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 リンクによって接続されるか、共有 LAN セグメントとの複数の接続がルータにある場合に限って存在できます。
- ディセーブル ポート：スパニング ツリーの動作において何もロールが与えられていません。

ルート ポートまたは DP の役割があるポートは、アクティブ トポロジーに組み込まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、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ポートの役割が一貫している安定したトポロジーの場合、RSTP は、すべてのルート ポートおよび DP をフォワーディング ステートにすぐに移行しますが、すべての代替ポートおよびバックアップ ポートは常に廃棄ステートになります（802.1D のブロッキングに相当）。ポートのステートにより、転送処理および学習処理の動作が制御されます。802.1D および RSTP のポート ステートの比較については、表 20-3 を参照してください。

表 20-3　ポート ステートの比較

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	No
イネーブル	リスニング	廃棄	No

表 20-3　ポート ステートの比較 （続き）

動作ステータス	STP ポート ステート（IEEE 802.1D）	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ラーニング	ラーニング	Yes
イネーブル	フォワーディング	フォワーディング	Yes
ディセーブル	ディセーブル	廃棄	No

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを*廃棄*ではなく*ブロッキング*として定義します。DP 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 は、ルータ、ルータ ポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。エッジ ポート、新しいルート ポート、ポイントツーポイント リンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- 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 ルータでエッジ ポートとしてポートを設定した場合、エッジ ポートはフォワーディング ステートにすぐに移行します。エッジ ポートは Port Fast 対応ポートと同じであり、単一エンド ステーションに接続しているポートだけでイネーブルにする必要があります。
- ルート ポート：RSTP は、新しいルート ポートを選択した場合、古いルート ポートをブロックし、新しいルート ポートをフォワーディング ステートにすぐに移行します。
- ポイントツーポイント リンク：ポイントツーポイント リンクで別のポートにポートを接続し、ローカル ポートが DP になると、提案と合意のハンドシェークを使用して別のポートと高速移行がネゴシエーションされ、ループがないトポロジーが確保されます。

  図 20-8 で示すように、ルータ A がポイントツーポイント リンク経由でルータ B に接続し、すべてのポートはブロッキング ステートになります。ルータ A のプライオリティの数値が、ルータ B のプライオリティより小さいとします。ルータ A は提案メッセージ（提案フラグを設定した設定 BPDU）をルータ B に送信し、指定ルータとして自分自身を提案します。

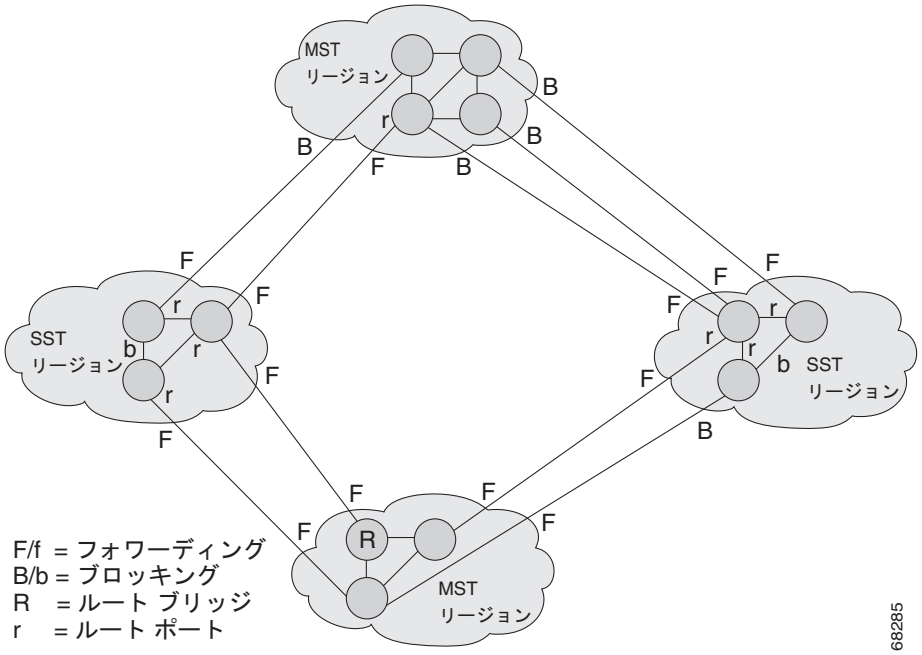
  ルータ B は、提案メッセージの受信後、提案メッセージを受信したポートを新しいルート ポートとして選択し、エッジ以外のすべてのポートを強制的にブロッキング ステートにして、新しいルート ポートを介して合意メッセージ（合意フラグを設定した BPDU）を送信します。

  ルータ A も、ルータ B の合意メッセージの受信後、指定ポートをフォワーディング ステートにすぐに移行します。ルータ B はすべてのエッジ以外のポートをブロックし、ルータ A およびルータ B の間にポイントツーポイント リンクがあるので、ネットワークにループは形成されません。

  ルータ C がルータ B に接続すると、同様のセットのハンドシェーク メッセージが交換されます。ルータ C はルータ B に接続されているポートをルート ポートとして選択し、両端がフォワーディング ステートにすぐに移行します。このハンドシェーク処理を繰り返して、もう 1 つのルータがアクティブ トポロジーに加わります。ネットワークの収束時には、この提案と合意のハンドシェーク処理がスパニング ツリーのルートからリーフに進みます。

  ルータは、ポートのデュプレックス モードからリンク タイプを学習します。全二重ポートはポイントツーポイント接続、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 コマンドを使用すると、デュプレックス設定によって制御されるデフォルト設定を無効にすることができます。

図 20-8　高速コンバージェンスの提案と合意のハンドシェーク



ポートの役割の同期

ルータがそのルータのポートの 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 によってその他すべてのポートが新しいルートの情報と強制的に同期化します。

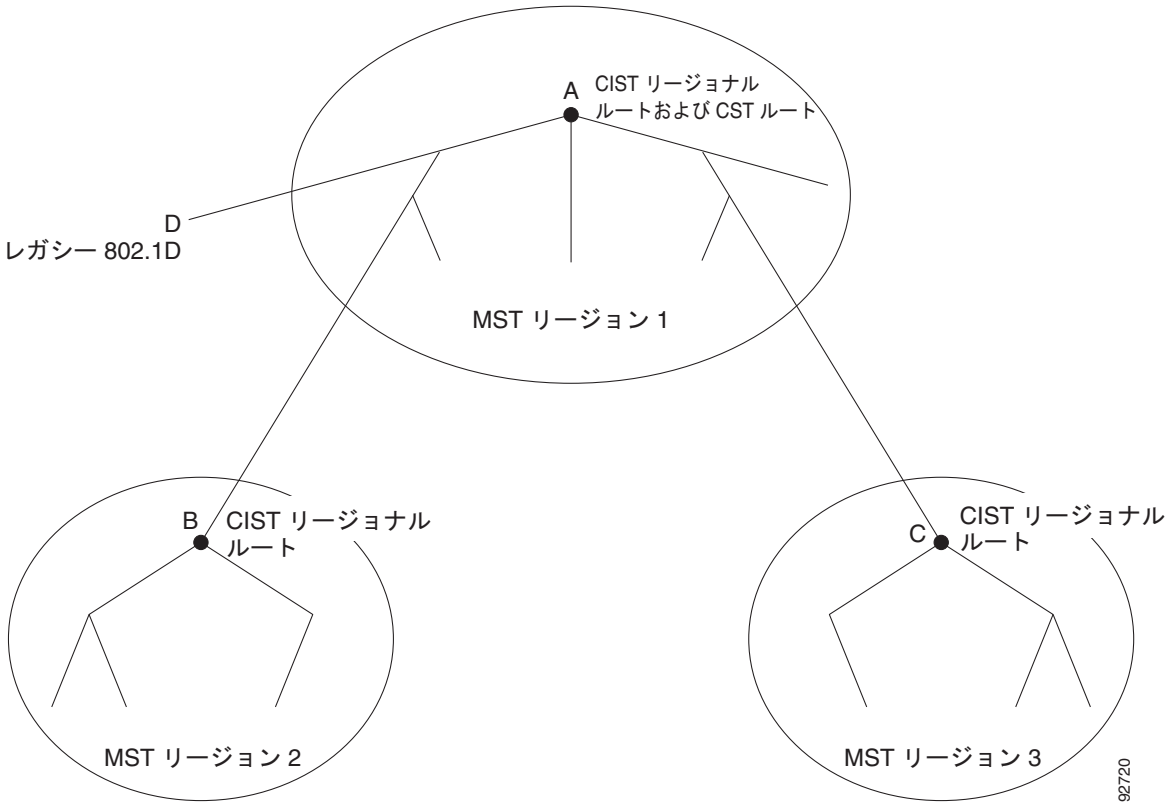
その他すべてのポートが同期化されている場合、ルータはルート ポートで受信した上位ルート情報で同期化されます。ルータのそれぞれのポートは、次のような場合に同期化します。

- ポートがブロッキング ステートである。
- エッジ ポート（ネットワークのエッジに存在するように設定されたポート）である。

DP は、フォワーディング ステートになっていてエッジ ポートとして設定されていない場合、RSTP によって DP が強制的に新しいルート情報で同期化すると、DP がブロッキング ステートに移行します。一般的に RSTP がルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポート ステートはブロッキングに設定されます。

ルータは、すべてのポートが同期化されたことを確認した後で、ルート ポートに対応する指定ルータに合意メッセージを送信します。ポイントツーポイント リンクで接続されたルータがポートの役割で合意すると、RSTP はポート ステートをフォワーディングにすぐに移行します。イベントのシーケンスについては、図 20-9 を参照してください。

図 20-9　高速コンバージェンス中のイベントのシーケンス



BPDU の形式および処理

ここでは、ブリッジ プロトコル データ ユニット（BPDU）の形式および処理について説明します。

- 「BPDU の形式および処理の概要」（P.20-16）
- 「優位 BPDU 情報の処理」（P.20-17）
- 「下位 BPDU 情報の処理」（P.20-17）

BPDU の形式および処理の概要

RSTP BPDU の形式は 802.1D BPDU の形式と同じですが、プロトコル バージョンは 2 に設定されます。新しい 1 バイトの Version 1 Length フィールドはゼロに設定されます。つまり、バージョン 1 のプロトコル情報は存在しません。表 20-4 に、RSTP フラグ フィールドを示します。

表 20-4　RSTP BPDU フラグ

ビット	機能
0	Topology change（TC; トポロジーの変化）
1	提案

表 20-4　RSTP BPDU フラグ （続き）

ビット	機能
2 ～ 3:	ポートの役割：
00	Unknown
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
6	合意
7	Topology Change Acknowledgement（TCA; トポロジー変更確認応答）

送信側ルータは RSTP BPDU の提案フラグを設定し、その LAN の指定ルータとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側ルータは、RSTP BPDU の合意フラグを設定して以前の提案を受け入れます。合意メッセージのポートの役割は、常にルート ポートに設定されます。

RSTP には TCN BPDU がありません。TC フラグが使用されて、TC が示されます。ただ 802.1D ルータとのインターオペラビリティのため、RSTP ルータは TCN BPDU の処理と生成を行います。

ラーニング フラグおよびフォワーディング フラグは、送信側ポートのステートに従って設定されます。

優位 BPDU 情報の処理

上位 BPDU は、ルート情報（低いスイッチ ID や低いパス コストなど）を持つ BPDU であり、ポート用に現在保存されているものより上位になります。

ポートが上位 BPDU を受信すると、RSTP は再設定を開始します。ポートが新しいルート ポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、ルータはその他すべてのポートが同期化されてから合意メッセージを送信します。BPDU が 802.1D BPDU である場合、ルータは提案フラグを設定せず、ポートの転送遅延タイマーを開始します。新しいルート ポートでは、フォワーディング ステートに移行するために、2 倍の転送遅延時間が必要となります。

ポートで受信した上位情報によってポートがバックアップ ポートか代替ポートになった場合、RSTP はそのポートをブロッキング ステートに設定して合意メッセージを送信します。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、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、ルート情報（高いスイッチ ID や高いパス コストなど）を持つ BPDU であり、ポート用に現在保存されているものより下位になります。

指定ポートは、下位 BPDU を受信すると、独自の情報ですぐに応答します。

トポロジの変更

RSTP と 802.1D の間では、スパニングツリーの TC の処理が異なります。

- 検出：ブロッキング ステートとフォワーディング ステート間の*いずれか*の移行によって TC が発生する 802.1D とは異なり、ブロッキング ステートからフォワーディング ステートへの移行*だけ*が、RSTP で TC の原因となります（接続の増加だけが TC と見なされます）。エッジ ポートにおけるステート変更は、TC の原因になりません。RSTP ルータは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。
- 通知：802.1D とは異なり、RSTP は TCN BPDU を使用しません。ただし 802.1D とのインターオペラビリティを保つため、RSTP ルータは TCN BPDU の処理と生成を行います。
- 確認応答：RSTP ルータは、802.1D ルータから DP で TCN メッセージを受信すると、TCA ビットを設定した 802.1D 設定 BPDU で応答します。ただし 802.1D ルータに接続しているルート ポートで TC-while タイマー（802.1D の TC タイマーと同じ）がアクティブであり、TCA が設定された設定 BPDU を受信した場合、TC-while タイマーはリセットされます。

  この動作方式が必要なのは、802.1D ルータを介してサポートする場合だけです。RSTP BPDU は TCA ビットが設定されていません。
- 伝播：RSTP ルータは、DP またはルート ポートを介して別のルータから TC メッセージを受信すると、エッジ以外のすべての DP、およびルート ポート（TC メッセージを受信したポートを除く）に変更を伝播します。ルータはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。
- プロトコル移行：802.1D ルータとの下位互換性を保つため、RSTP は 802.1D 設定 BPDU および TCN BPDU をポートごとに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 が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブである間、ルータはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

  ルータは、ポートの移行遅延タイマーの期限が切れたあとに 802.1D BPDU を受信した場合、802.1D ルータに接続されたと認識し、802.1D BPDU だけの使用を開始します。ただし RSTP ルータは、ポートで 802.1D BPDU を使用していて、タイマーが切れたあとで RSTP BPDU を受信すると、タイマーを再開してそのポートにおける RSTP BPDU の使用を開始します。

Rapid PVST

Rapid PVST は既存の PVST+ 用の設定を使用しますが、Rapid PVST は RSTP を使用した方がコンバージェンスが速くなります。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、TC 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 設定は Rapid PVST モードでは無視され、両機能は RSTP に含まれます。

MST の概要

ここでは MST について説明します。

- 「MST の概要」（P.20-19）
- 「MST 領域」（P.20-19）
- 「IST、CIST、CST」（P.20-20）

- 「ホップ カウント」（P.20-23）
- 「境界ポート」（P.20-23）
- 「規格準拠 MST 実装」（P.20-24）
- 「IEEE 802.1D-1998 STP とのインターオペラビリティ」（P.20-26）

MST の概要

MST では複数の VLAN がスパニングツリー インスタンスにマッピングされ、それぞれのインスタンスには、その他のスパニングツリー インスタンスに依存しないスパニングツリー トポロジーが含まれます。このアーキテクチャによって複数の転送パスがデータ トラフィックに提供され、ロードバランスが可能になり、多数の VLAN のサポートに必要となるスパニングツリー インスタンスの数が減ります。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向上します。

最も一般的には、レイヤ 2 スイッチド ネットワークのバックボーン レイヤおよび配布レイヤに最初に MST を配置します。この配置では、サービス プロバイダー環境で必要となる、一種の高可用性ネットワークが提供されます。

MST では明示的なハンドシェークによって高速スパニングツリー コンバージェンスが提供され、802.1D 転送遅延がなくなり、ルート ブリッジ ポートおよび DP がフォワーディング ステートに高速で移行します。

MST ではスパニング ツリーの動作が改善され、次の STP バージョンとの下位互換性を維持しています。

- 元の 802.1D スパニング ツリー
- 既存のシスコ固有の Multiple Instance STP（MISTP）
- 既存のシスコの PVST+
- 高速 Per-VLAN Spanning Tree Plus（高速 PVST+）

Port Fast、UplinkFast、ルート ガードなど、その他のスパニングツリー機能については、第 21 章「オプションの STP 機能の設定」を参照してください。

（注）
- IEEE 802.1w では RSTP が定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1s では MST が規定されて、IEEE 802.1Q に組み込まれました。

MST 領域

ルータが MST インスタンスに参加するには、同一 MST 設定情報でルータを一貫して設定する必要があります。MST 設定が同じである相互接続ルータの集合は、図 20-10（P.20-22）に示す MST リージョンを構成します。

MST 設定では、それぞれのルータが属する MST リージョンが制御されます。設定には、リージョンの名前、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ます。

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP ブリッジ プロトコル データ ユニット（BPDU）を処理できる必要があります。ネットワークにおける MST リージョンの数に制限はありませんが、各リージョンでは 65 まで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 の範囲の任意の番号で識別できます。スパニングツリー インスタンスに同時に割り当てられる VLAN は 1 つだけです。

IST、CIST、CST

ここでは、Internal Spanning Tree（IST）、Common and Internal Spanning Tree（CIST）、Common Spanning Tree（CST）について説明します。

- 「IST、CIST、CST の概要」（P.20-20）
- 「MST リージョン内におけるスパニングツリーの動作」（P.20-21）
- 「MST リージョン間のスパニングツリーの動作」（P.20-21）
- 「IEEE 802.1s の用語」（P.20-22）

IST、CIST、CST の概要

MST では、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その他のスパニングツリー プロトコルとは異なり、IST、CIST、CST のスパニングツリーが確立されて維持されます。

- IST は、MST リージョンで実行するスパニングツリーです。

  それぞれの MST リージョン内では、MST によって複数のスパニングツリー インスタンスが維持されます。インスタンス 0 は、IST という、リージョンの特殊インスタンスです。その他すべての MST インスタンスには、1 ～ 4094 の番号が付きます。

  IST は、BPDU の送受信を行う唯一のスパニングツリー インスタンスです。その他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、MST BPDU 内でカプセル化されます。MST BPDU はすべてのインスタンスの情報を搬送するので、複数のスパニングツリー インスタンスをサポートするために処理する必要がある BPDU の数は大きく削減されます。

  同一リージョン内のすべての MSTI は同一プロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、独自のトポロジー パラメータがあります。デフォルトでは、すべての VLAN が IST に割り当てられます。

  MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- CIST は、各 MST リージョンの IST の集合です。
- CST は、MST リージョンと単一スパニングツリーを相互接続します。

あるリージョンで算出されたスパニングツリーは、スイッチド ドメイン全体を含む CST のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D 規格をサポートするルータ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 リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内におけるスパニングツリーの動作」（P.20-21）および「MST リージョン間のスパニングツリーの動作」（P.20-21）を参照してください。

MST リージョン内におけるスパニングツリーの動作

IST は、リージョン内のすべての MST ルータを接続します。IST が収束するとき、IST のルートは、図 20-10（P.20-22）に示すように CIST リージョナル ルートになります（802.1s 規格の実装前の *IST マスター*）。ネットワークにリージョンが 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外にある場合、リージョンの境界にあるいずれかの MST ルータが CIST リージョナル ルートとして選択されます。

MST ルータは、初期化すると、CIST ルートおよび CIST リージョナル ルートへの両方のパス コストをゼロに設定して、CIST および CIST リージョナル ルートのルートとして自分自身を識別する BPDU を送信します。ルータはすべての MSTI を初期化し、そのすべてのルートであることを主張します。ルータは、ポート用に現在保存されているものより上位の MST ルート情報（低いスイッチ ID、低いパス コストなど）を受信した場合、CIST リージョナル ルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブ リージョンが含まれて、それぞれに独自の CIST リージョナル ルートが含まれることがあります。ルータは、同一リージョンのネイバーから上位 IST 情報を受信すると、古いサブ リージョンを脱退し、真の CIST リージョナル ルートを含む新しいサブ リージョンに加入します。これにより、真の CIST リージョナル ルートを含むサブ リージョンを除くすべてのサブ リージョンは縮小します。

正しい動作のためには、MST リージョンのすべてのルータが、同一 CIST リージョナル ルートで合意する必要があります。このため、リージョン内の任意の 2 つのルータは、共通 CIST リージョナル ルートに収束する場合、MSTI のポートの役割だけを同期化します。

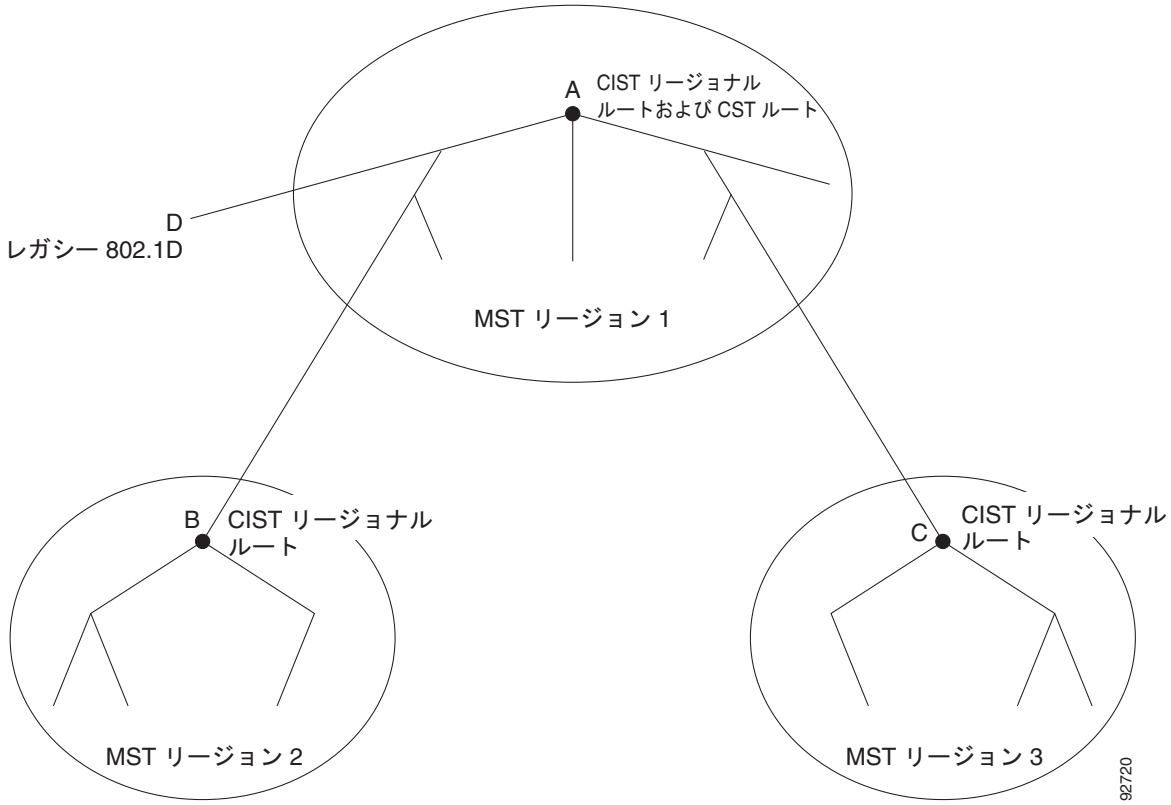
MST リージョン間のスパニングツリーの動作

ネットワーク内に複数のリージョンまたは 802.1D ルータがある場合、MST は 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 リージョンおよびすべての 802.1D STP ルータが含まれます。MSTI は、リージョンの境界にある IST と組み合わさり、CST になります。

IST はリージョン内のすべての MST ルータを接続し、スイッチド ドメイン全体を囲む CIST 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 リージョンは、隣接する STP ルータおよび MST リージョンへの仮想ルータとして認識されます。

図 20-10 は、3 つの MST リージョンおよび 1 つの 802.1D ルータ（D）を含むネットワークを示しています。リージョン 1 の CIST リージョナル ルート（A）は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート（B）、およびリージョン 3 の CIST リージョナル ルート（C）は、CIST 内のそれぞれのサブツリーのルートです。

図 20-10　MST リージョン、CIST リージョナル ルート、CST ルート



CST インスタンスだけが BPDU を送受信し、MSTI はスパニングツリー情報を BPDU に追加してネイバー ルータと相互作用し、最終的なスパニングツリー トポロジーを算出します。このため、BPDU 送信に関連するスパニングツリー パラメータ（hello タイム、転送時間、最大経過時間、最大ホップ数など）は CST インスタンス上でのみ設定されますが、すべての MSTI に影響します。スパニングツリー トポロジー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 インスタンスおよび MSTI の両方で設定できます。

MST ルータは、バージョン 3 の BPDU または 802.1D STP BPDU を使用して、802.1D ルータと通信します。MST ルータは、MST BPDU を使用して MST ルータと通信します。

IEEE 802.1s の用語

準規格の実装で使用される、一部の MST 命名規則は変更され、一部の*内部*パラメータおよび*リージョナル* パラメータの識別が組み込まれました。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。

- CIST ルートは CIST のルート ブリッジであり、ネットワーク全体に広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 ルートまでのコストです。このコストは MST 領域内で変化しません。MST リージョンは、CIST への単一ルータと見なすことに注意してください。CIST 外部ルート パス コストは、これらの仮想ルータ、およびどのリージョンにも属さないルータの間で算出されるルート パス コストです。

- CIST リージョナル ルートは、準規格の実装で 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。CIST ルートがリージョン内にない場合、CIST リージョナル ルートは、リージョン内の CIST ルートに最も近いルータです。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 ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

表 20-5 に、IEEE 規格とシスコ準規格の用語の比較を示します。

表 20-5　準規格と規格の用語

IEEE 規格の定義	シスコ準規格の実装	シスコ規格の実装
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
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

MST は、設定 BPDU のメッセージ エージ情報および最大エージ情報を使用せずにスパニングツリー トポロジーを算出します。その代わりに、IP Time To Live（TTL）メカニズムに似た、ルートまでのパス コストおよびホップ 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と、リージョン内で最大ホップ数を設定し、そのリージョンの 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 エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。ルータは、この BPDU を受信すると、受信した残りのホップ カウントから 1 を引き、生成する BPDU で残りのホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、ルータは BPDU を廃棄し、ポート用に維持されている情報を期限切れにします。

BPDU の RSTP 部分のメッセージ エージ情報および最大エージ情報は、リージョン全体で同じままです。同じ値が、境界にあるリージョンの DP によって伝播されます。

境界ポート

シスコ準規格の実装では、境界ポートが次のうちいずれかの STP リージョンに MST リージョンを接続します。

- RSTP が動作している単一スパニングツリー リージョン
- PVST+ または高速 PVST+ が動作している単一スパニングツリー リージョン
- MST 設定が異なる別の MST リージョン

境界ポートは、LAN、単一スパニングツリー ルータまたは MST 設定が異なるルータの指定ルータにも接続します。

802.1s 規格には、境界ポートの定義がありません。802.1Q-2002 規格では、内部（同一リージョンから着信）および外部という、ポートが受信できる 2 種類のメッセージが識別されています。メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。メッセージ

が内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。シスコ準規格の実装では、外部メッセージを受信するポートが境界ポートとして扱われます。つまりポートは、内部メッセージと外部メッセージを一緒に受信できません。

MST リージョンには、ルータおよび LAN の両方が含まれます。セグメントは、DP のリージョンに属します。このため、セグメントの DP と異なるリージョンのポートは境界ポートです。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ準規格の実装からの主な変更点は、DP が、STP 互換モードで動作していない場合、境界ポートとして定義されないことです。

（注）　802.1D STP ルータがセグメントにある場合、メッセージは常に外部と見なされます。

準規格の実装からの変更点には、RSTP またはレガシー 802.1s ルータに送信者スイッチ ID が含まれる場所に、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こともあります。リージョン全体は、一貫した送信者スイッチ ID をネイバー ルータに送信し、単一仮想ルータのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者スイッチ ID が同じである BPDU をルータ C が受信します。

規格準拠 MST 実装

規格準拠 MST 実装には、規格を満たすために必要となる機能、および公開されている規格にまだ組み込まれていない、必要な準規格機能の一部が含まれます。ここでは、規格準拠 MST 実装について説明します。

- 「ポートの役割の命名規則の変更点」（P.20-24）
- 「レガシーおよび規格準拠ルータの間のスパニングツリー相互運用」（P.20-24）
- 「単一方向リンク障害の検出」（P.20-25）

ポートの役割の命名規則の変更点

境界の役割は最終的な MST 規格から削除されましたが、この境界という概念は規格準拠実装で維持されます。ただしリージョンの境界にある MSTI ポートは、対応する CIST ポートの状態に従わないことがあります。現在、次の 2 つの状況があります。

- 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、提案されて同期化されると、合意を返送して、対応するすべての MSTI ポートが同期化された（フォワーディングになって）あとにだけフォワーディング ステートに移行します。MSTI ポートには、特別な マスターの役割があります。
- 境界ポートが CIST リージョナル ルートのルート ポートでない：MSTI ポートは、CIST ポートのステートおよび役割に従います。規格が提供する情報は少なく、MSTI ポートが BPDU（M レコード）を受信しないとき、交互にブロッキングできる理由を理解することは困難です。この状況の場合、境界の役割はすでに存在しませんが、**show** コマンドを入力すると、出力の *type* カラムでポートが境界として識別されます。

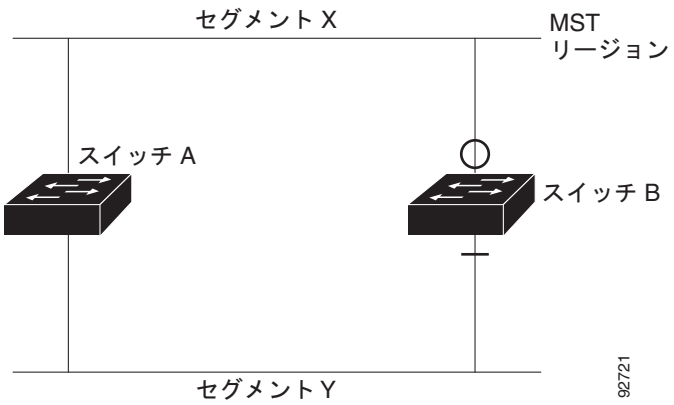
レガシーおよび規格準拠ルータの間のスパニングツリー相互運用

準規格ルータの自動検出はエラーになることがあるので、インターフェイス コンフィギュレーション コマンドを使用して準規格ポートを識別できます。規格ルータおよび準規格ルータの間にリージョンを形成できませんが、CIST の使用前に相互運用できます。この特定状況では、さまざまなインスタンス

におけるロードバランス機能だけが失われます。ポートが準規格 BPDU を受信したとき、CLI ではポート設定によって異なるさまざまなフラグが表示されます。ルータが準規格 BPDU 送信用に設定されていないポートで準規格 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

図 20-11 に、準規格ルータに接続された規格準拠ルータを示します。A は規格準拠ルータ、B は準規格ルータであり、両方とも同一リージョンに設定されているとします。A は CIST のルート ブリッジなので、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 のポートが代替になってから 1 つの準規格 BPDU を送信すると、準規格ルータが Y に接続されていることを AY は検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B の間でのロードバランスは不可能になります。セグメント X にも同じ問題がありますが、B は TC を送信することがあります。

図 20-11　規格準拠ルータと準規格ルータの相互運用



（注） 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

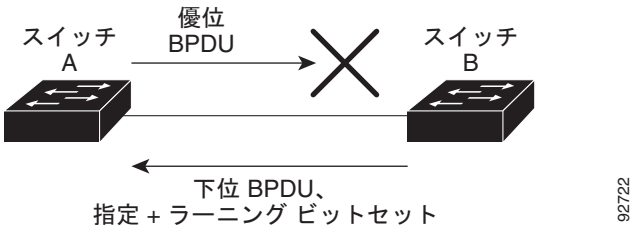
単一方向リンク障害の検出

この機能は IEEE MST 規格にまだ存在しませんが、規格準拠実装には組み込まれています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジング ループの原因となることがある単一方向リンク障害を検出します。

DP は、矛盾を検出すると、そのロールを維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジング ループを解決できるからです。

図 20-12 に、一般的にブリッジング ループになる単一方向リンク障害を示します。ルータ A はルート ブリッジであり、ルータ B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割とステートが含まれます。ルータ A はこの情報を使用し、ルータ A が送信する上位 BPDU にルータ B が反応しないこと、およびルータ B がルート ブリッジではなく指定ブリッジであることを検出できます。その結果、ルータ A はポートをブロックし（またはブロッキングを維持し）、ブリッジング ループを防止します。

図 20-12　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 を実行しているルータでは、組み込みプロトコル移行機能がサポートされます。これにより、802.1D ルータと相互動作できるようになります。このルータが、802.1D 設定の BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信した場合、そのポートでは 802.1D BPDU だけが送信されます。MST ルータは、802.1D BPDU、異なるリージョンに対応付けられた 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、ポートがリージョンの境界にあることを検出できます。

ただし、ルータが 802.1D BPDU を受信していない場合は、自動的に MST モードに戻りません。これは 802.1D ルータが指定ルータでない限り、802.1D ルータがリンクから削除されたかどうかを検出できないためです。このルータが接続するルータがリージョンに加入していると、ルータはポートに境界の役割を割り当て続ける場合があります。プロトコル移行プロセスを再開するには（強制的にネイバー ルータと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンクのすべての 802.1D ルータが RSTP ルータである場合、802.1D ルータは、RSTP BPDU であるかのように MST BPDU を処理できます。このため MST ルータは、バージョン 0 の設定および Topology Change Notification（TCN）BPDU、または境界ポートのバージョン 3 の MST BPDU を送信します。境界ポートは、LAN、単一スパニングツリー ルータまたは MST 設定が異なるルータのいずれかの指定のルータに接続します。

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 のデフォルト設定」（P.20-27）
- 「STP のイネーブル化」（P.20-27）
- 「拡張システム ID のイネーブル化」（P.20-29）
- 「ルート ブリッジの設定」（P.20-29）
- 「セカンダリ ルート ブリッジの設定」（P.20-30）
- 「STP ポート プライオリティの設定」（P.20-31）
- 「STP ポート コストの設定」（P.20-33）
- 「VLAN のブリッジ プライオリティの設定」（P.20-34）
- 「hello タイムの設定」（P.20-35）
- 「VLAN の転送遅延時間の設定」（P.20-36）
- 「VLAN の最大エージング タイムの設定」（P.20-36）

- 「Rapid-PVST のイネーブル化」（P.20-37）

（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になるのは、**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ーであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニング ツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。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 のデフォルト設定

表 20-6 に、STP のデフォルト設定を示します。

表 20-6　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
SPT ポート プライオリティ（ポート単位で設定可能：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
SPT ポート コスト（ポート単位で設定可能：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）	• 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）	• 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
Mode	PVST

STP のイネーブル化

（注）　STP は、VLAN 1 および新たに作成されたすべての 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できます。Cisco 7600 シリーズ ルータは 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 20-6（P.20-27）を参照）。
	`Router(config)# default spanning-tree vlan vlan_ID`	指定された VLAN のすべての STP パラメータを、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 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ない場合は、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。スパニングツリーは、VLAN の一部のスイッチおよびブリッジでディセーブルにしておきながら、VLAN のその他のスイッチおよびブリッジでイネーブルにしておくことはできません。スパニングツリーをイネーブルにしたスイッチとブリッジに、ネットワークの物理トポロジに関する不完全な情報が含まれることになるので、この処理によって予想外の結果となることがあります。

注意　物理的なループの存在しないトポロジーであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニング ツリーは、設定の誤りおよび配線の誤りに対する保護手段として動作します。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
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 200000    128.196  P2p
Gi1/5            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

拡張システム ID は、Cisco 7600 シリーズ ルータで永続的にイネーブルになっています。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

Cisco 7600 シリーズ ルータは、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 が対応付けられます。VLAN ごとに、最小のブリッジ ID を持つネットワーク デバイスが、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、ルータは各 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 をイネーブルにすると、24576 という値でルータが指定された VLAN のルートになる場合、ルータはその VLAN のブリッジ プライオリティを 24576 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、ルータはその 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 20-1（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** コマンドはエラーになります。

拡張システム ID がイネーブルで、たとえば VLAN 20 のすべてのネットワーク デバイスでデフォルト プライオリティが 32768 に設定されている場合に、ルータ上で **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、ルータが 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、バックボーンまたはディストリビューション ルータでなければなりません。アクセス ルータを 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（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間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、Cisco 7600 シリーズ ルータ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 トポロジーを安定した状態に保つには、Cisco 7600 シリーズ ルータをルート 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。

Cisco 7600 シリーズ ルータをルート 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]]`	Cisco 7600 シリーズ ルータをルート 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 20-6（P.20-27）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、Cisco 7600 シリーズ ルータを 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

Cisco 7600 シリーズ ルータをセカンダリ 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 デバイス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）、このルータが指定された 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 をイネーブルにしている場合、STP はブリッジ プライオリティを 28672 に設定します。

このコマンドを複数のルータ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。

Cisco 7600 シリーズ ルータをセカンダリ 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]]`	Cisco 7600 シリーズ ルータをセカンダリ 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、Cisco 7600 シリーズ ルータを 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 ポートのプライオリティ値が同じ場合、STP は最小の LAN ポート番号を持つ LAN ポートをフォワーディング ステートに移行させ、その他の 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 です）、16 ずつ増加するよう設定できます。

Cisco IOS は LAN ポートがアクセス ポートとして設定されている場合にはポート プライオリティ値を使用し、LAN ポートがトランク ポートとして設定されている場合には VLAN ポート プライオリティ値を使用します。

レイヤ 2 LAN インターフェイスの STP ポート 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 {{gigabitethernet 1/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 1 ～ 252 で、4 ずつ増加します。
	`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。
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 1 ～ 252 で、4 ずつ増加します。*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] 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。

	コマンド	目的
ステップ 5	Router# **show spanning-tree interface** {**gigabitethernet 1***/port*}	{**port-channel** *port_channel_number*} Router# **show spanning-tree vlan** *vlan_ID*	設定を確認します。

次に、ギガビット イーサネット ポート 1/4 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 gigabitethernet 1/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 1/4 の設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 1/4
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#
```

ギガビット イーサネット ポート 1/4 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、ギガビット イーサネット ポート 1/4 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 gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# end
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 gigabitethernet 1/4
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、次のコマンドも使用できます。

```
Router# show spanning-tree vlan 200 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            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 に最初に選択させる LAN インターフェイスには低いコスト値を、STP に最後に選択させる 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 {{gigabitethernet 1/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 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)# 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）。
	`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 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 {gigabitethernet 1/port} | {port-channel port_channel_number}` `show spanning-tree vlan vlan_ID`	設定を確認します。

次に、ギガビット イーサネット ポート 1/4 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 gigabitethernet 1/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree interface gigabitethernet 1/4
```

```
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 コストでポート 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 gigabitethernet 1/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show spanning-tree vlan 200 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 2000       64.196  P2p
```

（注） 次に示す出力では、他の VLAN（VLAN 1 など）はこの設定の影響を受けていません。

```
Router# show spanning-tree vlan 1 interface gigabitethernet 1/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            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。

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** {**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。

	コマンド	目的
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 32768
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          32768 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。

ルータの Rapid PVST モードをイネーブルにするには、特権モードで **spanning-tree mode rapid-pvst** コマンドを入力します。Rapid-PVST モードでのルータの設定手順については、「STP の設定」（P.20-26）を参照してください。

リンク タイプの設定

高速接続は、ポイントツーポイント リンク上だけに確立されます。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 つのスイッチだけを接続するセグメントとして見なします。ルータでは、すべての全二重リンクをポイントツーポイントとして、また半二重リンクを共有リンクとして見なすので、リンク タイプの明示的設定を回避できます。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 および RSTP の両方が稼働するルータでは、組み込みのプロトコル移行プロセスをサポートして、ルータがレガシー 802.1D スイッチと相互運用するのを可能にします。このルータが、レガシー 802.1D 設定の BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信した場合、そのポートでは 802.1D BPDU だけが送信されます。また、MSTP ルータは、レガシー BPDU、異なるリージョンに対応付けられた 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、ポートがリージョン境界にあることを検出できます。

ただし、ルータが 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシー ルータが指定ルータでない限り、レガシー ルータがリンクから削除されたかどうか判別できないためです。また、接続するルータがリージョンに加入していると、ルータはポートに境界の役割を割り当て続ける場合があります。

ルータ全体で、プロトコル移行プロセスを再開するには（強制的にネイバー スイッチと再びネゴシエートするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。特定のインターフェイスでプロトコル移行プロセスを再開するには、**clear spanning-tree detected-protocols interface** *interface-id* 特権 EXEC コマンドを入力します。

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 MST 設定」（P.20-38）
- 「MST 設定時の注意事項および制約事項」（P.20-38）
- 「MST リージョン設定の指定および MST のイネーブル化」（P.20-39）（必須）
- 「ルート ブリッジの設定」（P.20-41）（任意）
- 「セカンダリ ルート ブリッジの設定」（P.20-30）（任意）
- 「STP ポート プライオリティの設定」（P.20-31）（任意）
- 「パス コストの設定」（P.20-44）（任意）
- 「スイッチのプライオリティの設定」（P.20-45）（任意）
- 「hello タイムの設定」（P.20-46）（任意）
- 「送信保留カウントの設定」（P.20-47）（任意）
- 「最大経過時間の設定」（P.20-48）（任意）
- 「最大ホップ カウントの設定」（P.20-48）（任意）
- 「高速移行を保証するリンク タイプの指定」（P.20-49）（任意）
- 「ネイバー タイプの指定」（P.20-49）（任意）
- 「プロトコル移行プロセスの再開」（P.20-50）（任意）

デフォルト MST 設定

表 20-7 に、デフォルト MST 設定を示します。

表 20-7　デフォルト MST 設定

機能	デフォルト設定
スパニングツリー モード	PVST+（高速 PVST+ および MST はディセーブルです）
スイッチ プライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポートごとに設定可能）	128
スパニングツリー ポート コスト（CIST ポートごとに設定可能）	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 の設定時には、次の注意事項および制約事項に従ってください。

- 802.1s MST 規格では 65 までの MSTI が許可されます。無制限の数の VLAN を MSTI にマップできます。

- PVST+、高速 PVST+、MST はサポートされますが、同時にアクティブにできるバージョンは 1 つだけです。
- VTP は MST 設定を伝播しません。コマンドライン インターフェイス（CLI）または SNMP を使用し、MST リージョン内の各ルータで MST 設定（リージョン名、リビジョン番号、VLAN とインスタンスのマッピング）を手動で設定する必要があります。
- ネットワークの冗長パスでロードバランスを実現するには、すべての VLAN とインスタンスのマッピング割り当てが一致する必要があります。一致しない場合、すべてのトラフィックは単一リンクを流れます。
- すべての MST 境界ポートは、PVST+ と MST クラウドの間、または高速 PVST+ および MST クラウドの間におけるロードバランスのために転送する必要があります。このためには、MST クラウドの CIST リージョナル ルートが CST のルートである必要があります。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があり、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。
- ネットワークを多数のリージョンに分割することは推奨できません。ただしこの状況を避けられない場合は、レイヤ 2 デバイスによって相互接続された、より小さい LAN にスイッチド LAN を分割することを推奨します。

MST リージョン設定の指定および MST のイネーブル化

複数のルータを同一 MST リージョンに含めるには、それらのルータの VLAN とインスタンスのマッピング、設定リビジョン番号、および MST 名が同じである必要があります。

リージョンには、MST 設定が同一である、1 つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワークにおける MST リージョンの数に制限はありませんが、各リージョンでは 65 までのスパニングツリー インスタンスしかサポートできません。スパニングツリー インスタンスに同時に割り当てられる VLAN は 1 つだけです。

MST リージョン設定を指定して 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。
ステップ 3	`Router(config-mst)# instance` *instance_id* `vlan` *vlan_range*	VLAN を MSTI にマップします。 • *instance_id* の範囲は 0 ～ 4094 です。 • **vlan** *vlan_range* の範囲は 1 ～ 4094 です。 VLAN を MST インスタンスにマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば **instance 1 vlan 1-63** では、VLAN 1 ～ 63 が MSTI 1 にマップされます。 一連の VLAN を指定するには、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MSTI 1 にマップされます。

	コマンド	目的
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* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。
ステップ 5	`Router(config-mst)# revision version`	設定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`	保留中の設定を表示し、設定を確認します。
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 および 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、トラフィックが混乱することがあります。すべてのスパニングツリー インスタンスが以前のモードで停止し、新しいモードで再起動されるからです。 MST と PVST+ の両方、または MST と高速 PVST+ の両方を同時に実行することはできません。
ステップ 9	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Router# show running-config`	入力を確認します。
ステップ 11	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻すには、次のように操作します。

- デフォルトの MST リージョン設定に戻すには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。
- VLAN とインスタンスのデフォルト マップに戻すには、**no instance** *instance_id* [**vlan** *vlan_range*] MST コンフィギュレーション コマンド を使用します。
- デフォルト名に戻すには、**no name** MST コンフィギュレーション コマンド を使用します。
- デフォルトのリビジョン番号に戻すには、**no revision** MST コンフィギュレーション コマンド を使用します。
- PVST+ を再び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 コマンドを使用します。

次の例は、MST コンフィギュレーション モードを開始し、VLAN 10 ～ 20 を MSTI 1 にマッピングし、リージョンに *region1* という名前を付けて、設定リビジョンを 1 に設定し、保留中の設定を表示し、変更を適用してグローバル コンフィギュレーション モードに戻る方法を示しています。

```
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

ルータは、そのルータにマッピングされている VLAN の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ルータの MAC アドレスで構成されるスイッチ ID が対応付けられます。VLAN のグループの場合、スイッチ ID が最低であるルータがルート ブリッジになります。

ルータがルート ブリッジになるように設定するには、**spanning-tree mst** *instance_id* **root** グローバル コンフィギュレーション コマンドを使用して、デフォルト値（32768）から大幅に小さい値にスイッチ プライオリティを修正し、ルータが、指定したスパニングツリー インスタンスのルート ブリッジになるようにします。このコマンドを入力すると、ルータはルート ブリッジのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、24576 という値によってルータが指定スパニングツリー インスタンスのルート ブリッジになる場合、ルータは指定インスタンスに対して自身のプライオリティをこの値に設定します。

指定インスタンスのルート ブリッジのスイッチ プライオリティが 24576 より小さい場合、ルータは、最低スイッチ プライオリティより 4096 小さい値に自身のプライオリティを設定します （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 20-1（P.20-3）を参照）。

ネットワークが拡張システム ID をサポートするルータとサポートしないルータの両方で構成されている場合、拡張システム ID をサポートするルータがルート ブリッジになる可能性は低くなります。古いソフトウェアを実行している接続ルータのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってスイッチ プライオリティ値が増加します。

各スパニングツリー インスタンスのルート ブリッジは、バックボーンまたはディストリビューション ルータでなければなりません。アクセス ルータをスパニングツリー 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 ネットワークの任意の 2 つのエンド ステーション間にあるレイヤ 2 ホップの最大数）を指定するには、MSTI 0 だけに使用できる **diameter** キーワードを使用します。ネットワーク直径を指定すると、ルータ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 タイムを自動的に設定します。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したルータでは、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、**spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング時間を手動で設定しないでください。

ルータをルート 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）ルータをルート ブリッジとして設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。範囲は 0 ～ 4094 です。 • （任意）**diameter** *net_diameter* には、任意の 2 つのエンド ステーション間におけるレイヤ 2 ホップの最大数を指定します。範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。 • （任意）**hello-time** *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。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`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst` *instance_id*	入力を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータをデフォルト設定に戻すには、**no spanning-tree mst** *instance_id* **root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート ブリッジの設定

拡張システム ID をサポートするルータをセカンダリ ルートとして設定する場合、スイッチ プライオリティはデフォルト値（32768）から 28672 に修正されます。プライマリ ルート ブリッジで障害が発生した場合は、このルータが指定インスタンスのルート ブリッジになる可能性があります。ここでは、その他のネットワーク ルータが、デフォルト スイッチ プライオリティの 32768 を使用しているためにルート ブリッジになる可能性が低いことが前提となっています。

このコマンドを複数のルータ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。**spanning-tree mst** *instance_id* **root primary** グローバル コンフィギュレーション コマンドで、プライマリ ルート ブリッジの設定時に使用したものと同じネットワーク直径値と hello タイム値を使用してください。

ルータをセカンダリ 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）ルータをセカンダリ ルート ブリッジとして設定します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。範囲は 0 ～ 4094 です。 • （任意）**diameter** *net_diameter* には、任意の 2 つのエンド ステーション間におけるルータの最大数を指定します。範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。 • （任意）**hello-time** *seconds* には、ルート ブリッジが設定メッセージを生成する時間を秒単位で指定します。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.20-41）を参照してください。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst instance_id`	入力を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータをデフォルト設定に戻すには、**no spanning-tree mst** *instance_id* **root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、ポート プライオリティを使用します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）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のプライオリティ値が同一である場合、MST はインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

インターフェイスの MST 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# configure terminal`	グローバル コ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 1/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* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。範囲は 0 ～ 4094 です。 • *priority* 値の範囲は 0 ～ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他すべての値は拒否されます。
ステップ 4	`Router(config-if)# end`	特権 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`
		入力を確認します。

ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　**show spanning-tree mst interface** *interface_id* 特権 EXEC コマンドでは、ポートがリンクアップ動作状態になっている場合に限って情報が表示されます。ポートがリンクアップ動作状態になっていない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認できます。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance_id* **port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

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派生します。ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、コストを使用します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択される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のコスト値が同一である場合、MST はインターフェイス番号が最も低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、その他のインターフェイスをブロックします。

インターフェイスの MST 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# configure terminal`	グローバル コ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 1/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。 ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、パス コストを使用します。低いパス コストは高速送信を表します。 • *instance_id* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。範囲は 0 ～ 4094 です。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 4	`Router(config-if)# end`	特権 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`
		入力を確認します。

ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

（注）　**show spanning-tree mst interface** *interface_id* 特権 EXEC コマンドでは、リンクアップ動作状態になっているポートだけの情報が表示されます。ポートがリンクアップ動作状態になっていない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認できます。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst** *instance_id* **cost** インターフェイス コンフィギュレーション コマンドを使用します。

スイッチのプライオリティの設定

スイッチ プライオリティを設定し、ルータがルート ブリッジとして選択される可能性を高くすることができます。

（注）　このコマンドの使用には注意してください。スイッチ プライオリティを変更するには、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** グローバル コンフィギュレーション コマンドを使用することを推奨します。

スイッチ プライオリティを設定するには、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* には、単一インスタンスを指定したり、インスタンスの範囲をハイフンで区切って指定したり、一連のインスタンスをカンマで区切って指定したりすることができます。範囲は 0 ～ 4094 です。 • *priority* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値を小さくすると、ルータがルート 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、および 61440 です。その他すべての値は拒否されます。
ステップ 3	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show spanning-tree mst instance_id`	入力を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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 タイムを変更し、ルート ブリッジが設定メッセージを生成する時間を設定できます。

（注）　このコマンドの使用には注意してください。hello タイムを修正するには、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** グローバル コンフィギュレーション コマンドを使用することを推奨します。

すべての MSTI に 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 MSTI に hello タイムを設定します。hello タイムは、ルート ブリッジが設定メッセージを生成する間隔です。このメッセージは、ルータが活動中であることを表します。 *seconds* に指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。

	コマンド	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	Router# **show spanning-tree mst**	入力を確認します。
ステップ 5	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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 MSTI に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 MSTI に転送時間を設定します。転送遅延は、ポートがスパニングツリー 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 ステートに変更するまでに待機する秒数です。 *seconds* に指定できる範囲は 4 ～ 30 です。デフォルトは 15 です。
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	Router# **show spanning-tree mst**	入力を確認します。
ステップ 5	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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。

送信保留カウントの設定

すべての MSTI に送信保留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 MSTI に送信保留カウントを設定します。 *hold_count_value* の範囲は 1 ～ 20 で、デフォルトは 6 です。
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	Router# **show spanning-tree mst**	入力を確認します。
ステップ 5	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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。

最大経過時間の設定

すべての MSTI に最大エージング 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 MSTI に最大エージング タイムを設定します。最大エージング タイムは、ルータが再設定を試す前にスパニングツリー設定メッセージを受信せずに待機する秒数です。 *seconds* に指定できる範囲は 6 ～ 40 です。デフォルトは 20 です。
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	Router# **show spanning-tree mst**	入力を確認します。
ステップ 5	Router# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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 MSTI に最大ホップ 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 が廃棄されて、ポート用に維持された情報が期限切れになるまでの、リージョン内のホップ数を指定します。 *hop_count* の範囲は 1 ～ 255、デフォルトは 20 です。
ステップ 3	Router(config)# **end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	`Router# show spanning-tree mst`	入力を確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ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。

高速移行を保証するリンク タイプの指定

ポイントツーポイント リンクでポート間を接続し、ローカル ポートが DP になると、RSTP は提案と合意のハンドシェークを使用して別のポートと高速移行をネゴシエーションし、「高速コンバージェンス」（P.20-14）で説明したようなループがないトポロジーを保証します。

デフォルトの場合、リンク タイプはインターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続、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 ルータの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンク タイプのデフォルト設定を無効にして、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することができます。

デフォルトのリンク タイプ設定を無効にするには、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)# interface {{gigabitethernet 1/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であることを指定します。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface interface_id`	入力を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

ネイバー タイプの指定

トポロジーには、準規格準拠デバイスおよび 802.1s 規格準拠デバイスの両方を含めることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。ポートが STP 互換モードになっていても、すべての **show** コマンドで準規格フラグが表示されます。

デフォルトのリンク タイプ設定を無効にするには、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)# interface {{gigabitethernet 1/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`	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 4	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show spanning-tree mst interface interface_id`	入力を確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、**no spanning-tree mst prestandard** インターフェイス コンフィギュレーション コマンドを使用します。

プロトコル移行プロセスの再開

MST を実行しているルータでは、組み込みプロトコル移行機能がサポートされます。これにより、802.1D ルータと相互動作できるようになります。このルータが、802.1D 設定の BPDU（プロトコル バージョンが 0 に設定された BPDU）を受信した場合、そのポートでは 802.1D BPDU だけが送信されます。MST ルータは、802.1D BPDU、異なるリージョンに対応付けられた 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、ポートがリージョン境界にあることを検出できます。

ただし、ルータが 802.1D BPDU を受信していない場合は、自動的に MST モードに戻りません。これは 802.1D ルータが指定ルータでない限り、802.1D ルータがリンクから削除されたかどうかを検出できないためです。また、接続するルータがリージョンに加入していると、ルータはポートに境界の役割を割り当て続ける場合があります。

ルータでプロトコル移行プロセスを再開するには（強制的にネイバー ルータと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再開するには、**clear spanning-tree detected-protocols interface** *interface_id* 特権 EXEC コマンドを使用します。

MST の設定およびステータスの表示

スパニングツリーのステータスを表示するには、表 20-8 で説明する 1 つ以上の特権 EXEC コマンドを使用します。

表 20-8　MST ステータスを表示するコマンド

コマンド	目的
`show spanning-tree mst configuration`	MST リージョンの設定を表示します。
`show spanning-tree mst configuration digest`	現在の MSTCI に含まれる MD5 ダイジェストを表示します。

表 20-8　MST ステータスを表示するコマンド （続き）

コマンド	目的
show spanning-tree mst *instance_id*	指定インスタンスの MST 情報を表示します。
show spanning-tree mst interface *interface_id*	指定インターフェイスの MST 情報を表示します。

CHAPTER 21

オプションの STP 機能の設定

この章では、オプションの STP 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 7600 Series Routers Command References』を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「PortFast の機能概要」（P.21-2）
- 「BPDU ガードの機能概要」（P.21-2）
- 「PortFast BPDU フィルタリングの機能概要」（P.21-2）
- 「UplinkFast の機能概要」（P.21-3）
- 「BackboneFast の機能概要」（P.21-4）
- 「EtherChannel ガードの機能概要」（P.21-6）
- 「ルート ガードの機能概要」（P.21-7）
- 「ループ ガードの機能概要」（P.21-7）
- 「PortFast のイネーブル化」（P.21-8）
- 「PortFast BPDU フィルタリングのイネーブル化」（P.21-10）
- 「BPDU ガードのイネーブル化」（P.21-12）
- 「UplinkFast のイネーブル化」（P.21-12）
- 「BackboneFast のイネーブル化」（P.21-13）
- 「EtherChannel ガードのイネーブル化」（P.21-14）
- 「ルート ガードのイネーブル化」（P.21-15）
- 「ループ ガードのイネーブル化」（P.21-15）

（注） スパニングツリー プロトコル（STP）の設定手順については、第 20 章「STP および 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、デバイス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ブリッジ プロトコル データ ユニット（BPDU）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 は動作しています。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。ルータ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 ループが発生する可能性があります。

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、認証されていないデバイス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）　グローバルに設定されている 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 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、ポートはすぐに動作中の PortFast ステータスが解除されます。その場合、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 はこのポート上で BPDU の送信を再開します。

また、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 フィルタリングをポート上で明示的に設定すると、そのポートは BPDU を送出しなくなり、受信した BPDU をすべてドロップします。

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、このポートは受信したすべての BPDU を無視し、フォワーディングに移行するため、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.21-10）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 ステート	PortFast BPDU フィルタリング 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	N/A	ディセーブル
ディセーブル	N/A	N/A	ディセーブル
イネーブル	N/A	N/A	イネーブル

1. ポートは最低 10 個の BPDU を送信します。このポートが BPDU を受信すると、PortFast および PortFast BPDU のフィルタリングはディセーブルになります。

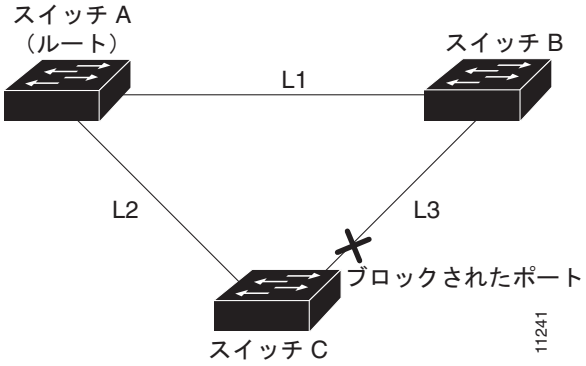
UplinkFast の機能概要

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スを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 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。

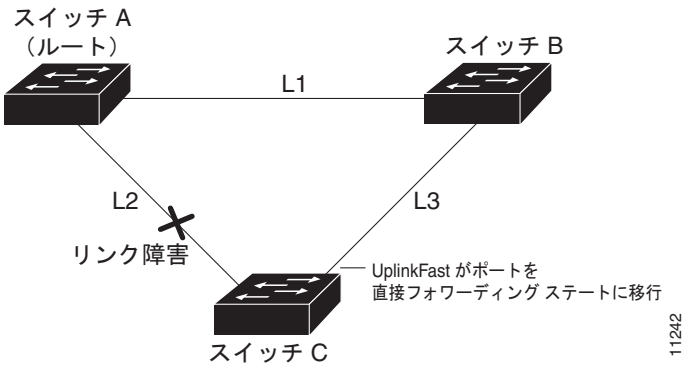
図 21-1 は、リンク障害が発生していないときのトポロジー例です。スイッチ A（ルート ブリッジ）は、リンク L1 を通じてスイッチ B に、リンク L2 を通じてスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 LAN インターフェイスは、ブロッキング ステートです。

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

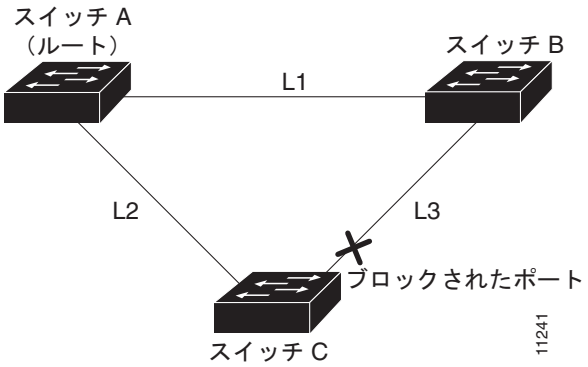
ネットワーク デバイス上のルート ポートまたはブロックされたポートが、そのポートの指定ブリッジから下位 BPDU を受信すると、BackboneFast が開始されます。下位 BPDU により、1 台のネットワーク デバイスをルート ブリッジおよび指定ブリッジの両方として識別します。ネットワーク デバイスが下位 BPDU を受信すると、ネットワーク デバイスはそのネットワーク デバイスが直接接続されていないリンク（*間接*リンク）で障害が発生した（つまり、指定ブリッジからルート ブリッジへの接続が切断された）ものと見なします。標準的な STP ルールに従う場合、ネットワーク デバイスは設定され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 デバイスは、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 デバイスのルート 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 デバイスはルート 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 デバイスにルート ブリッジへの代替パスがある場合、ネットワーク デバイスはそれらの代替パスを使用して、ルート リンク クエリー プロトコル データ ユニット（PDU）と呼ばれる新しい種類の PDU を送信します。ネットワーク デバイスはルート 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 デバイスは、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 デバイスとルート 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 デバイスは、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 デバイスは、下位 BPDU を受信したすべてのポートを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートから、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ー例です。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。この切り替えに要する時間は約 30 秒で、転送遅延時間の 2 倍にあたります（転送遅延時間がデフォルトの 15 秒に設定されている場合）。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ー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

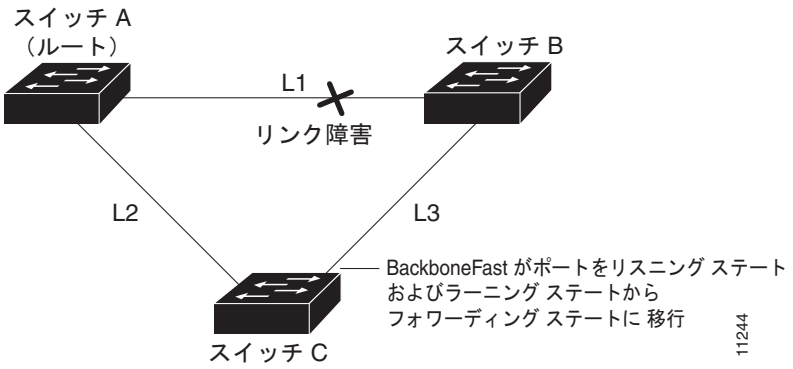
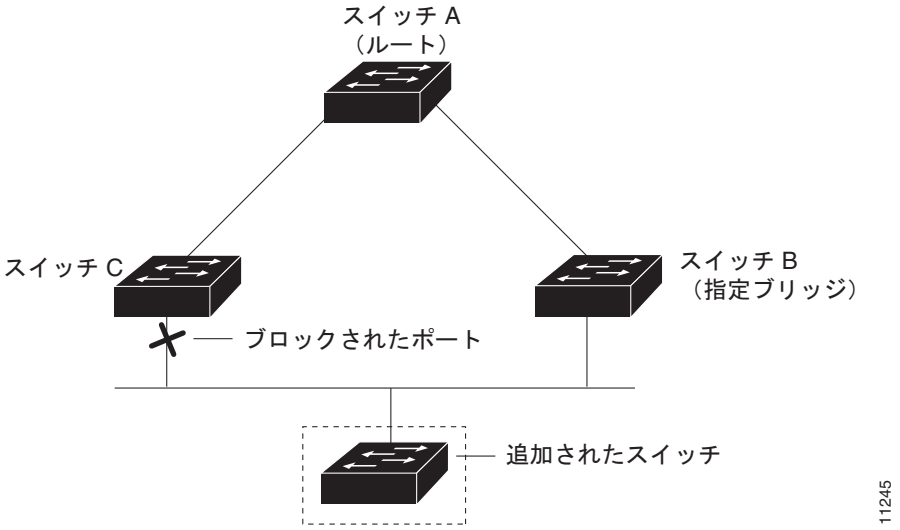


図 21-5 に示すメディア共有型トポロジーに新しいネットワーク デバイスが組み込まれた場合、BackboneFast は起動されません。これは、認識している指定ブリッジ（スイッチ B）から下位 BPDU が着信していないためです。新しいネットワーク デバイスは、自らがルート ブリッジであることを伝える下位 BPDU の送信を開始します。しかし、他のネットワーク デバイスはこれらの下位 BPDU を無視します。その結果、新しいネットワーク デバイスはスイッチ B がルート ブリッジであるスイッチ A への指定ブリッジであることを学習します。

図 21-5　メディア共有型トポロジーにおけるネットワーク デバイスの追加



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（Cisco 7600 シリーズ ルータのインターフェイスが EtherChannel として設定されているが、他のデバイス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）。

他のデバイスの設定に誤りがあることが検出されると、EtherChannel ガードは Cisco 7600 シリーズ ルータ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 ガードは、ポイントツーポイント リンク上の単一方向リンク障害が原因で発生することのあるブリッジング ループの防止に有効です。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設定し、最初のリンクが単一方向になった場合、ループ ガードは影響を受けたポートがチャネルから除外されるまで、チャネル全体をブロックします。
図 21-6 に、三角型のルータ構成におけるループ 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

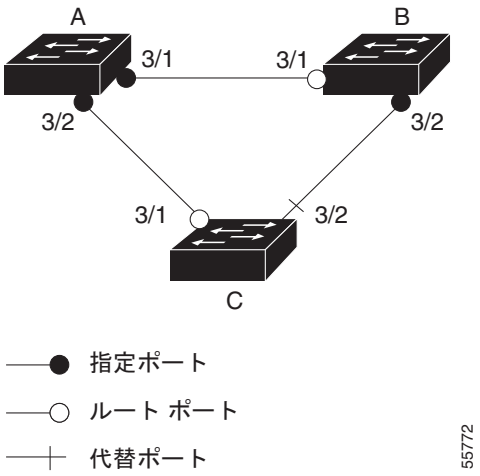


図 21-6 に、次の設定を示します。

- 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 ルータです。
- 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 ルータでループ ガードをイネーブルにしても、効果はありませんが、ルート ルータが非ルート ルータになった場合に保護されます。

ループ ガードの使用時には、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だけ、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、ポート集約プロトコル（PAgP）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ロールを使用して、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 フィルタリングを設定する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`	ルータ上で BPDU フィルタリングをグローバルにイネーブル化します。
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+ については、第 20 章「STP および 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、Cisco 7600 シリーズ ルータ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、ルータがルート ブリッジになる可能性が低くなります。*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

オリティに設定されている 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 プライオリティが設定されている 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、Cisco 7600 シリーズ ルータ上のすべての VLAN に影響します。個々の VLAN 上で UplinkFast を設定することはできません。

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 [max-update-rate max_update_rate]`	UplinkFast をイネーブルにします。
	`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 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 デバイス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 デバイス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。

	コマンド	目的
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、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 ステートになっている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。

誤っている設定が消去されると、errdisable ステートのインターフェイスは自動的に回復します。ポートを手動でサービス状態に戻すには、**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** Router(config-if)# **no spanning-tree guard root**	ルート ガードをイネーブルにします。 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

ルータ上でグローバルにループ 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)# **spanning-tree loopguard default**	ルータ上でグローバルにループ ガードをイネーブル化します。
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
```

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、Cisco 7600 シリーズ ルータでレイヤ 3 インターフェイス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、次の資料を参照してください。

- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_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」（P.22-1）
- 「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」（P.22-2）
- 「IPv4 ルーティングおよびアドレスの設定」（P.22-3）
- 「IPX ルーティングおよびネットワーク番号の設定」（P.22-7）
- 「AppleTalk ルーティング、ケーブルの範囲、およびゾーンの設定」（P.22-8）
- 「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」（P.22-9）

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 インターフェイスの設定時には、次の注意事項および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。
- レイヤ 3 VLAN インターフェイスでは **ip unnumbered** コマンドがサポートされます。
- [**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 メンバーシップを割り当てます。詳細については、第 14 章「VLAN の設定」および第 13 章「VTP の設定」を参照してください。
- Cisco 7600 シリーズ ルータでは次の機能をサポートしません。
  - Integrated Routing and Bridging（IRB）
  - Concurrent Routing and Bridging（CRB）
  - Remote Source-Route Bridging（RSRB）

- ルーティングされないプロトコルのブリッジングを行うには、VLAN インターフェイス上でブリッジ グループを使用します。これはフォールバック ブリッジングと呼ばれることもあります。VLAN インターフェイス上のブリッジ グループは MSFC のソフトウェアでサポートされます。
- Cisco 7600 シリーズ ルータでは、ブリッジ グループに IEEE ブリッジング プロトコルがサポートされません。VLAN ブリッジまたは Digital Equipment Corporation（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。
- 物理インターフェイス上でサブインターフェイスが dot1q ネイティブのカプセル化で設定されている場合は、同じ物理インターフェイス上で IP アドレスを設定しないでください。

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の設定時には、次の注意事項および制約事項に従ってください。

- LAN ポート サブインターフェイスでは、次の機能がサポートされます。
  - MPLS VPN を含む、IPv4 ユニキャスト転送
  - MPLS VPN を含む、IPv4 マルチキャスト転送
  - 6PE
  - EoMPLS
  - IPv4 の番号付けなし
  - MIBS および **show vlans** コマンドによる、サブインターフェイスのカウンタ
  - iBGP および eBGP
  - OSPF
  - EIGRP
  - RIPv1/v2
  - RIPv2
  - ISIS
  - スタティック ルーティング
  - 単方向リンク ルーティング（UDLR）
  - 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

- 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 はルータ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併用する VLAN を設定できません。

（注） 1 つのインターフェイス、別のインターフェイスまたはサブインターフェイス上のサブインターフェイスに、使用する VLAN を設定できません。

- VTP トランスペアレント 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 デバイス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 だけ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 モードをトランスペアレント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`	特権 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、次の資料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/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/index.htm

IPv4 ルーティングおよびアドレスの設定時には、次の注意事項および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 7600 Series Router Cisco IOS Command Reference*』を参照してください。
- ポリシー フィーチャ カード（PFC）および Distributed Feature Card（DFC）は、**match ip address**、**set ip next-hop**、**ip default next-hop** PBR キーワードを使用するルート マップ シーケンス用のポリシーベース ルーティング（PBR）をハードウェアでサポートします。

  PBR を設定するときは、次の注意事項および制約事項に従ってください。

  - PFC では、トンネル インターフェイスで設定されている PBR がハードウェアでサポートされます。
  - 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、PFC では、**set ip next-hop** キーワードで設定された PBR がハードウェアでサポートされません。
  - MSFC アドレスが PBR ACL の範囲内にある場合、MSFC にアドレス指定されたトラフィックは MSFC に転送されないで、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のポリシー ルーティングを禁止するには、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。
  - フローをソフトウェアでスイッチングする MSFC に送信する PBR ルートマップに、フィルタリングを実行する Cisco IOS ACL のオプションはいずれも無視されます。たとえば、ロギングは、PBR ルートマップに、フィルタリングを実行する Cisco IOS ACL の ACE ではサポートされません。
  - PBR が設定されているスイッチング モジュール ポートを介した PBR トラフィックは、スイッチング モジュールがリセットした場合にソフトウェアでルーティングされます。（CSCee92191）。
  - Cisco IOS Release 15.2(1)S1 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。
  - PBR は MPLS ラベル インターフェイスとしてのネクスト ホップでサポートされません。MPLS がラベルをインポーズしない場合、PBR はハードウェアで正常に機能します。これはハードウェアおよびソフトウェアの両方でサポートされません。PBR は、ラベル インポジションをしません。そのため、リモート PE への VPN トラフィックの転送に PBR を使用できません。これは、IP PBR と IPv6 PBR の両方に適用されます。

  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」の「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

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だけ、必須です）。
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。

	コマンド	目的
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の 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の 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）　MSFC では、Internetwork Packet Exchange（IPX）が高速スイッチングを使用してサポートされます。

詳しい説明および設定手順については、次の資料を参照してください。

- 次の URL の『*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 の『*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

レイヤ 3 インターフェイスに IPX のルーティングおよび 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**、**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、次の資料を参照してください。

- 次の URL の『*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 の『*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 に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**、**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、次の資料を参照してください。

- 次の URL の『*Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Configuration Guide*, Release 12.2』

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

- 次の URL の『*Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Command Reference*, Release 12.2』

  http://www.cisco.com/en/US/docs/ios/12_2/apollo/command/reference/fapolo_r.html

CHAPTER 23

GTP-SLB IPV6 サポートの設定

この章では、Cisco 7600 シリーズ ルータでの GPRS Tunneling Protocol - Server Load Balancing（GTP-SLB; GPRS トンネリング プロトコル - サーバ ロード バランシング）IPV6 サポートの設定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。

- 「GTP-SLB の IPv6 サポート」（P.23-1）
- 「GTP-SLB アーキテクチャの概要」（P.23-2）
- 「制約事項および使用上の注意事項」（P.23-4）
- 「GTP-SLB IPv6 サポートの設定」（P.23-4）

GTP-SLB の IPv6 サポート

GTP-SLB 機能は、Public Data Network（PDN; 公衆データ網）Gateway（P-GW; PDN ゲートウェイ）と **Gateway** GPRS Support Nodes（GGSN; ゲートウェイ GPRS サポート ノード）間で Packet Datagram Protocol（PDP）コンテキストを配信する機能を提供します。PDP には、加入者セッション情報が含まれており、次のものによって開始されます。

- GTPv2 での Create Session Request（CSR; セッション作成要求）。
- GTPv1 および GTPv0 での PDP 作成要求。

サーバ ロード バランシング モジュールは、7600 シャーシのスーパーバイザ エンジンに存在し、CPU、メモリ、およびセッション カウントなどのさまざまな要因を考慮した個々のロードに基づいて、新規のコールを各種のカードに配信します。Release 15.0(01)S 以降、GTP-SLB 機能は、IPv4 トラフィックに加えて IPv6 トラフィックをサポートするように拡張されました。

SLB では、実オブジェクト（サーバまたはゲートウェイ）に保存された IPv6 アドレスを使用し、IPv6 Forwarding Information Base（FIB; 転送情報ベース）ルックアップを実行して、Serving GPRS Support Node / Mobility Management Entity（SGSN/MME）から対応する GTP-SLB 仮想 IP アドレスに IPv6 パケットを転送します。IPv4 および IPv6 トラフィックに対応する実サーバのグループ（サーバファームとして知られる）が定義され、デュアルスタック仮想サーバ（IPv4 と IPv6 の両方のアドレスに関するテーブル マッピングを保持する）に関連付けられます。IPv4 対応の実サーバは、IPv4 Virtual IP（VIP; 仮想 IP）アドレスを宛先とする CSR 用に選択され、IPv6 対応の実サーバは、IPv6 VIP アドレスを宛先とする CSR 用に選択されます。

（注） GGSN/PGW による DFP 加重報告メカニズムには、IPv4 トランスポートが使用されます。

（注）　プローブ メッセージには、トランスポートとして IPv4 が使用されます。

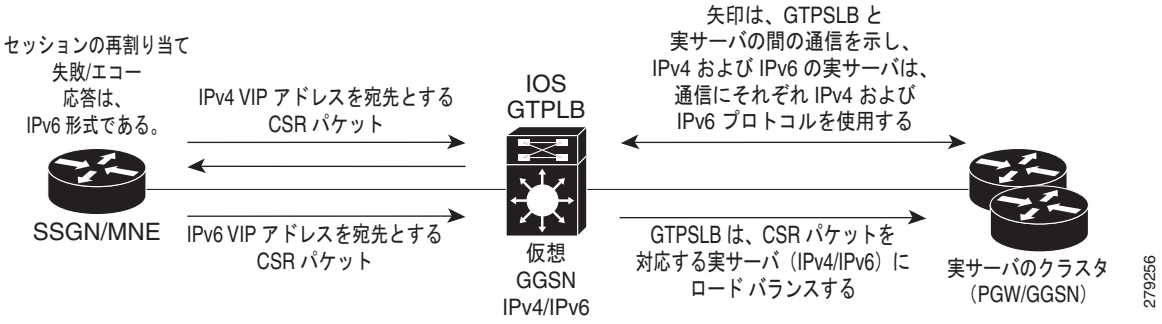
（注）　GTPv2 実サーバは、Serving Gateway（SGW; サービング ゲートウェイ）または PDN Gateway（PGW; PDN ゲートウェイ）として機能できます。GTPv2、V1、V0 要求をサポートするのは、PGW のみです。SGW は、GTPv2 要求のみをサポートします。GTPv0 または GTPv1 実サーバは、GTPv2 要求を処理できません。実サーバが異なる場合、GTPv2 要求および GTPv0/v1 要求に別個の仮想サーバを作成する必要があります。

GTP-SLB アーキテクチャの概要

図 23-1 に、GTP-SLB アーキテクチャを示します。GTP-SLB 実装の 3 つの主要コンポーネント（SGSN/MME、GTP-SLB VIP、および GGSN/PGW）は、次の目的で通信します。

- PDP セッションの作成（PDP の作成コール フロー）。
- ゲートウェイのステータスのチェック（GTP エコー コール フロー）。
- SLB とゲートウェイ間での通知メッセージの交換（GTP 通知メッセージ）。

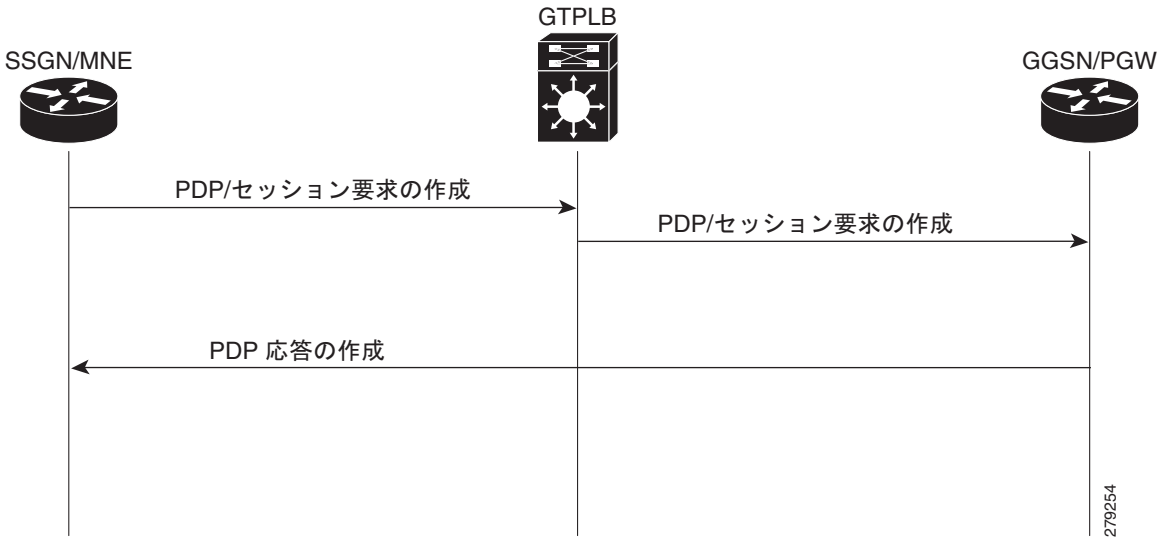
図 23-1　GTP-SLB アーキテクチャ



PDP の作成コール フロー

SGSN/MME は、宛先アドレスを IPv6 GTP-SLB VIP とした PDP の作成要求を開始します。SLB は、この要求をアクティブな IPv6 実（GGSN/PGW）サーバに転送します。GGSN は、PDP セッションを作成し、作成応答を直接 SGSN に送信します。図 23-2 に、PDP セッションの作成要求のコール フローを示します。

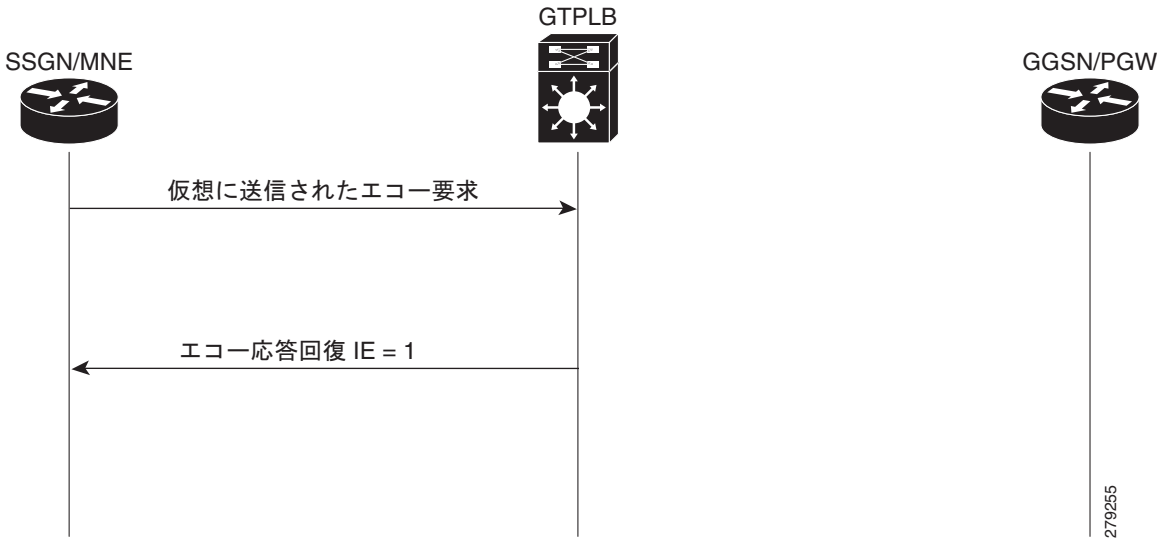
図 23-2　PDP セッションの作成要求のコール フロー



GTP エコー要求コール フロー

ゲートウェイのステータスをチェックするため、SGSN は SLB にエコーを送信します。仮想サーバがアクティブで動作可能である場合、SLB は IPv6 エコー応答でエコーに応答します。図 23-3 に、GTP エコー要求コール フローを示します。

図 23-3　GTP エコー要求コール フロー



GTP 通知メッセージ

ここでは、SLB とゲートウェイ間で交換される通知メッセージの一覧を示します。

- スティッキ アイドル タイマーがしきい値制限を超えると、SLB から実サーバに PDP クエリー要求が送信されます。GGSN は、PDP ステータス クエリーに対して PDP ステータス応答を返します。International Mobile Subscriber Identity（IMSI）タイマーに対応する PDP がゲートウェイに存在する場合はスティッキ タイマーが再起動し、存在しない場合は IMSI のタイマーおよびスティッキが削除されます。
- SGSN は実サーバ（GGSN/PGW）に PDP の削除要求を送信します。実サーバ（GGSN/PGW）は、PDP コンテキストを削除し、PDP 削除通知を SLB に送信します。削除通知を受信すると、SLB は IMSI のスティッキ エントリとスティッキ タイマー インスタンスを削除します。
- セッションを処理できない場合、実ゲートウェイは SLB に Call Admission Control（CAC; コール アドミッション制御）再割り当て通知を送信します。SLB は、セッションを別の実サーバに再割り当てすることによって応答します。

制約事項および使用上の注意事項

GTP-SLB の IPv6 サポートを設定する場合は、次の制約事項および使用上の注意事項に従ってください。

- 同じ仮想サーバに関連付けられたすべての IPv4 および IPv6 サーバファームには、同じ NAT 設定が必要です。
- クライアント側のインターフェイスに対するホットスタンバイ ルータ プロトコル（HSRP）インスタンス（IPv4 および IPv6）は、HSRP ステートが同じである必要があります。
- Long Term Evolution（LTE）ゲートウェイには、デュアル スタックを設定する必要があります。
- PGW/GGSN ゲートウェイには必ず、仮想サーバの IPv4 および IPv6 VIP アドレスを設定する必要があります。このアドレスは、ゲートウェイで通知用に使用されます。
- IPv6 アドレスに対しては、クライアント側の SLB 仮想サーバ コンフィギュレーション モードのコマンドはサポートされません。
- IOS SLB とゲートウェイ間のインタオーフェイスには、IPv6 と IPv4 の両方のアドレス（デュアル スタック）を設定する必要があります。

GTP-SLB IPv6 サポートの設定

GTP ロード バランシングに IPv6 サポートを設定する場合は、次の作業が必要です。

- SLB サーバファーム コンフィギュレーション モードで **real** コマンドを使用して、実サーバに IPv6 アドレスを指定する。
- SLB 仮想サーバ コンフィギュレーション モードで **virtual** コマンドを使用して、仮想サーバに IPv6 アドレスとオプションの IPv6 プレフィックスを指定する。
- SLB 仮想サーバ コンフィギュレーション モードで **serverfarm** コマンドを使用して、プライマリ IPv6 サーバ ファームとオプションのバックアップ IPv6 サーバファームを指定する。

GTP-SLB に IPv6 サポートを設定するこのプロセスでは、次の手順を実行します。

- サーバファームの設定
- 仮想サーバの設定

サーバファームの設定

ここでは、サーバファームの設定方法について説明します。

手順の概要

1. enable
2. **configure terminal**
3. ***ip slb serverfarm*** *server-farm*
4. **access *interface***
5. **nat {client *pool* | server}**
6. **predictor [roundrobin | leastconns | route-map *mapname*]**
7. **probe *probe***
8. **real ipv4-address [ipv6 *ipv6-address*] [*port*]**
9. **faildetect numconns *number-of-conns* [numclients *number-of-clients*]**
10. **maxclients *number-of-conns***
11. **maxconns *number-of-conns* [sticky-override]**
12. **reassign *threshold***
13. **retry *retry-value***
14. **weight *setting***
15. **inservice**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**ip slb serverfarm** *server-farm* **例：** *`Router(config)# ip slb serverfarm PUBLIC`*	サーバ ファームの定義を IOS SLB 設定に追加し、サーバ ファーム 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	**access** *interface* **例：** `Router(config-slb-sfarm)# access GigabitEthernet 0/1.1`	（任意）サーバ ファームのアクセス インターフェイスまたはサブインターフェイスを設定します。

	コマンド	目的
ステップ 5	***nat*** *{**client** pool* | ***server**}* **例：** `Router(config-slb-sfarm)# nat server`	（任意）サーバ ファームで、ネットワーク アドレス変換（NAT）クライアントの変換モードまたは NAT サーバ アドレス変換モードを設定します。
ステップ 6	**predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*] **例：** `Router(config-slb-sfarm)# predictor leastconns`	（任意）実サーバを選択する方法を決定するために使用するアルゴリズムを指定します。 GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングでは、デフォルト設定（加重ラウンド ロビン アルゴリズム）を受け入れる必要があります。 Home Agent Director は、デフォルト設定（加重ラウンド ロビン アルゴリズム）のみで機能します。 SLB サーバ ファーム コンフィギュレーション モードで **predictor route-map** コマンドを使用する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。
ステップ 7	**probe** *probe* **例：** `Router(config-slb-sfarm)# probe PROBE1`	（任意）プローブを実サーバに関連付けます。

ステップ 8	`real ipv4-address [ipv6 ipv6-address] [port]`
	
	例：
	`Router(config-slb-sfarm)# real 10.1.1.1 ipv6 100::10:10:10:1`
		サーバ ファームのメンバーとして、実サーバを IPv4 アドレスと IPv6 アドレス、およびオプションのポート番号で識別し、実サーバ コンフィギュレーション モードを開始します。
		
		（注） GPRS ロード バランシングでは、GGSN 機能を実行している実サーバの IP アドレス（Cisco GGSN の場合は仮想テンプレート アドレス）を指定します。

ステップ 9	**faildetect numconns** *number-of-conns* [**numclients** *number-of-clients*] **例：** `Router(config-slb-real)# faildetect numconns 10 numclients 3`	（任意）連続する接続エラーの回数、およびオプションで特定クライアントの接続エラーの回数を指定します。この回数を超えると、実サーバの障害と見なされます。 GPRS ロード バランシングの場合、環境内に単一の SGSN が設定されているときは、値 1 の numclients キーワードを指定します。 RADIUS ロード バランシングの場合、自動的なセッションベースの障害検出のために、値 1 の numclients キーワードを指定します。
ステップ 10	**maxclients** *number-of-conns* **例：** `Router(config-slb-real)# maxclients 10`	（任意）個々の仮想サーバに割り当てることができる IOS SLB RADIUS および GTP スティッキ加入者の最大数を指定します。

	コマンド	目的
ステップ 11	**maxconns** *number-of-conns* [**sticky-override**] **例：** `Router(config-slb-real)# maxconns 1000`	（任意）実サーバで 1 つのインスタンスに使用できるアクティブな接続の最大数を指定します。
ステップ 12	**reassign** *threshold* **例：** `Router(config-slb-real)# reassign 2`	（任意）連続して ACK が受信されない Synchronize Sequence Number（SYN）要求または PDP の作成要求のしきい値を指定します。しきい値を超えると、別の実サーバへの接続が試行されます。 **（注）** GPRS ロード バランシングの場合、SGSN の N3-REQUESTS カウンタ値未満の再割り当てしきい値を指定する必要があります。
ステップ 13	**retry** *retry-value* **例：** `Router(config-slb-real)# retry 120`	（任意）サーバ障害が検出されてから、そのサーバへの接続を再試行するまでの時間間隔を秒単位で指定します。
ステップ 14	**weight** *setting* **例：** `Router(config-slb-real)# weight 24`	（任意）実サーバの作業負荷容量をサーバ ファーム内の他のサーバと比較して指定します。 Dynamic Feedback Protocol（DFP; ダイナミック フィードバック プロトコル）を使用する場合、サーバ ファーム コンフィギュレーション モードで weight コマンドを使用して定義したスタティックな加重よりも、DFP によって算出された加重の方が優先されます。ネットワークから DFP を外すと、IOS SLB はスタティックなな加重に戻されます。

ステップ 15	`inservice`
	
	例：
	`Router(config-slb-real)# inservice`
		実サーバを IOS SLB で使用できるようにします。

仮想サーバの設定

ここでは、仮想サーバの設定方法について説明します。

手順の概要

1. enable
2. **configure terminal**
3. **ip slb vserver** ***virtual-server***
4. **virtual** ***ip-address*** **[*****netmask*** **[group]] {esp | gre |** ***protocol*****}** または **virtual** ***ip-address*** **[*****netmask*** **[group]] {tcp | udp} [port | any] [service service]** または **virtual** ***ip-address*** **[*****netmask*** **[group]] [ipv6** ***ipv6-address*** **[prefix** ***ipv6-prefix*****]] {tcp | udp} [port | any] [service** ***service*****]**

5. **serverfarm *primary-farm* [backup *backup-farm* [sticky] | [map *map-id* priority *priority*]] または serverfarm [*primary-farm* [backup *backup-farm*]] [[ipv6-primary *ipv6-primary-farm* [ipv6-backup *ipv6-backup-farm*]]] [map *map-id* priority *priority*]**
6. **access *interface* [route framed-ip]**
7. **advertise [active]**
8. **client {*ip-address netmask* [exclude] | gtp carrier-code [*code*]}**
9. **delay {*duration* | radius framed-ip *duration*}**
10. **gtp notification cac [*reassign-count*]**
11. **gtp session**
12. **hand-off radius *duration***
13. **idle [asn request *duration* | asn msid *msid* | gtp imsi *duration* [query [*max-queries*]] | gtp request *duration* | ipmobile request *duration*| radius {request | framed-ip} *duration*]**
14. **replicate casa *listen-ip remote-ip port* [*interval*] [password [*encrypt*] *secret-string timeout*]**
15. **replicate interval *interval***
16. **replicate slave**
17. **sticky {*duration* [group *group-id*] [netmask *netmask*] | asn msid [group *group-id*] | gtp imsi [group *group-id*] | radius *calling-station-id* | radius framed-ip [group *group-id*] | radius username [msid-cisco] [group *group-id*]}**
18. **synguard *syn-count interval***
19. **inservice [standby *group-name*] [*active*]**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**ip slb vserver** *virtual-server* **例：** *`Router(config)# ip slb vserver PUBLIC_HTTP`*	仮想サーバを指定し、仮想サーバ 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 4	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** [*ipv6-address* [**ipv6-prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] **例：** `Router(config-slb-vserver)# virtual 10.0.0.1 ipv6 100::100:1 udp 0 service gtp`	次の情報を指定します。 • 仮想サーバの IP アドレス • IPv6 アドレス（接続タイプを含む） • オプションの TCP または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号 • Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP; ワイヤレス セッション プロトコル）の設定 • サービスのカップリング GPRS ロード バランシングの場合： 仮想 GGSN IP アドレスを仮想サーバとして指定し、*udp* キーワード オプションを指定します。 GTP v1 および GTP v2 セッションをロード バランシングするには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 *2123* を指定します。また、全ポート仮想サーバを設定するには、ポート番号 0 または any を指定します（この場合、仮想サーバはすべてのポート宛てのフローを受け入れます）。 GTP v0 セッションをロード バランシングするには、GGSN および SGSN が ETSI 標準に準拠している場合はポート番号 3386 を指定し、全ポート仮想サーバを設定するにはポート番号 0 または any を指定します。
ステップ 5	**serverfarm** [*primary-farm* [**backup** *backup-farm*]] [[**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]]] [**map** *map-id* **priority** *priority*] **例：** `Router(config-slb-vserver)# serverfarm SF backup BACKUPSF ipv6-primary V6SF ipv6-backup BACKUPV6SF map 1 priority 1`	実サーバ ファームを仮想サーバに関連付け、任意でバックアップ サーバ ファームを設定します。 GPRS ロード バランシングで、複数のサーバ ファームに同じ実サーバが定義されている場合、各サーバ ファームは異なる仮想サーバに関連付ける必要があります。 複数のサーバ ファームを GTP 仮想サーバに関連付けるには、serverfarm コマンドを複数設定し、それぞれに固有のマップ ID と固有のプライオリティを指定します
ステップ 6	***access*** *interface* [***route framed-ip***] **例：** `Router(config-slb-vserver)# access Vlan20 route framed-ip`	（任意）入力インターフェイスを検査するには、framed-IP ルーティングをイネーブルにします。
ステップ 7	**advertise** [**active**] **例：** `Router(config-slb-vserver)# advertise`	（任意）仮想サーバ アドレスの Null またはゼロ インターフェイスに対するスタティック ルートのインストールを制御します。

	コマンド	目的
ステップ 8	**client** {*ip-address netmask* [**exclude**] | **gtp carrier-code** [*code*]} **例：** `Router(config-slb-vserver)# client 10.4.4.0 255.255.255.0`	（任意）仮想サーバの使用を許可するクライアントを指定します。 GTP Cause Code Inspection がイネーブルの場合に限り、GPRS ロード バランシングは **gtp carrier-code** オプションだけをサポートします。
ステップ 9	**delay** {*duration* | **radius framed-ip** *duration*} **例：** `Router(config-slb-vserver)# delay 30`	（任意）接続の終了後に IOS SLB が TCP 接続コンテキストを維持する時間を指定します。
ステップ 10	**gtp notification cac** [*reassign-count*] **例：** `Router(config-slb-vserver)# gtp notification cac 5`	（任意）IOS SLB が GGSN-IOS SLB メッセージングのために新しい実サーバにセッションを割り当てることができる回数を制限します。

ステップ 11	`gtp session`
	
	例：
	`Router(config-slb-vserver)# no gtp session`
		（任意）IOS SLB で GTP ロード バランシング セッションを作成できるようにします。これがデフォルト設定です。
		GTP 用の sticky-only ロード バランシングをイネーブルにするには、このコマンドの no 形式を使用します。
		sticky-only ロード バランシングをイネーブルにした場合は、**sticky**（**仮想サーバ**）コマンドを使用して、仮想サーバのスティッキ接続もイネーブルにする必要があります。

ステップ 12	**hand-off radius** *duration* **例：** `Router(config-slb-vserver)# hand-off radius 30`	（任意）外部エージェントのハンドオフ時に、IOS SLB が新しい Mobile IP 外部エージェントからの ACCT-START メッセージを待機する時間を変更します。
ステップ 13	**idle** [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*] **例：** `Router(config-slb-vserver)# idle 120`	（任意）パケット アクティビティが存在しない場合に、IOS SLB が接続コンテキストを維持する最短時間を指定します。 **（注）** GTP Cause Code Inspection をイネーブルにしない GPRS ロード バランシングの場合、SGSN 上の PDP コンテキスト要求間で可能な最も長い間隔よりも、長いアイドル タイマーを指定します。

	コマンド	目的
ステップ 14	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string timeout*] **例：** `Router(config-slb-vserver)# replicate casa 10.10.10.11 10.10.11.12 4231`	（任意）IOS SLB デシジョン テーブルのバックアップ スイッチへのステートフル バックアップを設定します。 **（注）** Home Agent Director はこのコマンドをサポートしません。 virtual コマンドに service *gtp* キーワードを指定して、**sticky** コマンドに *gtp imsi* キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません。これは、セッションが持続されず、何も複製されないためです。
ステップ 15	**replicate interval** *interval* **例：** `Router(config-slb-vserver)# replicate interval 20`	（任意）IOS SLB 仮想サーバの複製配信間隔を設定します。 Home Agent Director はこのコマンドをサポートしません。 virtual コマンドに service *gtp* キーワードを指定して、**sticky** コマンドに ***gtp imsi*** キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません。これは、セッションが持続されず、何も複製されないためです。
ステップ 16	**replicate slave** **例：** `Router(config-slb-vserver)# replicate slave`	（任意）IOS SLB 仮想サーバの冗長ルート プロセッサのステートフル バックアップをイネーブルにします。 Home Agent Director はこのコマンドをサポートしません。 virtual コマンドに service *gtp* キーワードを指定して、**sticky** コマンドに *gtp imsi* キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません。これは、セッションが持続されず、何も複製されないためです。 **（注）** replicate slave が設定された 1 つのスーパーバイザ エンジンを使用している場合は、そのスーパーバイザで out-of-sync メッセージを受信する可能性があります。
ステップ 17	**sticky** {*duration* [**group** *group-id*] [**netmask** *netmask*] | **asn msid** [**group** *group-id*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]} **例：** `Router(config-slb-vserver)# sticky 60 group 10`	（任意）クライアント接続の間隔が指定した期間を超えるまで、同じクライアントからの接続が同じ実サーバを使用するように指定します。 VPN サーバ ロード バランシングの場合、15 秒以上の duration を指定します。 GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。

	コマンド	目的
ステップ 18	**synguard** *syn-count interval* **例：** `Router(config-slb-vserver)# synguard 50`	（任意）SYN フラッド サービス拒否攻撃を阻止するために、仮想サーバによって管理される TCP Synchronize Sequence Number（SYN）のレートを指定します。 **（注）** GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。
ステップ 19	**inservice** [**standby** *group-name*] [**active**] **例：** `Router(config-slb-vserver)# inservice`	仮想サーバをイネーブルにします。

例

次に、IPv6 アドレスだけを受け入れるサーバファームを設定する例を示します。

```
mwtcL05-SLB1(config)#ip slb map 1 gtp
mwtcL05-SLB1(config-slb-map-gtp)#apn abc.com
mwtcL05-SLB1(config-slb-map-gtp)#apn 456.com
mwtcL05-SLB1(config-slb-map-gtp)#apn gprs.cisco.com
mwtcL05-SLB1(config-slb-map-gtp)#ip slb map 2 gtp
mwtcL05-SLB1(config-slb-map-gtp)#apn 123.com
mwtcL05-SLB1(config-slb-map-gtp)#apn xyz.com
mwtcL05-SLB1(config-slb-map-gtp)#apn gprs_intdhcp.cisco.com
mwtcL05-SLB1(config-slb-map-gtp)#end
mwtcL05-SLB1(config)#ip slb serverfarm GGSN_FARM1
mwtcL05-SLB1(config-slb-sfarm)#real 21.21.21.1 ipv6 2021::21:21:21:1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#real 22.22.22.1 ipv6 2022::22:22:22:1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#end
mwtcL05-SLB1#conf t
mwtcL05-SLB1(config)#ip slb vserver GGSN_SERVER1
mwtcL05-SLB1(config-slb-vserver)#virtual 20.20.20.1 ipv6 2020::20:20:20:1 udp 2123 service
gtp
mwtcL05-SLB1(config-slb-vserver)#serverfarm ipv6-primary GGSN_FARM1 map 1 priority 1
mwtcL05-SLB1(config-slb-vserver)#sticky gtp imsi group 1
mwtcL05-SLB1(config-slb-vserver)#gtp notification cac 2
mwtcL05-SLB1(config-slb-vserver)#idle 180
mwtcL05-SLB1(config-slb-vserver)#inservice
mwtcL05-SLB1(config-slb-vserver)#end
```

次に、IPv4 アドレスと IPv6 アドレスを受け入れるサーバファームを設定する例を示します。

```
mwtcL05-SLB1(config)#ip slb map 1 gtp
mwtcL05-SLB1(config-slb-map-gtp)#apn abc.com
mwtcL05-SLB1(config-slb-map-gtp)#apn 456.com
mwtcL05-SLB1(config-slb-map-gtp)#apn gprs.cisco.com
mwtcL05-SLB1(config-slb-map-gtp)#ip slb map 2 gtp
mwtcL05-SLB1(config-slb-map-gtp)#apn 123.com
mwtcL05-SLB1(config-slb-map-gtp)#apn xyz.com
mwtcL05-SLB1(config-slb-map-gtp)#apn gprs_intdhcp.cisco.com
```

```
mwtcL05-SLB1(config-slb-map-gtp)#end
mwtcL05-SLB1(config)#ip slb serverfarm GGSN_FARM1
mwtcL05-SLB1(config-slb-sfarm)#real 21.21.21.1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#real 22.22.22.1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#end
mwtcL05-SLB1(config)#ip slb serverfarm GGSN_FARM2
mwtcL05-SLB1(config-slb-sfarm)#real 21.21.21.1 ipv6 2021::21:21:21:1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#real 22.22.22.1 ipv6 2022::22:22:22:1
mwtcL05-SLB1(config-slb-real)#weight 1
mwtcL05-SLB1(config-slb-real)#reassign 0
mwtcL05-SLB1(config-slb-real)#inservice
mwtcL05-SLB1(config-slb-real)#end
mwtcL05-SLB1#conf t
mwtcL05-SLB1(config)#ip slb vserver GGSN_SERVER1
mwtcL05-SLB1(config-slb-vserver)#virtual 20.20.20.1 ipv6 2020::20:20:20:1 udp 2123 service
gtp
mwtcL05-SLB1(config-slb-vserver)#serverfarm GGSN_FARM1 ipv6-primary GGSN_FARM2 map 1
priority 1
mwtcL05-SLB1(config-slb-vserver)#sticky gtp imsi group 1
mwtcL05-SLB1(config-slb-vserver)#gtp notification cac 2
mwtcL05-SLB1(config-slb-vserver)#idle 180
mwtcL05-SLB1(config-slb-vserver)#inservice
mwtcL05-SLB1(config-slb-vserver)#end
```

検証

GTP-SLB IPv6 の設定を検証するには、次のコマンドを実行します。

- show ip slb real detail コマンド。実サーバに関する情報を表示します。

```
mwtcL05-SLB1#show ip slb real detail

21.21.21.1, GGSN_FARM1, state = OPERATIONAL, type = server
ipv6 = 2021::21:21:21:1
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 1, weight(admin) = 1, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0

22.22.22.1, GGSN_FARM1, state = OPERATIONAL, type = server
ipv6 = 2022::22:22:22:1
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 1, weight(admin) = 1, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

- **show ip slb sticky gtp imsi ipv6** コマンド。簡潔な GTP-SLB IPv6 の設定を表示します。

```
mwtcL05-SLB1# show ip slb sticky gtp imsi ipv6

IMSI             Real             Ver  Group Id vs_index refcount NSAPIs
-------------------------------------------------------------------------
12345678901234F6 21.21.21.1       1    1        7        1        0
                 2021::21:21:21:1
12345678901234F5 22.22.22.1       1    1        7        1        0
                 2022::22:22:22:1

mwtcL05-SLB1# show ip slb stats
Pkts via normal switching:     0
Pkts via special switching:    2
Pkts via slb routing:          0
Pkts Dropped:                  0
Pkts DMA punted:               0
Connections Created:           2
Connections Established:       2
Connections Destroyed:         0
Connections Reassigned:        0
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS framed-ip Sticky Count: 0
RADIUS username Sticky Count:  0
RADIUS cstn-id Sticky Count:   0
GTP imsi Sticky Count:         2
ASN msid sticky count:         0
ASN NAI count:                 0
Failed Correlation Injects:    0
Pkt fragments drops in ssv:    0
```

- **show ip slb session gtp ipv6** コマンド。セッション情報を表示します。

```
mwtcL05-SLB1# show ip slb session gtp ipv6
vserver = GGSN_SERVER1, key = 1112223334444100
 client = 2002::77:77:77:3
 real = 3003::21:21:21:1
 state = SLB_IPV6_GTP_ESTAB

vserver = GGSN_SERVER1, key = 1112223334444200
 client = 2002::77:77:77:3
 real = 3003::22:22:22:1
 state = SLB_IPV6_GTP_ESTAB

vserver = GGSN_SERVER1, key = 1112223334444300
 client = 2002::77:77:77:3
 real = 3003::23:23:23:1
 state = SLB_IPV6_GTP_ESTAB

vserver = GGSN_SERVER1, key = 1112223334444400
 client = 2002::77:77:77:3
 real = 3003::24:24:24:1
 state = SLB_IPV6_GTP_ESTAB

vserver = GGSN_SERVER1, key = 1112223334444500
 client = 2002::77:77:77:3
 real = 3003::21:21:21:1
 state = SLB_IPV6_GTP_ESTAB
```

- **show ip slb stats** コマンド。SLB 統計情報を表示します。

```
mwtcL05-SLB1# show ip slb stats
```

```
Pkts via normal switching:     0
Pkts via special switching:    2
Pkts via slb routing:          0
Pkts Dropped:                  0
Pkts DMA punted:               0
Connections Created:           2
Connections Established:       2
Connections Destroyed:         0
Connections Reassigned:        0
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS framed-ip Sticky Count: 0
RADIUS username Sticky Count:  0
RADIUS cstn-id Sticky Count:   0
GTP imsi Sticky Count:         2
ASN msid sticky count:         0
ASN NAI count:                 0
Failed Correlation Injects:    0
Pkt fragments drops in ssv:    0
```

- **show ip slb vservers name GGSN_SERVER2** コマンド。簡潔な仮想サーバの設定を表示します。

```
mwtcL05-SLB1# show ip slb vservers name GGSN_SERVER2
slb vserver      prot  virtual                 state         conns    interface(s)
-------------------------------------------------------------------------------
GGSN_SERVER2     UDP   20.20.20.1/32:2123      INSERVICE       0         any
                       2020::20:20:20:1/128
```

- **show ip slb vservers name GGSN_SERVER2 detail** コマンド。詳細な仮想サーバの設定を表示します。

```
mwtcL05-SLB1# show ip slb vservers name GGSN_SERVER2 detail

GGSN_SERVER2, state = OPERATIONAL, v_index = 10, interface(s) = <any>
virtual = 3.3.3.3/32:2123, UDP, service = GTP, advertise = TRUE
ipv6 = 3:3:3:3:3:3:3:3/128
serverfarm maps:
map 1: priority = 1, serverfarm = SF, backup serverfarm= SF1
ipv6 serverfarm = SF2 ipv6 backup serverfarm = SF3
severfarm = SF, backup serverfarm = SF1
ipv6 serverfarm = SF2, ipv6 backup serverfarm = SF3
backup_serverfarm_hits = 0
delay = 10, idle = 3600
gtp: request idle = 30
slb notification retry = 2
gtp sticky query: <disabled>
max retries: 0
sticky: <none>
group id = 0
synguard counter = 0, synguard period = 0
conns = 0, total conns = 0, syns = 0,  syn drops = 0
standby group = None
```

GTP-SLB IPv6 サポートの設定のトラブルシューティング

ここでは、GTP-SLB IPv6 サポートの設定をトラブルシューティングする手順について説明します。次に、一部のトラブルシューティング シナリオを示します。

- GTP-SLB で最少接続属性（Leastconns）を設定できない。

ロードバランサは、実サーバのオープン PDP セッション数を追跡しないので、GTP-SLB では Leastconns はサポートされません。SLB は、PDP の作成要求をロード バランスし、割り当てられた実サーバに要求が再送信されるように、各 PDP 要求のセッション オブジェクトを維持するだけです。

- IOS SLB スティッキ接続が予期したとおりに機能しない。

  有効なスティッキ接続を確認するには、次の手順を実行します。

  - すべてのスティッキ接続を再設定します。
  - クライアント接続を開始します。
  - **show ip slb reals detail** コマンドおよび **show ip slb conns** コマンドを実行します。
  - 実サーバの接続カウントを確認します。新しいクライアント接続は、カウントが増加した実サーバに割り当てられることに注意してください。
  - **show ip slb sticky** コマンドを実行して、IOS SLB に格納されているスティッキの関係を表示します。
  - 接続を終了します。
  - 実サーバ接続が 1 カウントずつ減少するかどうかを確認します。
  - スティッキ タイムアウト値内で接続を再開します。
  - **show ip slb conns** コマンドを実行します。
  - 実サーバの接続カウントをもう一度調べて、スティッキ接続が同じ実サーバに割り当てられていることを確認します。

- サーバ障害が適切に検出されない。

  サーバを確認するには、次の手順を実行します。

  - クライアント数が非常に少ないことを確認し、faildetect numconns（実サーバ）の numclients 値を最適な値まで減らします。
  - **show ip slb reals detail** コマンドを実行して、実サーバのステータスを表示します。
  - 実サーバのステータスと接続カウントを確認します。障害のあるサーバのステータスは、FAILED、TESTING、または READY_TO_TEST のいずれかになります。

（注） 実サーバに障害が発生すると、割り当て済みで確立していない（SYN または ACK を受信していない）接続は、reassign しきい値に達した後、最初に受信した SYN で、別の実サーバに再割り当てされます。ただし、実サーバへの接続がすでに確立されている場合は、同じ実サーバに転送されます。

（注） 加重最少接続の場合、新規の接続で過負荷状態にならないように、新規の実サーバはスロー スタートします （詳細については、「Slow Start」の項を参照してください）。また、新規の実サーバの接続カウントは、ダミー接続を示します。ダミー接続は、IOS SLB が実サーバのスロー スタート時の接続カウントを意図的につり上げるために使用されます。

- faildetect inband とインターネット制御メッセージ プロトコル（ICMP）プローブの両方を実サーバに設定しても、障害検出が向上しない。

  実サーバに ICMP プローブと faildetect inband の両方が設定されている場合、faildetect が優先されます。ICMP プローブは health プローブであり、実サーバの物理インターフェイスがアクセス可能である限り、ICMP プローブの状態は OPERATIONAL のままとなります。faildetectinband に

よって、実サーバでクライアント要求を処理するアプリケーションの障害が検出されます。物理インターフェイスに障害が発生すると、ICMP プローブは状態を送信します。実サーバの障害検出用に、ICMP プローブか faildetect のいずれかをイネーブルにすることを推奨します。

- **no inservice** コマンドを実行しても、リソースがただちにディセーブルにならない。

  no inservice コマンドでは、リソースをディセーブルにする前に接続でプロセスを実行することが許可されます。ファイアウォール ファームまたは仮想サーバ全体について、すべての既存の接続をただちに停止するには、**clear ip slb connections** コマンドを使用します。

- GTPLB および HSRP が設定された仮想サーバのステータス、アクティブまたはスタンバイ シャーシが、両方のシャーシに対して表示される。1 つのインスタンスで、両方のシャーシがアクティブまたはスタンバイとして表示される。

  これらの問題については、次の設定を確認してください。

  - 複数の HSRP インスタンスが設定されている場合、HSRP インターフェイスに固有のグループ番号が設定されている必要があります。
  - HSRP グループ名は大文字と小文字を区別し、固有である必要があります。

- NAT サーバのサーバファーム設定では、レイヤ 3 および非レイヤ 2 隣接接続を利用してパケットをロードバランスできます。
- GGSN（PGW）で dispatched モードが機能しない。

  GGSN にループバックとして VIP アドレスが設定されていることを確認します。

- directed モードでは、通知メッセージが SLB に到達しない。

  ネクスト ホップ IP アドレスを持つ仮想サーバ アドレスが、ゲートウェイに設定されていることを確認します。

- GGSN にアドレス プールが設定されているが、MS アドレスを割り当てることができない。

  SGPRS からの PDP 要求の作成時に指定されたアドレスが、定義されているプール内のアドレスに一致していない可能性があります。

CHAPTER 24

IP Subscriber Awareness over Ethernet

この章では、Cisco 7600 のさまざまな機能をスケールして IP Subscriber Awareness over Ethernet 機能（*IP 加入者集約*とも呼ばれる）をサポートする方法について説明します。この機能は Cisco IOS Release 12.2SRB で Cisco 7600 シリーズ ルータ用に導入されたものです。Cisco IOS Release 12.2(33)SRE 以降は、Cisco 7600 シリーズ ルータ上の分散 IP および PPPoE セッション内での ISG 機能が Ethernet Services Plus（ES+）アクセス対向ラインカード上でサポートされています。

この章の内容は、次のとおりです。

- 「概要」（P.24-1）
- 「IP 加入者セッションの機能」（P.24-4）
- 「IP Subscriber Awareness over Ethernet 設定時の注意事項」（P.24-28）
- 「IP Subscriber Awareness over Ethernet の設定」（P.24-29）
- 「コマンド リファレンス」（P.24-33）

（注） IP および PPPoE セッションのための ISG 機能のサポートは、ES+ ラインカードおよび SIP400 に対して廃止され、将来のリリースでは使用できません。

概要

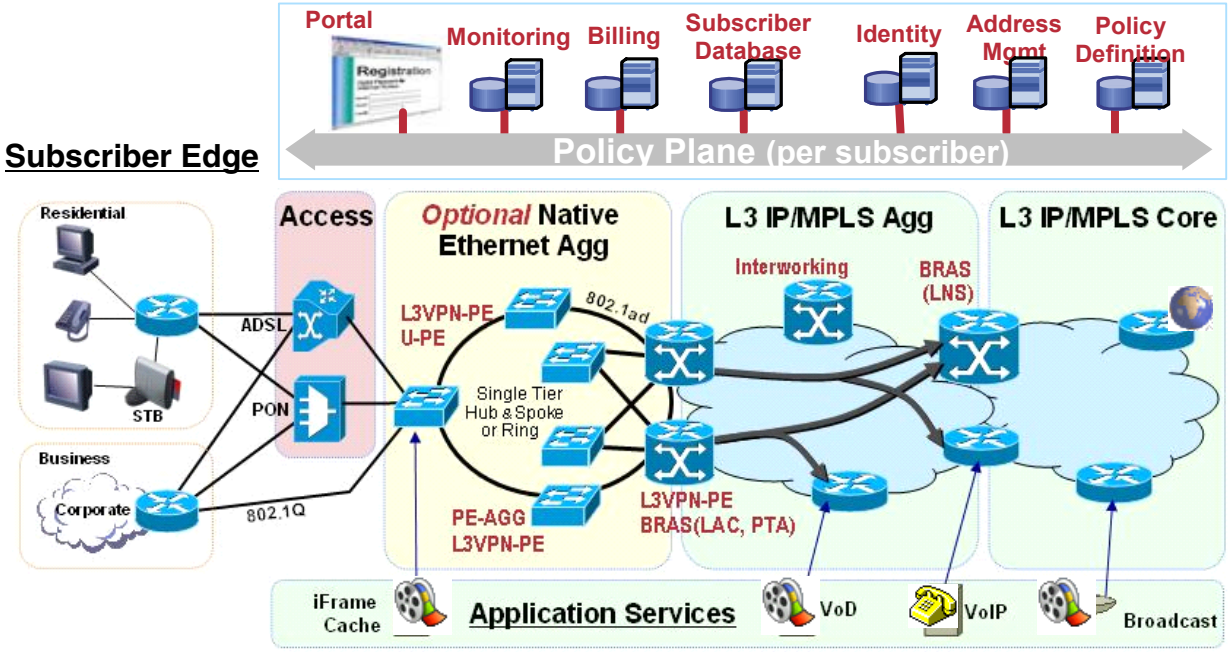
IP Subscriber Awareness over Ethernet は Cisco 7600 ルータを DSLAM Gigabit Ethernet（GE; ギガビット イーサネット）集約器として使用するアーキテクチャで使用できるよう設計されています。このシナリオでは、DSLAM は複数の VLAN 向けにデータ伝送可能な物理ポートを介してルータに接続されています。

IP Subscriber Awareness over Ethernet 機能は、加入者と DSLAM との間でサービスを伝送する下記の 2 つのモデルをサポートします。

- サービス単位の VLAN モデル：1 つまたは複数の ATM VC を使用して、各タイプのサービス（ビデオ、音声、およびデータ）を加入者と VLAN 間で伝送します。
- 加入者単位の VLAN モデル：単一の ATM VC を使用して、すべてのトラフィック（ビデオ、音声、およびデータ）を加入者と DSLAM 間で伝送します。

図 24-1 に、IP Subscriber Awareness over Ethernet が使用されるワイヤライン イーサネット アーキテクチャの例を示します。

図 24-1　ワイヤライン イーサネット アーキテクチャ



ここでは、IP Subscriber Awareness over Ethernet 機能の詳細を説明します。

- 「利点」（P.24-2）
- 「IP 加入者のインターフェイス」（P.24-3）
- 「IP 加入者セッション」（P.24-3）
- 「IP 加入者セッションの機能」（P.24-4）

利点

IP Subscriber Awareness over Ethernet 機能には次の利点があります。

- Cisco 7600 ルータ上での IP セッションの終端および IP セッションの集約
- ルータ上で最大 32000 の IP 加入者をサポート（単一の Cisco 7600 SIP-400 では最大 8000 の加入者）
- ルータ上で最大 32000 インターフェイスに対応するインターフェイス スケーラビリティ
  - 各物理ポートで最大 1000 サブインターフェイスをサポート
  - 各 Cisco 7600 SIP-400 で最大 8000 サブインターフェイスをサポート
- IP 加入者の DHCP および Radius アカウンティング。256 の DHCP プールをサポート。DHCP は IP 加入者セッションに対し最大 150 コール/秒を処理可能。
- 各 IP 加入者に対する QoS サポート（最大 32000 の加入者）。分類（IP prec および DSCP）、ポリシング、シェーピング、マーキング、プライオリティ キュー、および Weighted Random Early Detection（WRED; 重み付きランダム早期検出）を含む。
- 加入者単位の統計情報およびアカウンティング情報

- 最大 96000 ARP エントリをサポート
- IP 加入者に RPR、RPR+、Stateful Switchover（SSO）、Non-Stop Forwarding（NSF）を提供
- Control Plane Protection（CoPP）により Denial of Service（DoS; サービス拒絶）攻撃および他の攻撃から保護

IP 加入者のインターフェイス

Cisco IOS Release 12.2SRB では、IP 加入者を表すための新しいタイプのインターフェイスが導入されています。

- アクセス：各 IP 加入者を表すサブインターフェイス。アクセス サブインターフェイスは、.1Q または Q-in-Q カプセル化向けに設定できます。

  トラフィック シェーピングおよびポリシング ポリシー（HQoS など）をアクセス インターフェイスに適用して、さまざまなタイプの加入者トラフィック（音声やデータなど）に割り当てる帯域幅の量を定義します。

（注）　アクセス インターフェイスを、IP 加入者が接続されている物理インターフェイスのサブインターフェイスとして設定します。

例

次に、インターフェイス上のアクセス サブインターフェイスの例を示します。

```
interface GigabitEthernet 1/0/0.100 access
    ip vrf forwarding vrf0
    encapsulation dot1q 100
```

- ES+ ラインカード上では、この機能がアクセス インターフェイスと非アクセス インターフェイス（上限 500 サブインターフェイス）でサポートされます。

IP 加入者セッション

IP 加入者が共有 VLAN を使用してネットワークへアクセスする間、IP 加入者セッションが存在します。IP 加入者セッションを開始するには、ルータは IP アドレスを加入者のアクセス サブインターフェイスに割り当てる必要があります。サブインターフェイスに静的 IP アドレスを割り当てることも、DHCP を使用してアドレスを割り当てることもできます。これら 2 つの方法を使用して IP アドレスを割り当てる際の注意事項を次に示します。

- 静的 IP アドレス：アクセス サブインターフェイスに静的 IP アドレスを割り当てた場合、IP 加入者セッションは常に起動していると見なされます。多数の IP 加入者を静的 IP アドレスを使って設定しないことを推奨します。
- DHCP で割り当てた IP アドレス：DHCP を使用して加入者セッションに IP アドレスを割り当てることができます。ルータが加入者の DHCP 検出パケットを受信すると、IP 加入者セッションが開始され、加入者に IP アドレスが割り当てられます。加入者が DHCP 解放メッセージを受信すると、セッションは終了し、IP アドレスが解放されます。加入者セッションが VRF を認識する場合（つまり、加入者が VRF に属している場合）、VRF を認識する DHCP プールを使用する必要があります。

（注）
- ルータは DHCP サーバまたは DHCP リレー デバイスとして動作できます。

- IP 加入者を VRF の一部として設定する（つまり、加入者セッションを VRF 認識できるようにする）には、VRF をアクセス サブインターフェイス下で設定します。

この機能は、ES+ ラインカード上の次のセッションをサポートします。

- IP セッション（ルーティング型と L2 接続型）
- IP を使用した DHCP 統合セッション
- スタティック IP サブネット セッション
- 送信元 IP アドレスおよび MAC アドレス セッション（IP セッション）
- PPP Termination and Aggregation（PTA）モードでサポートされる PPPoE
- PTA モードでサポートされる PPPoEoVLAN
- PTA モードでサポートされる PPPoEoQinQ
- PTA モードでサポートされる PPPoEoDot1Q

IP 加入者セッションの機能

IP 加入者セッションは次の機能を備えています。

- 加入者単位の Control Plane Policing and Protection（CoPP）：各加入者を Denial of Service（DoS; サービス拒否）攻撃および他の攻撃から保護します。攻撃が発生した場合、ルータはネットワーク管理者に通知し、悪質なトラフィックのポリシングを開始します。この機能により、ARP、DHCP、および ICMP トラフィックをポリシングできます。Cisco 7600 SIP-400 での CoPP の動作方法については、次の URL を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351662

- 加入者単位のセキュリティ ACL：セキュリティ アクセス コントロール リスト（ACL）を各加入者に適用できます。Cisco 7600 SIP-400 でのこの機能の動作方法については、次の URL を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351562

- 加入者単位の Radius アカウンティング：システム管理者による各加入者の IP セッション アクティビティの追跡や、加入者のアカウンティング レコードの定期的な抽出をイネーブルにします。加入者単位の Radius アカウンティングは DHCP IP アドレス割り当てと連動し、ブロードバンド サービスを提供するうえでの認証、許可、アカウンティング（AAA）を向上させます。この機能の詳細については、次の URL に記載されている説明を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/ipradacc.htm

- 合法的傍受：Law Enforcement Agency（LEA）をイネーブルにして、裁判所命令によって許可された、加入者に対する電子機器を用いた情報収集を実行します。情報収集を支援するため、サービス プロバイダーは加入者のトラフィックがこれらのルータのいずれかを通過する際に代行受信し、代行受信したトラフィックのコピーを加入者に通知することなく LEA に送信します。この機能の詳細については、次の URL のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76licfg/index.htm

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a0080440138.html#wp1351508

- Quality of Service：各加入者（アクセス サブインターフェイス）に対して標準 QoS 機能（分類、マーキング、ポリシング、シェーピング、プライオリティ キューイング、Weighted Random Early Detection（WRED; 重み付きランダム早期検出）など）がサポートされています。IP Subscriber Awareness over Ethernet で推奨される QoS 設定については、次のセクション（「QoS に関する推奨事項」）を参照してください。Cisco 7600 SIP-400 の QoS 機能の詳細については、次の URL の「Cisco 7600 SIP-400 Features」の項の QoS 機能に関する説明を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008044013b.html#wp1094663

  標準 QoS 機能に加えて、次に示す新しい Cisco 7600 SIP-400 QoS 機能が導入され、ブロードバンド サービスを展開できるようになりました。

  - デュアルプライオリティ キュー：4000 ～ 8000 の加入者に音声およびビデオ トラフィック用の 2 つのプライオリティ キューを提供します。各トラフィック クラスには異なるプライオリティ レベルを割り当てて（たとえば、音声トラフィックにビデオ トラフィックより高い優先順位を与えることで）、ルータがどちらのタイプのトラフィックもプライオリティ トラフィックとして処理し、また両トラフィックを個別に処理することができます。
  - Bandwidth Remaining Ratio（BRR; 帯域幅余剰比率）：輻輳時にサービス プロバイダーが加入者のトラフィックの優先順位を設定できます。残りの帯域幅使用比率の分配機能を使用して、サブインターフェイスまたはクラス キューの他のサブインターフェイスまたはクラス キューに対する相対的重みを指定できます。この機能の詳細については、「帯域幅余剰比率に関する推奨事項」（P.24-21）を参照してください。
  - プライオリティ レート伝播：下位レベル キュー内のプライオリティ トラフィックに割り当てられているプライオリティ レベルとトラフィック レートを取り込み、キュー階層内のすべてのより高いレベルのキューが最低レートまたはプライオリティ向けに設定されていない場合であっても、それらのキューのプライオリティ トラフィックにそのレベルとレートを適用します。詳細については、「プライオリティ レート伝播に関する推奨事項」（P.24-26）を参照してください。

IP アドレス割り当て

- DHCP ベースの IP アドレスの割り当て：IP アドレスの割り当てに DHCP が使用されている場合で、DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しい場合、ISG は、その加入者の IP アドレスを割り当てる必要がありません。DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しくない場合、または VRF 転送によってドメインが変更された場合、ISG は、DHCP IP アドレスの割り当てに関与するように設定できます。
- スタティック IP アドレス割り当て：加入者のスタティック IP アドレスがサービス ドメインに適切に設定されている場合は、ISG が加入者の IP アドレスの割り当てに関与しません。
- IP サブネット：IP サブネット セッションの場合は、IP サブネットがユーザ プロファイル内で指定されます。

IP インターフェイス：ISG が加入者 IP アドレスの割り当てに関与しません。

IP サブネット（IP 範囲）セッション

クライアント サブネットは、IP サブネット セッションを識別して、特定の IP サブネットに関連付けられたパケットに対して一貫したエッジ処理を適用します。IP サブネット セッションは、直接接続されたクライアントに対して、または、複数のホップ上でホストされます。次の機能は、IP サブネット セッションではサポートされませんが、IP セッションではサポートされます。

- DHCP セッション開始

- 送信元 MAC アドレス セッション
- ダイナミック VPN 選択

IP インターフェイス セッション

IP インターフェイス セッションでは、特定の物理インターフェイスまたは論理インターフェイス上で受信されたすべてのトラフィックが順番に処理されます。ただし、ダイナミック VRF 転送は IP インターフェイス セッションでサポートされません。VRF 転送はスタティック VRF 設定でのみ使用することができます。ログインしている加入者に関係なく、デフォルトでセッションが構築されます。

ポート チャネル上での PPPoE セッションと IPoE セッションのサポート（1:1 冗長性）

ポート チャネル上の 1:1 冗長性とリンク集約制御プロトコル（LACP）を組み合わせれば、ポート チャネル バンドル内のメンバー リンクを動的に処理することができます。ポート チャネルは 2 つのメンバー（アクティブなメンバーとスタンバイ状態または冗長モードのメンバー）で構成されます。メンバーのポートには、異なるラインカードのポートを使用できますが、Ethernet Services Plus（ES+）ラインカードにする必要があります。常に、いずれかのリンクが物理モードになっています。

次のセッションで ES+ ラインカード上の 1:1 冗長性がサポートされます。

- IP サブネット セッション
- IP インターフェイス セッション
- PPPoEoX セッション

IEEE 802.1AH Customer Ethertype を使用した QinQ サブインターフェイス上での PPPoE セッションと IPoE セッションのサポート

この機能を使用すれば、カスタム ethertype を使用して設定された QinQ サブインターフェイス上に PPPoE セッションと IPoE セッション（ISG 機能）を実装することができます。メイン インターフェイス上に実装されたカスタム ethertype は、すべてのサブインターフェイスに継承されます。この機能を実装するには、それぞれの QinQ サブインターフェイスのメイン インターフェイス上で **dot1q tunnel ethertype** コマンドを使用します。

PPPoE または IPoE セッション パケット上のその他の VLAN タグが QinQ サブインターフェイスのカスタム ethertype VLAN 設定に一致する場合、パケットは受け入れられ、一致しない場合はドロップされます。外部 VLAN タグは次の値に設定することができます。

- 0x9100
- 0x9200
- 0x8100
- 0x88a8

ISG とクライアント間の ethertype が一致しなかった場合は、PPPoE セッションまたは IPoE セッションが到着しません。たとえば、パケットの外部 VLAN タグが 0x9100 に設定されており、カスタム ethertype を使用してインターフェイスが 0x88a8 VLAN タグのパケットのみを受け入れるように設定されている場合は、このパケットが QinQ サブインターフェイス内でドロップされます。図 x-x は、QinQ のイーサネット フレーム形式を示しています。

インターフェイスの定義時に、access キーワードを使用して QinQ サブインターフェイスを作成することができます。次のコードは、access キーワードを使用してインターフェイスを定義し、VLAN QinQ サブインターフェイスを作成して、PPPoE セッションをイネーブルにする方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9100
Router(config-if)# interface gigabitethernet 1/0/0.100 access
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
Router(config-subif)# ip subscriber interface
```

制約事項と使用上のガイドライン

ES+ ラインカード上で IP セッションまたは PPPoE セッションを設定する場合は、次の制約事項と使用上のガイドラインに従ってください。

- IP セッションは、定義が曖昧な VLAN 上でサポートされません。
- Radius プロキシは、IP セッションに対してサポートされません。
- IP アドレスと MAC アドレスのなりすまし防止は、SIP400 ラインカード以外の ES+ ラインカード上のサブインターフェイスでサポートされません。
- IP セッションは、リンク アグリゲーション（Ether-Channel）インターフェイス上でサポートされます。LAG etherchannel インターフェイスは、1 つ以上のラインカード上のリンクに対してサポートされます。
- PPPoE セッションは、定義が曖昧な VLAN インターフェイスと VLAN 範囲でサポートされます。
- カスタム ethertype の不一致が原因でドロップされたパケット数をカウントするためのドロップ カウンタがありません。
- PPPoE セッションのセキュリティを強化するために、VLAN、送信元 MAC アドレス、およびポートがセッション ID と照合されます。

ES+ ラインカード上で 1:1 冗長性を設定する場合は、次の制約事項と使用上のガイドラインに従ってください。

- 加入者冗長性は、1:1 アクセス スタンバイ モデル上でしか使用することができません。
- ポート チャネル内でアクセス インターフェイスをサポートすることによって、ポート チャネル サブインターフェイス数を 4,001 以上にスケールします。
- LACP を使用すれば、GEC バンドル内のメンバー リンクを動的に処理することができます。
- 8 リンクで最大 64 の GEC バンドルをサポートします。
- 1 つの GEC バンドル内のメンバー リンクは複数の NP またはラインカードにわたって構築されます。
- LAG は複数のラインカード全体のメンバーでサポートされます。
- 複数のラインカード全体で LAG をサポートします。LAG のメンバーシップは新しいセッションが開始されても変化しません。
- この機能は、32,000 のアクセス サブインターフェイスと 8,000 のアクセス インターフェイスをサポートします。
- 1 つのセッションの全トラフィックが 1 つのポート上でリレーされる複数のメンバー リンク全体のセッション単位ロード バランシングをサポートします。

- メンバー リンクの追加または削除中のダウンタイムを短縮するために、ポート チャネルに属しているすべてのメンバー リンクに対して QOS クエリーが割り当てられます。入力トラフィックと出力トラフィックでメンバー リンクを変えることができますが、ピアは、1 つのメンバー リンクを通して 1 つのセッションの全トラフィックをリレーします。
- LAG は、非アクセス サブインターフェイス上のセッションをサポートすることによって、マルチキャスト ストリームの共存を可能にします。

検証

ここでは、設定情報を表示するためのコマンドについて説明します。

- PPPoE を設定するためのコマンド：

```
Router-DJ4-dfc9#sh debug
CWAN iEdge LC:
  CWAN iEdge LC session event debug debugging is on
X40G XLIF Client:
  XLIF NP events debugging is on

Router-DJ4-dfc9# sh log
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 308 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

Log Buffer (1000000 bytes):

Nov 19 16:08:48.247 IST: DFC9: provision_pppoe_routed_ac: switch_info 2CDEC4A4
seghandle 2CD93474 uid 40 if_number 80
Nov 19 16:08:48.247 IST: DFC9:  type 1 2 0opaque handle = 0x186DAB48
Nov 19 16:08:48.247 IST: DFC9: inserting 186DAB48 105 40
Nov 19 16:08:48.247 IST: DFC9: cwan_iedge_session_pending_timer started
Nov 19 16:08:48.247 IST: DFC9: no dbus vlan session pending on int 105
Nov 19 16:08:48.251 IST: DFC9:  cwan_iedge_update_dbus_vlan: Session 40 gets hidden
vlan 1020 through update for Virtual-Access2.1
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_common_session_notify: cfg_type 2 va_if_num
105 phy_if_num 80 uid 0action 0
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_session_config: sess_type 2 if_num 105
pid 0
Nov 19 16:08:50.247 IST: DFC9: cwan_iedge_get_pppoe_config: if_num 80 va_if_num 105
vlan 1020 sess-id 40 cond_debug off
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create Cfn[965F2BC] Creating Xlif:
GigabitEthernet9/5 Xid[0] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_create_internal successfully created
xlif: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_eg_xlif_update_port Cfn[92D1658] Xlif Update
Port 4 : GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352]
efp[0]
```

```
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_tag_rewrite Cfn[965F334] Tag(i-0,
o-2) Dir[2]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352]
efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_dbus_vlan Cfn[965F36C] Updatng
Dbus Vlan 1020: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_stats_id Cfn[965D780] Updatng
StatId 599056 Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_stats_id Cfn[965D8A8] Updatng
StatId 599064 Dir[1]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_fwd_feat_enable Cfn[965F3BC] Xlif Fwd
Feat 0x1 Enable 1 : GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_enable Cfn[965F3F0] Xlif Enable 1:
GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0] Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_feat_info Cfn[965F604] Xlif update
feature Dir[0]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]
Nov 19 16:08:50.247 IST: DFC9: x40g_npc_xlif_update_feat_info Cfn[965F700] Xlif update
feature Dir[1]: GigabitEthernet9/5 Xid[205352] Typ[4] Ch[0] Ifn[105] Xreg[0]
Xidx[205352] efp[0]

Router-DJ4#sh debug
PPP:
  PPP protocol negotiation debugging is on
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE control packets debugging is on

Router-DJ4#sh log
Syslog logging: enabled (3340 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 5280 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 203 message lines logged

Log Buffer (1000000 bytes):

Nov 19 16:08:48.231 IST: PPPoE 0: I PADI  R:bb00.1912.0001 L:ffff.ffff.ffff 2 Gi9/5.1
contiguous pak, size 60
 FF FF FF FF FF FF BB 00 19 12 00 01 81 00 00 02
 88 63 11 09 00 00 00 04 01 01 00 00 00 0A 03 06
 B6 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 06 F8 00 00 9C 88
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
Nov 19 16:08:48.231 IST: PPPoE 0: O PADO, R:a110.0050.0006 L:bb00.1912.0001 1019
Gi9/5.1
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
```

```
contiguous pak, size 100
 06 02 00 10 03 FB 28 00 03 80 00 00 44 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 02 04 00 00
 BB 00 19 12 00 01 A1 10 00 50 00 06 81 00 00 02
 88 63 11 07 00 00 00 24 01 01 00 00 01 02 00 08
 52 69 61 7A 2D 44 4A 34 ...
Nov 19 16:08:48.231 IST: PPPoE 0: I PADR  R:bb00.1912.0001 L:000c.31c9.7000 2 Gi9/5.1
contiguous pak, size 60
 00 0C 31 C9 70 00 BB 00 19 12 00 01 81 00 00 02
 88 63 11 19 00 00 00 18 01 01 00 00 01 04 00 10
 E2 DB 75 8D E5 9C 95 C1 83 35 DC 91 B2 14 32 89
 63 63 65 73 73 2D 70 70 6C 63 70 30
Nov 19 16:08:48.231 IST:  Service tag: NULL Tag
Nov 19 16:08:48.231 IST: PPPoE : encap string prepared
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Access IE handle allocated
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get retrieved attrs
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get nas port details
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA get dynamic attrs
Nov 19 16:08:48.231 IST: [40]PPPoE 40: AAA unique ID allocated
Nov 19 16:08:48.231 IST: [40]PPPoE 40: No AAA accounting method list
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Service request sent to SSS
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Created, Service: None R:000c.31c9.7000
L:bb00.1912.0001 2 Gi9/5.1
Nov 19 16:08:48.231 IST: [40]PPPoE 40: State NAS_PORT_POLICY_INQUIRY    Event SSS MORE
KEYS
Nov 19 16:08:48.231 IST: PPP: Alloc Context [19C03860]
Nov 19 16:08:48.231 IST: ppp40 PPP: Phase is ESTABLISHING
Nov 19 16:08:48.231 IST: [40]PPPoE 40: data path set to PPP
Nov 19 16:08:48.231 IST: [40]PPPoE 40: Segment (SSS class): PROVISION
Nov 19 16:08:48.231 IST: [40]PPPoE 40: State PROVISION_PPP    Event SSM PROVISIONED
Nov 19 16:08:48.231 IST: [40]PPPoE 40: O PADS  R:bb00.1912.0001 L:000c.31c9.7000 1019
Gi9/5.1
contiguous pak, size 100
 00 02 00 10 03 FB 28 00 03 80 00 00 44 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 02 04 00 00
 BB 00 19 12 00 01 A1 10 00 50 00 06 81 00 00 02
 88 63 11 65 00 28 00 18 01 01 00 00 01 04 00 10
 E2 DB 75 8D E5 9C 95 C1 ...
Nov 19 16:08:48.231 IST: ppp40 PPP: Using vpn set call direction
Nov 19 16:08:48.231 IST: ppp40 PPP: Treating connection as a callin
Nov 19 16:08:48.231 IST: ppp40 PPP: Session handle[28] Session id[40]
Nov 19 16:08:48.231 IST: ppp40 LCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.231 IST: ppp40 PPP LCP: Enter passive mode, state[Stopped]
Nov 19 16:08:48.231 IST: ppp40 LCP: I CONFREQ [Stopped] id 0 len 14
Nov 19 16:08:48.231 IST: ppp40 LCP:    MagicNumber 0xA4E30BAF (0x0506A4E30BAF)
Nov 19 16:08:48.231 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.231 IST: ppp40 LCP: O CONFREQ [Stopped] id 1 len 19
Nov 19 16:08:48.231 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.231 IST: ppp40 LCP:    AuthProto CHAP (0x0305C22305)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0x0F501712 (0x05060F501712)
Nov 19 16:08:48.235 IST: ppp40 LCP: O CONFACK [Stopped] id 0 len 14
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0xA4E30BAF (0x0506A4E30BAF)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.235 IST: ppp40 LCP: Event[Receive ConfReq+] State[Stopped to ACKsent]
Nov 19 16:08:48.235 IST: ppp40 LCP: I CONFACK [ACKsent] id 1 len 19
Nov 19 16:08:48.235 IST: ppp40 LCP:    MRU 1492 (0x010405D4)
Nov 19 16:08:48.235 IST: ppp40 LCP:    AuthProto CHAP (0x0305C22305)
Nov 19 16:08:48.235 IST: ppp40 LCP:    MagicNumber 0x0F501712 (0x05060F501712)
Nov 19 16:08:48.235 IST: ppp40 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, by this end
Nov 19 16:08:48.243 IST: ppp40 CHAP: O CHALLENGE id 1 len 29 from "Router-DJ4"
Nov 19 16:08:48.243 IST: ppp40 LCP: State is Open
Nov 19 16:08:48.243 IST: ppp40 CHAP: I RESPONSE id 1 len 29 from "PPP_USER"
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
```

```
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is AUTHENTICATING, Unauthenticated User
Nov 19 16:08:48.243 IST: ppp40 IPCP: Authorizing CP
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP stalled on event[Authorize CP]
Nov 19 16:08:48.243 IST: ppp40 IPCP: CP unstall
Nov 19 16:08:48.243 IST: ppp40 PPP: Phase is FORWARDING, Attempting Forward
Nov 19 16:08:48.243 IST: [40]PPPoE 40: State LCP_NEGOTIATION    Event SSS CONNECT
LOCAL
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): UPDATED
Nov 19 16:08:48.247 IST: [40]PPPoE 40: Segment (SSS class): BOUND
Nov 19 16:08:48.247 IST: [40]PPPoE 40: data path set to Virtual Acess
Nov 19 16:08:48.247 IST: [40]PPPoE 40: State LCP_NEGOTIATION    Event SSM UPDATED
Nov 19 16:08:48.247 IST: Vi2.1 PPP: Phase is AUTHENTICATING, Authenticated User
Nov 19 16:08:48.247 IST: Vi2.1 CHAP: O SUCCESS id 1 len 4
Nov 19 16:08:48.247 IST: [40]PPPoE 40: AAA get dynamic attrs
Nov 19 16:08:48.247 IST: Vi2.1 PPP: Phase is UP
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Protocol configured, start CP. state[Initial]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFREQ [Starting] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[UP] State[Starting to REQsent]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFREQ [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 0.0.0.0 (0x030600000000)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Start.  Her address 0.0.0.0, we want
0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP AUTHOR: Done.  Her address 0.0.0.0, we want
0.0.0.0
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Pool returned 182.0.0.1
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: O CONFNAK [REQsent] id 0 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[Receive ConfReq-] State[REQsent to REQsent]
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: I CONFACK [REQsent] id 1 len 10
Nov 19 16:08:48.247 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.247 IST: Vi2.1 IPCP: Event[Receive ConfAck] State[REQsent to ACKrcvd]
Nov 19 16:08:48.251 IST: [40]PPPoE 40: State PTA_BINDING    Event STATIC BIND RESPONSE
Nov 19 16:08:48.251 IST: [40]PPPoE 40: Connected PTA
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: I CONFREQ [ACKrcvd] id 1 len 10
Nov 19 16:08:48.251 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: O CONFACK [ACKrcvd] id 1 len 10
Nov 19 16:08:48.251 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.251 IST: Vi2.1 IPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[DOWN] State[Open to Starting]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[CLOSE] State[Starting to Initial]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[OPEN] State[Initial to Starting]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: O CONFREQ [Starting] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[UP] State[Starting to REQsent]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: I CONFREQ [REQsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Start.  Her address 182.0.0.1, we want
182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Reject 182.0.0.1, using 182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP AUTHOR: Done.  Her address 182.0.0.1, we want
182.0.0.1
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: O CONFACK [REQsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 182.0.0.1 (0x0306B6000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: I CONFACK [ACKsent] id 2 len 10
Nov 19 16:08:48.255 IST: Vi2.1 IPCP:    Address 100.0.0.1 (0x030664000001)
Nov 19 16:08:48.255 IST: Vi2.1 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: State is Open (Indicates that the PPPoE session
is up)
Nov 19 16:08:48.275 IST: Vi2.1 Added to neighbor route AVL tree: topoid 0, address
182.0.0.1
Nov 19 16:08:48.275 IST: Vi2.1 IPCP: Install route to 182.0.0.1
```

```
Router-DJ4#

interface GigabitEthernet9/17.1
 encapsulation dot1Q 2000
 ip address 180.0.0.1 255.255.255.0

interface GigabitEthernet9/5.1
 encapsulation dot1Q 2
 ip address 192.0.0.1 255.255.255.0
 pppoe enable group dj4_bba_group1

aaa new-model
aaa authentication login default group radius local
aaa authentication ppp default local
aaa authorization network default local
aaa authorization subscriber-service default group radius
aaa session-id common

bba-group pppoe dj4_bba_group1
 virtual-template 1
 sessions per-vc limit 16000
 sessions per-mac limit 16000
 sessions per-vlan limit 8000

interface Loopback1
 ip address 100.0.0.1 255.255.255.255

interface Virtual-Template1
 ip unnumbered Loopback1
 no logging event link-status
 peer default ip address pool PPPPool_1
 no snmp trap link-status
 keepalive 300
 ppp authentication chap
```

Use the following commands to verify the PPPoE session:

```
Router-DJ4#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                               1       1       0       0
GigabitEthernet9/5                  1       1       0       0
Router-DJ4#sh pppoe ses
Router-DJ4#sh pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                    VA-st      Type
     42     42  bb00.1912.0001  Gi9/5.1                  1  Vi2.1      PTA
                000c.31c9.7000  VLAN:   2                   UP
Router-DJ4#sh sss session uid 42 detailed
Unique Session ID: 42
Identifier: PPP_USER
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:19:04, Last Changed: 00:19:04
Interface: Virtual-Access2.1

Policy information:
  Context 137426FC: Handle 2400002A
```

```
  AAA_id 00000038: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "PPP_USER"
  Downloaded User profile, including services:
    Framed-Protocol      1 [PPP]
    username             "PPP_USER"
  Config history for session (recent to oldest):
    Access-type: PPP Client: SM
     Policy event: Process Config Connecting
      Profile name: apply-config-only, 2 references
        Framed-Protocol      1 [PPP]
        username             "PPP_USER"
  Rules, actions and conditions executed:
    subscriber rule-map PPPoE-SUB
      condition always event session-start
        1 service local

Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:19:04

Router-DJ4# sh pppoe session packets
Total PPPoE sessions 1


SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
42      12              13              184             190
Router-DJ4#

Router-DJ4#sh cef int gig 9/5.1
GigabitEthernet9/5.1 is up (if_number 80)
  Corresponding hwidb fast_if_number 80
  Corresponding hwidb firstsw->if_number 25
  Internet address is 192.0.0.1/24
  ICMP redirects are always sent
  IP unicast RPF check is disabled
  Output features: MFIB Adjacency, HW Shortcut Installation
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is GigabitEthernet9/5
  Fast switching type 28, interface type 146
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP prefix lookup IPv4 mtrie generic
  Input fast flags 0x40000000, Output fast flags 0x0
  ifindex 24(24)
  Slot 9/0 (9) Slot unit 5 VC -1
  IP MTU 1500
```

- IP セッションを設定するためのコマンド：

```
aaa new-model
!
aaa session-id common
!
interface GigabitEthernet2/9
 no ip address
 load-interval 30
!
interface GigabitEthernet2/9.1 access
 encapsulation dot1Q 2 second-dot1q 2
```

```
 ip address 182.0.0.1 255.255.255.0
 ip subscriber routed
  initiator unclassified ip-address
!
interface GigabitEthernet2/10
 no ip address
 load-interval 30
!
interface GigabitEthernet2/10.1
 encapsulation dot1Q 2000 second-dot1q 2001
 ip address 180.0.0.1 255.255.255.0
!
no ip http server
no ip http secure-server
!
arp 182.0.0.2 aa00.0000.0001 ARPA
arp 180.0.0.2 0000.0000.0001 ARPA
!
```

IP セッションをデバッグするためのコマンド：

```
ISG_NMB#sh deb
CWAN iEdge RP:
  CWAN iEdge RP debug debugging is on

IP Subscriber:
  all IP subscriber debugs debugging is on
ISG_NMB#
Nov 19 16:02:46.087 IST: IPSUB_DP: [Gi2/9.1:I:CEF:DFL:21.0.0.1] Packet triggers
session initiation
Nov 19 16:02:46.087 IST: IPSUB_DP: [Gi2/9.1:I:CEF:DFL:21.0.0.1] Packet classified,
results = 0x1
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Insert new entry for mac 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Processing new in-band session request
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Delete mac entry 0000.1500.0001
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] In-band session request event for session
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Added upstream entry into the classifier
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] VRF = DFL, IP = 21.0.0.1, MASK =
255.255.255.255
Nov 19 16:02:46.087 IST: IPSUB: Try to create a new session
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: Check IP DHCP session recovery: 21.0.0.1
Gi2/9.1 mac aa00.0000.0001
Nov 19 16:02:46.087 IST: IPSUB: IPSUB: No DHCP binding found
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] IPSUB: Proceed to create the IP inband session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Session start event for session
Nov 19 16:02:46.087 IST: IPSUB: [uid:0] Event session start, state changed from idle
to requesting
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Session init-notification on Active
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Allocated SHDB handle (0xF1000020)
Nov 19 16:02:46.087 IST: IPSUB: HA[uid:32]: Successfully initialized for HA
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] AAA unique ID allocated
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Added session 21.0.0.1 to L3 session table
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Added session to session table with access
session keys
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] IP session(0x63000020) to be associated to
Gi2/9.1
Nov 19 16:02:46.087 IST: IPSUB: [uid:32] Inserted IP session(0x63000020) to
sessions-per-interface db with interface Gi2/9.1
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Sent message to control plane for in-band
session creation
Nov 19 16:02:46.087 IST: IPSUB_DP: [uid:0] Event inband-session, state changed from
idle to intiated
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Recieved Message = connect local
```

```
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Connect Local event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event connect local, state changed from
requesting to waiting
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Inside processing IPSIP info
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Checking whether routes to be
inserted/removed
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Context not present, creating context
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Entered the sg subrte context alloc
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Returning the sg subrte context
0x1348DD20
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Added Fib Prefix [DFL]:
21.0.0.1/255.255.255.255
Nov 19 16:02:46.091 IST: IPSUB-ROUTE: [uid:32] Both IP addresses and VRF are same, no
need to add route
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Keys not changed, seg needn't be updated
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Key list to be created to update SM
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Created key list to update SM
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Session Keys Available event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event session keys available, state changed
from waiting to provisioning
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Access and service keys same, no need to add
session with service keys
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Data plane prov successful event for session
Nov 19 16:02:46.091 IST: IPSUB: [uid:32] Event dataplane prov successful, state
changed from provisioning to connected
Nov 19 16:02:46.091 IST: IPSUB: HA[uid:32]: Session up notification
Nov 19 16:02:46.091 IST: IPSUB: HA[uid:32]: Session ready to sync data (0xF1000020)
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:0] Setup event for session (session hdl
3858759691)
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Added downstream entry into the classifier
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] VRF = DFL, IP = 21.0.0.1, MASK =
255.255.255.255
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Session setup successful
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Event setup-session, state changed from
intiated to established
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Activate event for session
Nov 19 16:02:46.091 IST: IPSUB_DP: [uid:32] Event activate-session, state changed from
established to connected
```

IP セッションを確認するためのコマンド：

```
ISG_NMB#sh ip sub
Displaying subscribers in the default service vrf:

Type        Subscriber Identifier    Display UID    Status
---------   ----------------------   ------------   ------
routed      21.0.0.1/32              [32]           up
ISG_NMB#
ISG_NMB#sh sss sess
Current Subscriber Information: Total sessions 1

Uniq ID Interface    State         Service      Identifier           Up-time
32      IP           unauthen      Local Term   21.0.0.1             00:02:40

ISG_NMB#sh sss sess uid 32
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:46, Last Changed: 00:02:46

Policy information:
  Authentication status: unauthen
```

```
Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:46

ISG_NMB#sh sss sess uid 32 de
ISG_NMB#sh sss sess uid 32 detailed
Unique Session ID: 32
Identifier: 21.0.0.1
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:49, Last Changed: 00:02:49

Policy information:
  Context 133B22FC: Handle DF000020
  AAA_id 00000030: Flow_handle 0
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:02:49
```

次の詳細は、Dot1Q インターフェイス上の L2 接続の DHCP セッション用です。

```
==========================================================================
```

L2 接続の DHCP セッションを設定するためのコマンド :

```
aaa new-model
!
!
aaa session-id common
!
!
!
clock timezone IST 5
ip source-route
!
!
ip dhcp excluded-address 182.0.0.11 182.0.0.15
no ip dhcp ping packets
!
ip dhcp pool pool_global1
   network 182.0.0.0 255.255.255.240
   lease 0 0 3
   update arp
!
!
!
interface Loopback10
 ip address 182.0.0.11 255.255.255.255
!
!
interface GigabitEthernet2/9
 no ip address
 load-interval 30
!
interface GigabitEthernet2/9.1 access
 encapsulation dot1Q 2
 ip unnumbered Loopback10
 ip subscriber l2-connected
  initiator dhcp class-aware
!
interface GigabitEthernet2/10
 no ip address
 load-interval 30
!
```

```
interface GigabitEthernet2/10.1
 encapsulation dot1Q 2000
 ip address 180.0.0.1 255.255.255.0
!
!
no ip http server
no ip http secure-server
ip route 7.0.0.0 255.0.0.0 7.38.0.1
ip route 202.153.0.0 255.255.0.0 7.38.0.1
!
!
```

L2 接続の DHCP セッションをデバッグするためのコマンド：

```
ISG_NMB#sh deb
DHCP server packet debugging is on.
DHCP server event debugging is on.

IP Subscriber:
  IP subscriber events debugging is on
  IP subscriber errors debugging is on
  IP subscriber packets debugging is on


ISG_NMB#
Nov 19 15:40:33.595 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Packet classified,
results = 0x40
Nov 19 15:40:33.595 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Rx driver allowing
IP routing
Nov 19 15:40:33.595 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.595 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.595 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.595 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.595 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.595 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.595 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.595 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.595 IST: IPSUB: Create session keys from SSS key list
Nov 19 15:40:33.595 IST: IPSUB: Mac_addr = aa00.1314.0001, Recvd Macaddr =
aa00.1314.0001
Nov 19 15:40:33.599 IST: IPSUB: Session input interface(0x13348754) =
GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST: IPSUB: SHDB Handle = 5A00000B
Nov 19 15:40:33.599 IST: IPSUB: Remote_id = 020a0000b600000b21010002
Nov 19 15:40:33.599 IST: IPSUB: Vendor_Class_id = Ixia
Nov 19 15:40:33.599 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.599 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.599 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.599 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.599 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.599 IST: DHCPD: Saving workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: New packet workspace 0x1333D0D8 (ID=0x2700000C)
Nov 19 15:40:33.599 IST: IPSUB: Try to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Request to create a new session
Nov 19 15:40:33.599 IST: IPSUB: [uid:0] Session start event for session
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] AAA unique ID allocated
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session aa00.1314.0001 to L2 session
table
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Added session to session table with access
session keys
```

```
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session(0xC500000B) to be associated to
Gi2/9.1
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Inserted IP session(0xC500000B) to
sessions-per-interface db with interface Gi2/9.1
Nov 19 15:40:33.599 IST: DHCPD: Callback for workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: No authentication required. Continue
Nov 19 15:40:33.599 IST: DHCPD: Callback: class '' now specified for client
01aa.0013.1400.01
Nov 19 15:40:33.599 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.599 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.599 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.599 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.599 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.599 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.599 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.599 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.599 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to radix tree (182.0.0.1)
Nov 19 15:40:33.599 IST: DHCPD: Adding binding to hash tree
Nov 19 15:40:33.599 IST: DHCPD: assigned IP address 182.0.0.1 to client
01aa.0013.1400.01. (13 1)
Nov 19 15:40:33.599 IST: DHCPD: DHCPOFFER notify setup address 182.0.0.1 mask
255.255.255.240
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IP session context 0x133D28C8 available to
authorize
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Entered allocate feature info
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Allocated sg vrfset info 0x13488EE0
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Freeing the sg vrfset info 0x13488EE0
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] IPSIP Parsing HostIP: 182.0.0.1 SubnetMask=
255.255.255.255
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Recieved Message = connect local
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Connect Local event for session
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Inside processing IPSIP info
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Processing IPSIP info: 0x1330208C (APPLY)
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Got IP address- IP:-182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Set IP address- IP:-182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] Applying SG VRFSET info
Nov 19 15:40:33.599 IST: IPSUB-VRFSET: [uid:11] DHCP Initiated session, no config,
ignore
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be
inserted/removed
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Context not present, creating context
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Entered the sg subrte context alloc
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Returning the sg subrte context
0x1348DD04
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Installed ARP entry [DFL]: 182.0.0.1
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Added Fib Prefix [DFL]:
182.0.0.1/255.255.255.255
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Route insert not required for DHCP
hosts with IP unnumbered config on: GigabitEthernet2/9.1
Nov 19 15:40:33.599 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no
need to add route
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found that seg to be updated with new session
keys
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11]   Update IP-Address-VRF key: 182.0.0.1:0
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Found address change to be notified
Nov 19 15:40:33.599 IST: IPSUB: [uid:11] Session Keys Available event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session 182.0.0.1 to L3 session table
```

```
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Added session to session table with service
session keys
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Recieved Message = update SIP config
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Config Update event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Inside processing IPSIP info
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Checking whether routes to be
inserted/removed
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Ctx present, No config change, Nothing
to be done
Nov 19 15:40:33.603 IST: IPSUB-ROUTE: [uid:11] Both IP addresses and VRF are same, no
need to add route
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Keys not changed, seg needn't be updated
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Key list to be created to update SM
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Created key list to update SM
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Data plane prov successful event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Notifying about address change: 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: Callback for workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: DHCPD: Callback: switching path now setup for client
01aa.0013.1400.01
Nov 19 15:40:33.603 IST: DHCPD: Reprocessing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: DHCPD: Sending notification of DISCOVER:
Nov 19 15:40:33.603 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
Nov 19 15:40:33.603 IST:   DHCPD: remote id 020a0000b600000b21010002
Nov 19 15:40:33.603 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST:   DHCPD: class id 49786961
Nov 19 15:40:33.603 IST: DHCPD: DHCPDISCOVER received from client 01aa.0013.1400.01 on
interface GigabitEthernet2/9.1.
Nov 19 15:40:33.603 IST: DHCPD: Found previous server binding
Nov 19 15:40:33.603 IST: DHCPD: Sending DHCPOFFER to client 01aa.0013.1400.01
(182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: ARP entry exists (182.0.0.1, aa00.1314.0001).
Nov 19 15:40:33.603 IST: DHCPD: unicasting BOOTREPLY to client aa00.1314.0001
(182.0.0.1).
Nov 19 15:40:33.603 IST: DHCPD: unicast BOOTREPLY output i/f override
GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:O:PROC:DFL:182.0.0.1] Packet classified,
results = 0x0
Nov 19 15:40:33.603 IST: DHCPD: removing ARP entry (182.0.0.1 vrf default).
Nov 19 15:40:33.603 IST: DHCPD: Freeing saved workspace (ID=0x8900000B)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Setup event for session (session hdl 0)
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Insert new entry for mac aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Added upstream entry into the classifier
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] MAC = aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Added downstream entry into the classifier
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] VRF = DFL, IP = 182.0.0.1, MASK =
255.255.255.255
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Session setup successful
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Sent update msg to the control plane
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:11] Activate event for session
Nov 19 15:40:33.603 IST: IPSUB: [uid:11] Data plane prov successful event for session
Nov 19 15:40:33.603 IST: IPSUB_DP: [uid:0] Found mac entry aa00.1314.0001
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Packet classified,
results = 0x40
Nov 19 15:40:33.603 IST: IPSUB_DP: [Gi2/9.1:I:PROC:aa00.1314.0001] Rx driver allowing
IP routing
Nov 19 15:40:33.603 IST: DHCPD: input i/f override GigabitEthernet2/9.1 for client
Nov 19 15:40:33.603 IST: DHCPD: Reload workspace interface GigabitEthernet2/9.1
tableid 0.
Nov 19 15:40:33.603 IST: DHCPD: tableid for 182.0.0.11 on GigabitEthernet2/9.1 is 0
Nov 19 15:40:33.603 IST: DHCPD: client's VPN is .
Nov 19 15:40:33.603 IST: DHCPD: DHCPREQUEST received from client 01aa.0013.1400.01.
Nov 19 15:40:33.603 IST: DHCPD: Sending notification of ASSIGNMENT:
Nov 19 15:40:33.603 IST:  DHCPD: address 182.0.0.1 mask 255.255.255.240
Nov 19 15:40:33.603 IST:   DHCPD: htype 1 chaddr aa00.1314.0001
```

```
Nov 19 15:40:33.603 IST:   DHCPD: lease time remaining (secs) = 180
Nov 19 15:40:33.603 IST:   DHCPD: interface = GigabitEthernet2/9.1
Nov 19 15:40:33.603 IST: DHCPD: Sending DHCPACK to client 01aa.0013.1400.01
(182.0.0.1).
Nov 19 15:40:33.603 IST:  DHCPD: lease time = 180
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_lookup_route: host = 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_lookup_route: index = 183
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_create_and_hash_route: host = 182.0.0.1
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_create_and_hash_route index = 183
Nov 19 15:40:33.603 IST: DHCPD: dhcpd_add_route: lease = 180
Nov 19 15:40:33.607 IST: DHCPD: ARP entry exists (182.0.0.1, aa00.1314.0001).
Nov 19 15:40:33.607 IST: DHCPD: Changing arp entry 182.0.0.1 to secure arp entry
Nov 19 15:40:33.607 IST: DHCPD: Failed to secure arp entry 182.0.0.1
Nov 19 15:40:33.607 IST: DHCPD: unicasting BOOTREPLY to client aa00.1314.0001
(182.0.0.1).
Nov 19 15:40:33.607 IST: DHCPD: unicast BOOTREPLY output i/f override
GigabitEthernet2/9.1
Nov 19 15:40:33.607 IST: IPSUB_DP: [Gi2/9.1:O:PROC:DFL:182.0.0.1] Packet classified,
results = 0x10
```

L2 接続の DHCP セッションを確認するためのコマンド：

```
ISG_NMB#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
182.0.0.1           01aa.0013.1400.01       Nov 19 2009 03:45 PM    Automatic

ISG_NMB#sh sss session
Current Subscriber Information: Total sessions 1

Uniq ID Interface    State         Service      Identifier           Up-time
11      IP           unauthen      Local Term   aa00.1314.0001       00:00:58

ISG_NMB#sh sss session uid 11
Unique Session ID: 11
Identifier: aa00.1314.0001
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:04, Last Changed: 00:01:04

Policy information:
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:01:04

ISG_NMB#sh sss session uid 11 de
Unique Session ID: 11
Identifier: aa00.1314.0001
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:07, Last Changed: 00:01:07

Policy information:
  Context 133B2154: Handle 9000000B
  AAA_id 00000017: Flow_handle 0
  Authentication status: unauthen

Configuration sources associated with this session:
Interface: GigabitEthernet2/9.1, Active Time = 00:01:07
```

QoS に関する推奨事項

IP Subscriber Awareness over Ethernet 機能と併用できるよう Cisco 7600 SIP-400 で QoS 機能を設定する場合、次に示す設定時の注意事項および推奨事項に注意してください。

- Cisco 7600 SIP-400 のスループットは 5.1 ～ 5.6 ギガビット Gbps です。カードのオーバーサブスクライブが 8 Gbps を超えないことを推奨します。この制限を超えると、予期しないカードの動作が発生します （CSCsg67629）。
- オーバーサブスクライブがサポートされるのは、5 ポート ギガビット イーサネット SPA（SPA-5X1GE-V2）だけです。

出力オーバーサブスクライブ

- ハイ プライオリティ トラフィック（通常は音声およびビデオ）の IP precedence 値は、5、6、または 7 であることが必要です。
- IP precedence 値が 0、1、2、3、または 4 の場合、トラフィックが QoS ポリシーでプライオリティ トラフィックとして分類されていても、オーバーサブスクライブ発生時に廃棄されます（CSCsg67721）。

（注） パケットの IP precedence 値および VLAN ユーザ プライオリティ値を一致させることを強くお勧めします。入力オーバーサブスクライブが発生した場合、IP precedence 値および VLAN ユーザ プライオリティ値が一致していないプライオリティ トラフィックは、SPA レベルで廃棄される可能性があります （CSCsg97434）。

入力オーバーサブスクライブ

- ハイ プライオリティ トラフィック（通常は音声）の VLAN ユーザ プライオリティ値は 5、6、または 7 であることが必要です。プライオリティ値が 0、1、2、3、または 4 の場合、トラフィックが QoS ポリシーでプライオリティ トラフィックとして分類されていても、オーバーサブスクライブ発生時に廃棄されます （CSCsg97434、CSCsg67721）。

QoS カウンタの更新

- 各 IP 加入者セッションの統計情報を取得するには、**show policy-map interface** コマンドを 2 回または 3 回実行します。このコマンドの初回実行時はカウンタに既存の値が保持されるため、この操作は必要です。
- **show policy-map interface** コマンドを実行して、インターフェイスを指定しなかった場合、ルータはすべてのセッション カウンタを更新します。加入者が 32000 の場合、更新には最大 30 分かかることがあります。

帯域幅余剰比率に関する推奨事項

Bandwidth-Remaining Ratio（BRR; 帯域幅余剰比率）機能（「残りの帯域幅使用比率の分配」とも呼ばれる）を使用して、サービス プロバイダーは輻輳時に加入者のトラフィックの優先順位を設定できます。この機能を使用して、サブインターフェイスまたはクラス キューの他のサブインターフェイスまたはクラス キューに対する相対的重みを指定できます。輻輳時に、ルータは帯域幅余剰比率を使用してサブインターフェイスおよびクラス キュー上でまだ認定されていない帯域幅のスケジューリングを最適化します。BRR を使用しない場合、物理インターフェイス上で未割り当ての帯域幅はすべてのキューで均等に分配されます。この機能の概要については、次の URL の機能説明を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/bwratio.htm

ここでは、IP Subscriber Awareness over Ethernet をサポートするため Cisco 7600 SIP-400 で BRR を設定する際の推奨事項と注意事項を示します。ここで説明する内容は、次のとおりです。

- BRR 設定時の注意事項
- BRR の設定方法

BRR 設定時の注意事項

BRR 機能を設定する際は、次に示す Cisco 7600 固有のガイドラインと考慮事項に従ってください。

- 2 ポートおよび 5 ポート ギガビット イーサネット（GE）SPA を備えた Cisco 7600 SIP-400 でのみサポート。
- GE インターフェイス上だけで使用可能（この機能が GE SPA 上だけでサポートされるため）。
- RSP720、Sup720、または Sup32 が必要。
- 2 つのサブインターフェイスの帯域幅余剰比率が大きく異なる場合（1000 対 1 など）は、比率の低い方のサブインターフェイスの子のデフォルト クラスにキュー下限値（2 ～ 50）を設定します。キュー下限値が設定されていない場合、デフォルトの queue-limit 値によりバッファに入れられているパケットはトラフィックの停止後通過が許可されるため、帯域幅余剰比率に大幅に影響を与えます。低いキュー制限値を設定することで、トラフィック停止後でも比率が確実に維持されます。

（注）　BRR とプライオリティ レート伝播を併用することを推奨します。詳細については、「プライオリティ レート伝播に関する推奨事項」（P.24-26）を参照してください。

BRR の設定方法

Cisco 7600 SIP-400 で加入者（アクセス）インターフェイスに BRR を定義する QoS ポリシーの設定に必要な手順の概要を次に示します。詳しい手順は、以降の表に示します。

（注）　コマンドラインには BRR の設定に必要な引数とキーワードだけが含まれます。

1. **enable**
2. **configure terminal**
3. **qos scheduler priority-rate-propagation platform sip-400**（省略可能だが推奨）
4. **policy-map *child-policy-name***
5. **class** *class-map-name*
6. **priority level** *level*（省略可能だが推奨）
7. **police** *bps*
8. exit
9. exit
10. **policy-map *parent-policy-name***
11. **class class-default**
12. **bandwidth remaining ratio** *ratio*
13. **shape average *cir*** [*bc*] [*be*]
14. **service-policy** *child-policy-name*

15. exit
16. exit
17. **interface** *type slot/module/port.subinterface* **access**
18. **service-policy output** ***parent-policy-name***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**qos scheduler priority-rate-propagation platform sip-400** **例：** `Router(config)# qos scheduler priority-rate-propagation platform sip-400`	Cisco 7600 SIP-400 でプライオリティ レート伝播機能をイネーブルにします。この機能により、キュー階層内のすべてのより高いレベルのキューが最低レートまたはプライオリティに設定されていない場合であっても、それらのキューにプライオリティ トラフィック向けのプライオリティ レベルとトラフィック レートが適用されます。 **（注）** この手順は省略可能ですが、BRR を使用する場合は、この手順を実行することを推奨します。
ステップ 4	**policy-map** *child-policy-name* **例：** `Router(config)# policy-map child`	子ポリシー マップを作成または変更して、ポリシーマップ コンフィギュレーション モードを開始します。 • *child-policy-name* は、子ポリシー マップの名前です。
ステップ 5	**class** *class-map-name* **例：** `Router(config-pmap)# class precedence_0`	指定したクラス マップを設定します。ポリシーマップ クラス コンフィギュレーション モードを開始します。 • *class-map-name* は前回作成したクラス マップの名前です。
ステップ 6	**priority level** *level* **例：** `Router(config-pmap-c)# priority level 1`	このトラフィック クラスにプライオリティ レベルを指定します。 • *level* は指定するプライオリティ レベルです。有効値は 1（ハイ）および 2（ロー）です。 **（注）** 同じポリシー マップ内の異なる 2 つのクラスに同じプライオリティ レベルを指定しないでください。
ステップ 7	police *bps* **例：** `Router(config-pmap-c)# police 200000000`	（任意）このトラフィック クラスに属するトラフィックのポリシングを行うレートを指定します。 • *bps* には平均レートをビット/秒（bps）で指定します。有効値は 8,000 ～ 2,488,320,000 bps です。
ステップ 8	exit	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。
ステップ 9	exit	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 10	**policy-map** *parent-policy-name* **例：** `Router(config)# policy-map Parent`	親ポリシー マップを作成または変更します。ポリシーマップ コンフィギュレーション モードを開始します。 • *parent-policy-name* は、親ポリシー マップの名前です。

	コマンドまたはアクション	目的
ステップ 11	**class class-default** **例：** `Router(config-pmap)# class class-default`	class-default クラスを設定します。ポリシーマップ クラス コンフィギュレーション モードを開始します。 **（注）** ルータは、サブインターフェイスの集約機能として class-default クラスで設定された任意の機能を解釈します。
ステップ 12	**bandwidth remaining ratio** *ratio* **例：** `Router(config-pmap-c)# bandwidth remaining ratio 10`	サブインターフェイスの帯域幅余剰比率を指定します。他のサブインターフェイスに対して超過している帯域幅がスケジューラにより割り当てられます。 • *ratio* は、輻輳時にサブインストールの各キューに割り当てるための未使用帯域幅の量を決定する際に使用する値です。有効値は 1 ～ 1000 です。デフォルト値および最小値は 1 です。 **（注）** CLI は 1 ～ 65535 の *ratio* 値をサポートしますが、1000 を超える BRR 値が設定されたポリシーは Cisco 7600 SIP-400 インターフェイスに適用できません。
ステップ 13	**shape average** *cir* [*bc*] [*be*] **例：** `Router(config-pmap-c)# shape average 100000000`	（任意）平均レートを指定されたレートにシェーピングします。 • **average** で平均レート シェーピングを指定します。 • *cir* は committed information rate（CIR; 認定情報レート）を bps で指定します。 • （任意）*bc* は認定バースト サイズをビットで指定します。 • （任意）*bc* は超過バースト サイズをビットで指定します。
ステップ 14	**service-policy** *child-policy-name* **例：** `Router(config-pmap-c)# service-policy child`	指定された子ポリシー マップを、親ポリシー マップのデフォルト トラフィック クラスに適用します。ルータは、子ポリシー マップで指定された QoS アクションをトラフィック クラスに適用します。 • *child-policy-name* は、子ポリシーの名前です。 **（注）** 子ポリシーを親ポリシーに適用する際は、**input** または **output** キーワードを含めないでください。 **（注）** サブインターフェイスでは、子ポリシーは親のデフォルト トラフィック クラスにだけ適用できます。
ステップ 15	`exit`	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。
ステップ 16	`exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 17	**interface** *type slot*/*module*/*port.subinterface* **access** **例：** `Router(config)# interface GigabitEthernet 1/0/0.1 access`	指定されたアクセス サブインターフェイスを作成または変更します。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。 • *type* はインターフェイスのタイプ（ギガビット イーサネットなど）です。 • *slot/module/port.subinterface* はサブインターフェイスを識別します（1/0/0.1 など）。 • **access** はこれを IP 加入者インターフェイスとして識別します。
ステップ 18	**service-policy output** *parent-policy-name* **例：** `Router(config-subif)# service-policy output parent`	親ポリシーをサブインターフェイスに適用します。 • **output** はサービス ポリシーをアウトバウンド トラフィックに適用します。 • *parent-policy-name* は、親ポリシーの名前です。 **（注）** BRR が設定されたポリシー マップは出力方向だけに使用できます。 ルータはサブインターフェイス トラフィックを、親の class-default クラスで指定されたシェーピング レートに合わせてシェーピングし、子ポリシーで指定された QoS アクションをトラフィック クラスに一致するトラフィックに適用します。 輻輳時は、ルータは親ポリシー マップで指定された帯域幅余剰比率を使用して、他のサブインターフェイスを基準としてこのサブインターフェイス上で未使用の帯域幅を割り当てます。

プライオリティ レート伝播に関する推奨事項

プライオリティ レート伝播は、上層のキューが最低のレートまたはプライオリティに設定されていない場合であっても、下位レベルのキューからキュー階層内のすべての上層のキューにプライオリティ レベルとトラフィック レートを適用（伝播）します。たとえば、子ポリシー内のトラフィック クラス（ビデオなど）にプライオリティ レベルとトラフィック レートを設定する場合、プライオリティ レート伝播を使用して、すべてのキュー レベル（親キュー、サブインターフェイス キュー、およびインターフェイス キュー）のビデオ トラフィックに目的のレートを適用できます。

デュアルプライオリティ キューを使用して、単一のポリシー マップで 2 つのクラスのハイ プライオリティ トラフィックを定義できます。また **priority level** コマンドを使用して、各プライオリティ キューにプライオリティ（ハイまたはロー）を指定できます。**priority level** コマンドにより、トラフィックのクラスが他のクラスに関して遅延要件を持つよう指定します。現在、ルータは 2 つのプライオリティ レベル 1（ハイ）と 2（ロー）をサポートしています。ルータは、ロー プライオリティ レベルのトラフィックよりも前に、ハイ プライオリティ レベルのトラフィックをアウトバウンド リンクに配置します。したがって、ハイ プライオリティ パケットはロー プライオリティ パケットより遅れることはありません。

ルータは 1 つのプライオリティ キューを各プライオリティ レベルに関連付け、高レベルのプライオリティ キューのサービスをキューが空になるまで行ってから、次のレベルのプライオリティ キューおよびプライオリティのないキューのサービスを行います。ルータがキューのサービスを行う間、サービス レートはできる限り速くなり、基礎となるリンクのレートまたは階層内の親ノードによってだけ抑制さ

れます。レートが設定されていて、トラフィック ストリームが設定されているレートを超過したとルータが判断した場合、ルータは輻輳時に超過したパケットを廃棄します。リンクが現在輻輳していない場合、ルータは超過したパケットをアウトバウンド リンクに配置します。

Bandwidth Remaining Ratio（BRR; 帯域幅余剰比率）も設定されている場合、ルータはプライオリティ トラフィックのサービスを最初に行います。プライオリティ トラフィックの帯域幅のサービスを行った後、ルータは、設定されている帯域幅余剰比率に基づいて、論理キューに未使用の帯域幅を割り当てます。このデフォルトのケースでは、3 つのレベルのスケジューラが未使用の帯域幅を各論理キューに均等に割り当てます。

高プライオリティ トラフィックのポリシングが適切でない場合、低プライオリティの帯域幅不足が発生する可能性があります。したがって、必須ではありませんが、**police** コマンドを使用して高プライオリティ トラフィックのポリサーを設定することをお勧めします。プライオリティ キューに **police** コマンドを設定した場合、各プライオリティ キューのポリシー レートに合わせてトラフィック レートをポリシングされます。

プライオリティ レート伝播設定時の注意事項

プライオリティ レート伝播を BRR と併用できるよう設定する際は、次の注意事項に従ってください。

- プライオリティ レート伝播機能をイネーブル/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 **[no] qos scheduler priority-rate-propagation platform sip400** コマンドを使用します。
- **[no] qos scheduler priority-rate-propagation platform sip400** コマンドは、インターフェイスに付加されている QoS ポリシーには影響を与えません。したがって、QoS ポリシーを付加する前にこのコマンドを実行することを推奨します。

（注）　QoS ポリシーを Cisco 7600 SIP-400 インターフェイスに付加した後で **[no] qos scheduler priority-rate-propagation platform sip400** コマンドを実行した場合、コマンドを有効にするには、設定を保存してルータをリロードする必要があります。

- プライオリティ レート伝播と BRR は次のように連動して機能します。
  - プライオリティ レート伝播がイネーブルの場合、ルータはすべてのサブインターフェイス ポリシーについてプライオリティ帯域幅のサービスを行います。残りの帯域幅は、帯域幅余剰比率に応じて分配されます。このシナリオでは、プライオリティ レートは子レベルからインターフェイス キューへ伝播されています。
  - プライオリティ レート伝播がディセーブルの場合、集約サブインターフェイスの帯域幅（プライオリティおよびベスト エフォート型）は帯域幅余剰比率に応じて共有されます。このシナリオでは、プライオリティ帯域幅は子のキューからインターフェイス キューへ伝播されません。

プライオリティ レート伝播および BRR の設定例

次に、子ポリシー マップでビデオ トラフィックにプライオリティ レベル（2）が割り当てられ、BRR と併用されている例を示します。この設定は親ポリシー マップで行われています。

```
policy-map parent
 class class-default
   bandwidth remaining ratio 1
   service-policy child

policy-map child
 class video
   priority level 2
   police 200 Mbps
```

サポートされない IP 加入者セッションの機能

内部 LAN を IP 加入者間で共有できるよう割り当てる方法により、個々の加入者は次の機能を使用できません。

- Policy-based Routing（PBR; ポリシー ベース ルーティング）、ネットワーク アドレス変換（NAT）、unicast Reverse Path Forwarding (uRPF; ユニキャスト RPF)
- IPv4 および IPv6 マルチキャスト
- Encoded address resolution logic（EARL）機能（再帰 ACL、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネリング、Context-Based Access Control（CBAC; コンテキスト ベースのアクセス コントロール）、および Server Load Balancing（SLB）など）

IP Subscriber Awareness over Ethernet 設定時の注意事項

（注）　IP Subscriber Awareness over Ethernet 機能は IP サービスのソフトウェア イメージ（*xxx*-ipservices_wan-mz）では使用できません。イメージには **interface** コマンドで **access** キーワードが使用可能として表示されますが、加入者認識機能は使用できません。

Cisco 7600 ルータで IP Subscriber Awareness over Ethernet を設定する際は、次のガイドラインと制約事項に従ってください。

- ソフトウェアおよびハードウェアの要件
  - Cisco IOS Release 12.2SRB 以降
  - PFC3C または PFC3CXL を備えた RSP720（他のスーパーバイザ エンジンはサポートされません）
  - Cisco 7600 SIP-400 および 5 ポート ギガビット イーサネット SPA（SPA-5X1GE-V2）
  - 12.2(33)SRE 以降の ES+ ラインカードに対するサポート
- オーバーサブスクライブがサポートされるのは、5 ポート ギガビット イーサネット SPA だけです。
- ルータでは最大 32000 のインターフェイスがサポートされます。32000 インターフェイスをサポートするには：
  - RSP720 には 2 GB の RP メモリと 1 GB の SP メモリが必要です。
  - Cisco 7600 SIP-400 には 1 GB のメモリが必要です。
- Cisco 7600 SIP-400 は最大 8000 の IP 加入者をサポートします。
- 5 ポート ギガビット イーサネット SPA（SPA-5X1GE-V2）は最大 8000 VLAN をサポートします。
- IP 加入者を表すアクセス サブインターフェイスを .1Q または Q-in-Q カプセル化向けに設定することが必要です。
- アクセス サブインターフェイスの MTU は 1500 で、この値は変更できません。
- 通常の GE サブインターフェイスをアクセス インターフェイスに変更できますが、アクセス インターフェイスを通常の GE インターフェイスには変更できません。代わりに、アクセス サブインターフェイスを削除する必要があります。

- EARL ベースの機能はサポートされません。この機能には、Network Address Translation（NAT）、再帰 ACL、Generic Routing Encapsulation（GRE）トンネリング、Context-Based Access Control（CBAC）、および Server Load Balancing（SLB）が含まれます。
- リンク冗長性に対して Hot Standby Routing Protocol（HSRP）を設定しないことを推奨します。
- QoS の注意事項については、「QoS に関する推奨事項」（P.24-21）を参照してください。

他の機能との相互作用

IP Subscriber Awareness over Ethernet とルータで設定される他の機能との相互作用を次に示します。

- マルチキャスト トラフィックはこの機能による影響を受けません。ルータは IGMP 機能および複製に関与でき、このとき IP Subscriber Awareness over Ethernet による影響を受けません。さらにルータは、データ サービスの認証を受けていないマルチキャスト トラフィックをサポートします。これにより、データ サービスなしで基本ビデオ サービスが提供されます。

  （ルータではなく）DSLAM がマルチキャスト トラフィックの複製と、IP 加入者への複製の配信を行います。したがって、IP Subscriber Awareness over Ethernet 機能が IP 加入者インターフェイス（アクセス インターフェイス）上でマルチキャストトラフィックをサポートする必要はありません。

IP Subscriber Awareness over Ethernet の設定

ここでは、Cisco 7600 シリーズ ルータ上での IP Subscriber Awareness over Ethernet 機能の設定について説明します。

- 「設定の概要」（P.24-29）
- 「設定例」（P.24-31）

設定の概要

次に Cisco 7600 ルータ上で IP Subscriber Awareness over Ethernet を設定する際に必要な手順の概要を説明します。次のセクションで、詳細な設定の手順を説明します。

設定を開始する前に

- 各 IP 加入者をどの VPN routing and forwarding（VRF）テーブルに含めるかを決定します。VRF 内のすべての加入者は、データ サービスについて単一の内部 VLAN を共有します。**ip vrf** および **rd** コマンドを使用して、必要な VRF テーブルを作成します。

  同じ VRF を使用するには、加入者は同じ Network Service Provider（NSP; ネットワーク サービス プロバイダー）、Internet Service Provider（ISP; インターネット サービス プロバイダー）、または Access Service Provider（ASP; アクセス サービス プロバイダー）に属していることが必要です。加入者を VRF に割り当てなかった場合、加入者は、システム起動時にルータが作成するデフォルトの VRF に追加されます。

- ルータを必ず DHCP サーバまたは DHCP リレー デバイスとして設定し、IP 加入者セッションに IP アドレスが動的に割り当てられるようにします。そうでなければ、各 IP 加入者のアクセス サブインターフェイスに静的 IP アドレスを割り当てることが必要となります（この作業は推奨できません）。

  DHCP の設定方法については、次の URL の『*Cisco IOS IP 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

- IP 加入者が使用する物理インターフェイスを指定します。各 IP 加入者に対して、加入者が接続する物理インターフェイス上のアクセス サブインターフェイスを設定します。

IP 加入者に QoS および HQoS ポリシーを設定する

- QoS ポリシー（クラス マップおよびポリシー マップ）を定義して、加入者トラフィックに対して加入者トラフィック帯域幅とシェーピング ポリシーを定義します。階層型 QoS（HQoS）ポリシーを使用して、トラフィックをさまざまなレベルでシェーピングできます。たとえば、親ポリシーで加入者の総帯域幅を定義し、子ポリシーで異なるタイプの加入者トラフィック（ビデオなど）の帯域幅を定義できます。サブインターフェイスでは、子ポリシーを付加できるのは親のデフォルト クラスだけです。
- （任意）デュアルプライオリティ キューを作成して、加入者の音声およびビデオ トラフィックを処理できます。
- また、さまざまなタイプの加入者トラフィックに対して Class-Based Weighted Fair Queue（CBWFQ）または Priority Queue（PQ; プライオリティ キューイング）を定義できます。

アクセス リストおよびセキュリティ ACL を設定する

- IP 加入者に必要なセキュリティ ポリシーを決定します。アクセス リストとセキュリティ ACL を作成して、これらのポリシーを定義します。

  次に、IP 加入者に適用される 2 つのアクセス リスト（2 および 3）の例を示します。

```
access-list 2 permit 18.18.18.18
access-list 3 permit 23.23.23.23
access-list 101 deny   ip 44.1.1.0 0.0.0.255 any
access-list 101 permit icmp any any
```

  次に、アクセス サブインターフェイス gig0/1/1.100 によって表される IP 加入者セッションの入力および出力セキュリティ ACL を設定する例を示します。

```
interface gig0/1/1.100 access
  encapsulation dot1q 100
  ip address 10.10.10.1 255.255.255.0
  ip access-group 101 in
  ip access-group 102 out
```

IP 加入者インターフェイスを設定する

- 各 IP 加入者のアクセス インターフェイスを作成します。アクセス インターフェイスを加入者の物理インターフェイスのサブインターフェイスとして作成します。たとえば、加入者が Gig1/0/0 に接続されている場合、アクセス インターフェイスを Gig1/0/0.100 と設定できます。
- アクセス インターフェイスを次のとおり設定します。
  - 必要に応じて、インターフェイスに IP アドレス（スタティック IP アドレス）を割り当てます。多数のアクセス インターフェイスを静的 IP アドレスを使って設定しないことを推奨します。代わりに、DHCP が IP 加入者セッションの IP アドレスを動的に割り当てられるようにする必要があります。
  - IP 加入者が特定の VRF テーブルに属している場合、設定に **ip vrf forwarding** *vrf-name* コマンドを含めて、インターフェイスをテーブルに関連付けます。VRF テーブルを指定しなかった場合、加入者はデフォルトの VRF に追加されます。
  - カプセル化タイプ（.1Q または Q-in-Q）を設定し、インターフェイスが属する VLAN を指定します。

- インターフェイスに QoS ポリシーを付加して、加入者トラフィックに対するトラフィック帯域幅とシェーピング ポリシーを定義します。

次の例では、2 つの IP 加入者アクセス インターフェイス（gig1/0/0.100 および gig1/0/0.300）を示します。加入者は Gig1/0/0 を介して接続されているので、アクセス インターフェイスは Gig1/0/0 のサブインターフェイスとして作成されます。gig1/0/0.100 には静的 IP アドレスが割り当てられ、gig1/0/0.300 は DHCP を使用して IP アドレスを取得していることに注意してください。また、gig1/0/0.300 は VRF を認識します。

```
interface gig1/0/0.100 access
 ip address 10.10.10.10 255.255.255.255
 encapsulation dot1q 100
 service-policy input bband-in1
 service-policy output bband-out1

interface gig1/0/0.300 access
 ip vrf forwarding vrf1
 encapsulation dot1q 300
 service-policy input bband-in1
 service-policy output bband-out1
```

機能を確認する IP Subscriber Awareness over Ethernet

次のコマンドを使用して、IP 加入者を表す各アクセス インターフェイスのステータスを確認します。各加入者についてアクセス インターフェイスが存在し、インターフェイスが起動状態であることが必要です。

- **show running-config interface** *interface.subinterface* コマンドを発行して、各アクセス サブインターフェイスの設定を確認します（ここでの *interface* は物理インターフェイスで、*.subinterface* はアクセス サブインターフェイスです）。たとえば、**show running-config interface Gig1/0/2.1** は、物理インターフェイス Gig1/0/2 上に存在するアクセス サブインターフェイス（.1）を表示します。

設定例

次の例では、3 つの加入者（Gig3/2/0.10、Gig3/2/0.11、Gig3/2/0.12）を持つ設定を示します。それぞれ、gold（30 Mbps）、silver（15 Mbps）、bronze（5 Mbps）という異なるタイプのサービスを受けています。各加入者には、加入者単位のアカウンティングおよび加入者単位の ACL が設定されています。

ビデオ トラフィックが廃棄されないよう QoS ポリシー マップが設定されており、デフォルト トラフィックは 30:15:5 の比率で共有されています（したがって、帯域幅余剰比率は 6:3:1 となります）。

```
aaa new-model
aaa accounting network defaul start group radius
radius-server key cisco
radius-server host 2.2.2.2
int loopback 1
ip address 13.0.7.254 255.255.248.0

ip dhcp pool Loopback1
  network 13.0.0.0 255.255.248.0

Class-map voip
 match ip precedence 5

Class-map video
 match ip precedence 6

policy-map data_gold_child_out
```

```
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 30000000
   set cos 3

policy-map data_gold_parent_out
 class class-default
   shape average 29900000
   bandwidth remaining ratio 6
   service-policy data_gold_child_out

policy-map data_silver_child_out
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 15000000
   set cos 2

policy-map data_silver_parent_out
 class class-default
   shape average 29900000
   bandwidth remaining ratio 3
   service-policy data_silver_child_out

policy-map data_bronze_child_out
 class video
   priority level 2
   police 27000000
   set cos 5
 class class-default
   police 5000000
   set cos 1

access-list 102 permit ip any any precedence 5
access-list 102 permit ip any any precedence 2
access-list 102 permit ip any any precedence 0

policy-map data_bronze_parent_out
 class class-default
   shape average 29900000
   bandwidth remaining ratio 1
   service-policy data_bronze_child_out

policy-map data_gold_in
  class class-default
    police 5000000
policy-map data_silver_in
  class class-default
    police 2000000
policy-map data_bronze_in
  class class-default
    police 2000000


interface gig 3/2/0.10 access
    ip unnumbered Loopback 1
    encapsulation dot1q 10
    service-policy output data_gold_parent_out
    service-policy input data_gold_in
```

```
    accounting dhcp source-ip aaa list default
    ip access-group 103 in

interface gig 3/2/0.11 access
    ip unnumbered Loopback 1
    encapsulation dot1q 11
    service-policy output data_silver_parent_out
    service-policy input data_silver_in
    accounting dhcp source-ip aaa list default
    ip access-group 103 in

interface gig 3/2/0.12 access
    ip unnumbered Loopback 1
    encapsulation dot1q 12
    service-policy output data_bronze_parent_out
    service-policy input data_bronze_in
    accounting dhcp source-ip aaa list default
    ip access-group 103 in
```

コマンド リファレンス

ここでは、IP Subscriber Awareness over Ethernet の新しいコマンドを説明します。この機能の一部として、次の新しいコマンドが導入されています。

- interface access

interface access

IP 加入者にアクセス インターフェイスを作成するには、グローバル コンフィギュレーション モードで **interface access** コマンドを使用します。IP 加入者のアクセス インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface *interface***.***subinterface* **access**

no interface *interface***.***subinterface* **access**

構文の説明

interface	この IP 加入者が接続されている物理インターフェイスを識別します。
.*subinterface*	アクセス インターフェイスに割り当てるサブインターフェイス番号

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IP 加入者のアクセス インターフェイスが作成されます。アクセス インターフェイスは、加入者が接続されている物理インターフェイスのサブインターフェイスとして作成します。たとえば、加入者が Gig1/0/0 に接続されている場合、アクセス インターフェイスを Gig1/0/0.1、Gig1/0/0.2、Gig1/0/0.3、などのように設定できます。

指定した VRF テーブルに IP 加入者を関連付けるには、設定に **ip vrf forwarding** *vrf-name* コマンドを含めます。VRF テーブルを指定しなかった場合、加入者はデフォルトの VRF テーブル（ルータの起動時に作成される）に追加されます。

例

次に、IP 加入者のアクセス インターフェイスを作成して、vrf1 という名前の VRF テーブルに加入者を割り当てるコマンドの例を示します。アクセス インターフェイスは、物理インターフェイス Gig2/0/1 上のサブインターフェイス .300 として作成されます。その他追加するコマンド（カプセル化タイプの指定や QoS ポリシーの割り当てなど）があれば実行して、設定を完了します。

```
Router(config)# interface Gig2/0/1.300 access
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)#
```

CHAPTER 25

UDE および UDLR の設定

この章では、Cisco 7600 シリーズ ルータにおける Unidirectional Ethernet（UDE）および Unidirectional Link Routing（UDLR）の設定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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「UDE および UDLR の概要」（P.25-1）
- 「UDE および UDLR の設定」（P.25-3）

UDE および UDLR の概要

ここでは、UDE および UDLR について説明します。

- 「UDE および UDLR の概要」（P.25-1）
- 「サポート対象ハードウェア」（P.25-2）
- 「UDE の概要」（P.25-2）
- 「UDLR の概要」（P.25-3）

UDE および UDLR の概要

単一方向リンクが双方向リンクをエミュレートする場合に限り、ルーティング プロトコルは同一インターフェイスにおけるトラフィックを送受信するはずなので、ルーティング プロトコルでは単一方向リンクがサポートされます。

単一方向リンクには有利な点があります。ほとんど確認応答されていない単一方向の大量のトラフィック（ビデオ ブロードキャスト ストリームなど）を大容量全二重双方向リンクで送信する場合は、送信元からレシーバへのリンク、および同様に大容量な逆方向リンク（レシーバから送信元への少ない確認応答を搬送する「バック チャネル」と呼ばれる）の両方を使用するからです。

UDE および UDLR では、大量トラフィック用の大容量単一方向リンクの使用が、バック チャネル用の同様に大容量のリンクを消費せずにサポートされます。UDE では、大容量単一方向リンクが提供されます。UDLR では、通常の容量のリンクで設定されるトンネルでバック チャネルが提供されます。また、トランスペアレントにバック チャネルと大容量単一方向リンクと同じインターフェイス上にあるかのようにして双方向リンクをエミュレートします。

サポート対象ハードウェア

Cisco 7600 シリーズ ルータでは、次のスイッチング モジュールのインターフェイスで UDE および UDLR がサポートされます。

- 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」（P.25-2）
- 「ハードウェアベース UDE の概要」（P.25-2）
- 「ソフトウェアベース UDE の概要」（P.25-3）

UDE の概要

Cisco 7600 シリーズ ルータでは、ハードウェアまたはソフトウェアで 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 の両方で、双方向トラフィックが必要とする 2 本のファイバではなく、1 本のファイバだけが使用されます。

単一方向トランシーバは、ハードウェアベース UDE が受信専用であるか送信専用であるかを判断します。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かに設定できます。

ハードウェアベース UDE を実装するポートで、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含むモジュールのリストについては、「サポート対象ハードウェア」（P.25-2）を参照してください。

ハードウェアベース UDE の概要

双方向トランシーバより安価の単一方向トランシーバを使用して、単一方向リンクを作成できます。では、次の単一方向トランシーバがサポートされます。Cisco 7600 シリーズ ルータでは、単一方向トランシーバがサポートされます。

- 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

トラフィックを単一方向で送信するか受信するように、双方向トランシーバに装備されているポートを設定し、単一方向リンクを作成できます。適切な単一方向トランシーバを使用できない場合は、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は、ソフトウェアベース UDE で送信専用リンクを設定する必要があります。

UDLR の概要

UDLR では、単一方向大容量リンクのバック チャネルとしての単一方向トンネルが提供され、ユニキャスト トラフィックおよびマルチキャスト トラフィック用に 1 つの双方向リンクがトランスペアレントにエミュレートされます。

UDLR は、受信専用インターフェイスで送信する必要があるパケットを代行受信し、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 トンネルでこのようなパケットを受信すると、パケットは、UDLR によって、送信専用インターフェイスで受信したかのような形になります。

UDLR バックチャネル トンネルでは、次の IPv4 機能がサポートされます。

- アドレス解決プロトコル（ARP）
- Next Hop Resolution Protocol（NHRP）
- すべての IPv4 トラフィック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の制御トラフィックだけではない）
- 受信専用トンネルにおける IPv4 GRE マルチポイント

（注）　UDLR バックチャネル トンネルでは、IPv6 または MPLS がサポートされません。

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。

- 「UDE の設定」（P.25-3）
- 「UDLR の設定」（P.25-6）

（注）　次の説明は、UDLR をサポートするリリースで公開されています。ネイバー ISIS ルータは、UDLR トポロジで認識されません （CSCee56596）。

UDE の設定

ここでは、UDE を設定する手順について説明します。

- 「UDE 設定時の注意事項」（P.25-4）
- 「ハードウェアベース UDE の設定」（P.25-5）
- 「ソフトウェアベース UDE の設定」（P.25-5）

UDE 設定時の注意事項

UDE を設定する場合は、次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。
- STP では、単一方向リンクを含むトポロジにおいてレイヤ 2 ループを防止できません。
- 送信専用ポートは、BPDU を受信しないので、STP フォワーディング ステートに常に移行します。
- 受信専用ポートは BPDU を送信できません。
- 単一方向ポートでは、次のようにリンクの反対側の終端にあるポートとのネゴシエーションが必要になる機能またはプロトコルがサポートされません。
  - 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
  - IEEE 802.3Z フロー制御
  - ダイナミック トランキング プロトコル（DTP）

  レイヤ 2 プロトコルによって一般的に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 トランキング プロトコル（VTP）サーバが VTP ドメインのすべてのルータに VTP フレームを送信できる場合、単一方向リンクを含むトポロジでは、VTP だけがサポートされます。
- VTP プルーニングは情報の双方向の交換によって異なるので、送信専用ポートがあるルータでは VTP プルーニングをディセーブルにしてください。
- 単一方向 EtherChannel では PAgP または LACP をサポートできません。単一方向 EtherChannel を作成するには、EtherChannel「オン」モードを設定する必要があります。
- EtherChannel の物理ポートでソフトウェアベース UDE を設定できます。ポートチャネル インターフェイスなどの物理的でないインターフェイスでは、ソフトウェアベース UDE を設定できません。
- ハードウェアベース UDE をポートで実装するか、ソフトウェアベース UDE をポートで設定する場合、UDLD はそのポートで自動的にディセーブルになります。
- CDP は、送信専用ポートから CDP フレームを送信し、受信専用ポートから 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にあるルータは、CDP 情報を受信しません。
- SPAN は、単一方向ポートの設定を送信側や宛先に限定しません。
  - 送信専用ポートは、SPAN 宛先にすることができます。
  - 受信専用ポートは、SPAN 送信元にすることができます。
- 単一方向ポートでは、IEEE 802.1X ポートベース認証がサポートされません。
- 12.2(33) SRD4 リリースよりも前は、インターフェイスが SPAN 宛先ポートになっているポート上で SPAN と UDLD の組み合わせを設定すると、UDLD がローカル エンドでディセーブルになっているように、UDLD ピアの現在の動作状態がディセーブルになります。12.2(33) SRD4 リリース以降は、インターフェイスが SPAN 宛先として設定されている場合は、UDLD ピアの現在の動作状態が「Disabled」ではなく、「Advertisement」と表示されます。
- IGMP スヌーピングでは、ルータおよびマルチキャスト トラフィックを受信するホストの間に単一方向リンクがあるトポロジがサポートされません。
- スイッチの IGMP スヌーピングとマルチキャスト ルータの間で単一方向リンクによる通信をサポートするには、UDLR を UDE とともに設定します。
- 単一方向リンクでは ARP がサポートされません。
- OIR の間は、ラインカードがオンラインではない場合、UDE 設定を削除すべきではありません。削除した場合、ポート上の UDLD 機能が失われます。

カードがオフラインの間に UDE 設定を削除してしまった場合で、UDLD を再度イネーブルにするには、次の作業を行う必要があります。

- ルータをリロードするか、または、
- そのポートの UDE を再度設定し、ラインカードがオンラインのときにだけ、UDE の設定を解除します。

ハードウェアベース UDE の設定

ハードウェアベース UDE をサポートする場合に、必要なソフトウェア設定手順はありません。単一方向トランシーバを設置し、ハードウェアベース UDE を実装してください。

ポートの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

ポートのソフトウェアベース UDE 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** | **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 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 で UDE 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
```

次の例は、単一方向イーサネットをサポートしないポートで **show interface** コマンドを入力した結果を示しています。

```
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.25-6）
- 「UDE 送信専用ポートの受信専用トンネル インターフェイスの設定」（P.25-7）
- 「UDE 受信専用ポートの送信専用トンネル インターフェイスの設定」（P.25-7）

UDLR バックチャネル トンネル設定時の注意事項

UDLR バックチャネル トンネルの設定時には、次の注意事項に従ってください。

- PFC3 では、UDLR バックチャネル トンネルがハードウェアでサポートされません。MSFC3 および MSFC4（RSP720）では UDLR バックチャネル トンネルがソフトウェアでサポートされます。
- 単一方向リンクごとに、UDLR バックチャネル トンネルを設定してください。
- UDE 送信専用インターフェイスでは、UDLR バックチャネル トンネル インターフェイスを受信に設定してください。

- UDE 受信専用インターフェイスでは、UDLR バックチャネル トンネル インターフェイスを送信に設定してください。
- 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は、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 トンネルでは、IPv6 または MPLS がサポートされません。

UDE 送信専用ポート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}`	トンネル宛先を設定します。

UDE 受信専用ポート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。

次の UDE および UDLR の設定例は、次のようになっています。

- ルータ A の場合 :
  - Open Shortest Path First（OSPF）および 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 は送信専用 UDE ポートです。
  - UDLR バックチャネル トンネルは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 と関連しています。

- ルータ B の場合:
  - OSPF および 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 1/2 は受信専用 UDE ポートです。
  - UDLR バックチャネル トンネルは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 と関連しています。
  - ARP および NHRP がイネーブルです。

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 26

PFC のマルチプロトコル ラベル スイッチングの設定

この章では、Cisco 7600 PFC カードの Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を設定する手順について説明します。この章で扱う内容は、PFC3B、PFC3BXL、PFC3C、および PFC3CXL カードの MPLS 動作です。特に説明がない場合、MPLS の動作は、これらの PFC カードすべてで同じです。

（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、次の資料を参照してください。

- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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。

- 「PFC MPLS ラベル スイッチング」（P.26-1）
- 「PFC の VPN スイッチング」（P.26-15）
- 「Any Transport over MPLS」（P.26-19）

PFC MPLS ラベル スイッチング

ここでは MPLS ラベル スイッチングについて説明します。

- 「MPLS の概要」（P.26-2）
- 「MPLS ラベル スイッチングの概要」（P.26-2）
- 「サポート対象ハードウェア機能」（P.26-5）
- 「サポート対象 Cisco IOS 機能」（P.26-5）
- 「MPLS に関する注意事項および制約事項」（P.26-7）
- 「MPLS の設定」（P.26-8）
- 「MPLS のラベル単位ロード バランシング」（P.26-8）
- 「MPLS の設定例」（P.26-9）

- 「スケーラブル EoMPLS とポートモード EoMPLS」（P.26-22）
- 「SwEoMPLS および VPLS のサンプル設定」（P.26-22）

MPLS の概要

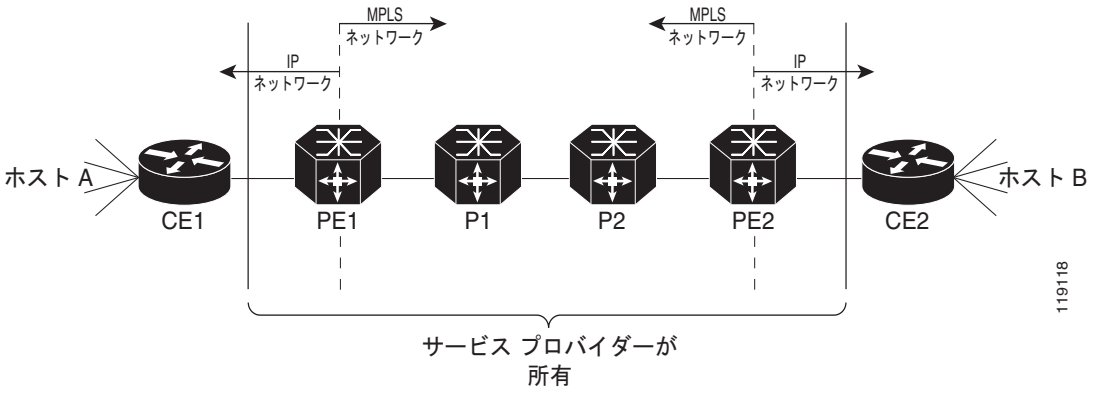
MPLS はラベル スイッチングを使用して、Packet-over-SONET（POS）、フレーム リレー、ATM、イーサネットなどのさまざまなリンクレベル テクノロジーを通してパケットを転送します。ラベルはグループ化または Forwarding Equivalence Class（FEC）に基づいて、パケットに割り当てられます。ラベルはレイヤ 2 ヘッダーとレイヤ 3 ヘッダーの間に追加されます。

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 Switching Router（LSR; ラベル スイッチング ルータ）のネクスト ホップに送信します。ラベルがパケットに対してインポーズ（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定されます。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があります。集約ラベルの場合は、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 検索を通して着信 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は、パケットに IP ネクスト ホップ情報が格納されます。

図 26-1 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 26-1　　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

MPLS ラベル スイッチングの概要

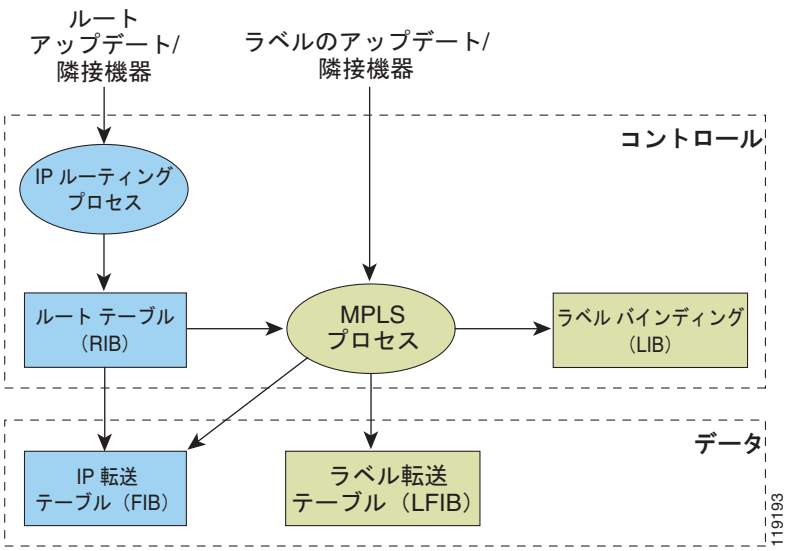
PFC では、レイヤ 3 マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）、およびレイヤ 2 Ethernet over MPLS（EoMPLS）が、Quality of Service（QoS）およびセキュリティとともにサポートされます。

スーパーバイザ エンジンの MSFC 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 制御プレーン機能を実行します。MSFC はルーティング プロトコルおよびラベル配布プロトコルからの情報を処理し、IP 転送（FIB）テーブルおよびラベル転送（LFIB）テーブルを構築します。MSFC は両方のテーブルの情報を PFC に配布します。

PFC は情報を受信し、FIB および LFIB テーブルのコピーを独自に作成します。同時に、これらのテーブルから FIB TCAM を作成します。DFC は FIB TCAM 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です。この隣接エントリには、ラベルのプッシュ（IP から MPLS へのパスの場合）、ラベルのスワップ（MPLS から MPLS へのパスの場合）、ラベルのポップ（MPLS から IP へのパスの場合）、およびカプセル化に関する適切な情報が格納されます。

図 26-2 に、MPLS ラベル スイッチングをサポートする PFC の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されるルーティング情報ベース（RIB）を生成します。シスコ エクスプレス フォワーディング（CEF）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 26-2　　MPLS 転送、制御、およびデータ プレーン



IP から MPLS

PFC 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です。隣接エントリには、ラベルのプッシュ（IP から MPLS へのパスの場合）およびカプセル化に関する適切な情報が格納されています。PFC は、MPLS パケットのスイッチングに必要なインポジション ラベルを含む結果を生成します。

（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.26-9）を参照してください。

MPLS から MPLS

PFC 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。正常な検索結果によって隣接を示すと、パケット内の最上位ラベルが、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られます。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 または PFC3CXL 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 から IP

MPLS ネットワークの出口では、いくつかの処理が考えられます。

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）、PFC は FIB TCAM 内でルートを検索します。

MPLS VPN パケットの場合は、内部ゲートウェイ プロトコル（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。PFC 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、集約ラベルのポップ後に、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、PFC 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 ラベルが付加されたパケットの場合、最後から 2 番めのホップでのポッピング（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。PFC 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。その後、PFC は上記段落の説明に従って、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、および MPLS VPN の場合、明示的 null ラベルが付加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

直接接続ネットワークまたは集約ルート用の集約ラベル、および非集約ラベルという 2 種類の VPN ラベルがあります。集約ラベルを伝送するパケットでは、集約ラベルのポップ後に、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、およびラベル）は、Multiprotocol-Border Gateway Protocol（MP-BGP）によって配布されます。

再循環

場合により、PFC 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、ACL 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。再循環は次の状況で必要となります。

- 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 ルーティングおよび転送（VRF）番号が 511 よりも大きい場合
- 出力インターフェイスの IP ACL の場合（非集約（プレフィックス単位）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 フローに対してだけです。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 PFC に転送されて、さらに処理されます。

サポート対象ハードウェア機能

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で 3 つに、ポップするラベル数を最大で 2 つにしてください。
- IP から MPLS へのパス：IP パケットを受信して、MPLS パスに送信できます。
- MPLS から IP へのパス：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 から MPLS へのパス：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 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。
- Time to Live（TTL）処理：MPLS ネットワークの入力エッジでは、MPLS フレーム ヘッダーの TTL 値を、IP パケット ヘッダーの TTL フィールドから受信したり、隣接エントリのユーザ設定値から受信したりできます。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）　均一モードの場合、TTL は IP TTL から取得されます。パイプ モードの場合、発信ラベルにはハードウェア レジスタから取得された値 255 が使用されます。

- QoS：IP パケットから取得された Differentiated Services（DiffServ）および ToS 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（511 個を超える VRF を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、出口でカプセル化解除できます。
- パケット再循環：PFC にはパケット再循環機能があります。「再循環」（P.26-4）を参照してください。
- 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。

サポート対象 Cisco IOS 機能

PFC 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）　CE ルータの multi-VPN ルーティング/転送（VRF）（VRF Lite）は、VRF インターフェイスの間の IPv4 転送、IPv4 ACL、IPv4 Hot Standby Router Protocol（HSRP）機能とともにサポートされています。

- CE ルータの multi-VRF（VRF Lite）：VRF Lite は、IP アドレスが VPN 間で重複使用できる複数の VPN（VRF ベース IPv4 だけを使用）を、サービス プロバイダーがサポートできるようにするための機能です。次の資料を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html

- Cisco 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および削除したり、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。次の資料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 エンジニアリングは従来のレイヤ 2 機能をレイヤ 3 トラフィック フローでも利用できるようにします。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/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。次の資料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：この機能を使用すると、ネットワーク管理者はトラフィック エンジニアリングおよびラベルスイッチド パス（LSP）トンネルを、Shortest Path First（SPF）アルゴリズムに基づいた内部ゲートウェイ プロトコル（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）ルーティングによる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 エリア間トンネル：この機能を使用すると、ルータは複数の内部ゲートウェイ プロトコル（IGP）領域およびレベルにわたって 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という制限事項を解消できます。次の資料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）：この機能により、Cisco IOS ネットワーク上にスケーラブルな IPv4 レイヤ 3 VPN バックボーン サービスを導入できます。次の資料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。次の資料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 Carrier Supporting Carrier IPv4 BGP 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 プロバイダー エッジ（PE）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 ラベルを転送できるように、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/ftcscl13.htm

- MPLS VPN 相互自律システム（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自律システムに拡張できます。次の資料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 Inter-AS IPv4 BGP ラベル配布：この機能を使用すると、自律システム境界ルータ（ASBR）が IPv4 ルートを PE ルータの MPLS ラベルと交換するように 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/ftiasl13.htm

- MPLS VPN ホットスタンバイ ルータ プロトコル（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。次の資料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 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）プロトコルが稼働する VPN クライアント サイトに接続し、MPLS VPN 設定内で OSPF リンクを共有できます。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/122t8/ospfshmk.htm

- Any Transport Over MPLS（AToM）：MPLS バックボーン上でレイヤ 2 パケットを転送します。「Any Transport over MPLS」（P.26-19）を参照してください。

MPLS に関する注意事項および制約事項

PFC で MPLS を設定するときは、次の注意事項および制約事項に従ってください。

- PFC は最大 8 個の負荷分散パスをサポートします。その他のプラットフォームの Cisco IOS リリースでは、8 個の負荷分散パスだけがサポートされます。
- PFC では、MTU チェックおよび分割がサポートされます。
- 分割はソフトウェアでサポートされます（IP から MPLS のパスの場合）。『*Cisco 7600 Series Router Cisco IOS Command Reference*』の **mtu** コマンドの説明を参照してください。
- MPLS を設定するときには、次の最大伝送単位（MTU）の注意事項に従ってください。
  - MPLS リンクの両端は同じ MTU サイズにする必要があります。そうでなければ、MPLS はインターフェイスのミスマッチを検出し、動作しなくなります。

    MPLS over RBE では異なる MTU サイズが可能です（たとえば、デフォルトのギガビット イーサネットと ATM など）。ただし、OSPF over RBE が稼働している場合、**ip ospf mtu-ignore** コマンドを ATM インターフェイスで追加する必要があります。そうしなければ、OSPF はミスマッチを検出し、アクティブになりません。

– MPLS MTU サイズは、MPLS リンクが使用する物理インターフェイスの MTU サイズより小さい値にする必要があります。そうしなければ、問題が発生し、MPLS パケットが廃棄される場合があります。

推奨されませんが、**mpls mtu override** *bytes* コマンドを使用すると、MPLS MTU サイズをインターフェイスの MTU サイズより大きい値に設定できます（*bytes* には MPLS MTU サイズを指定します）。

（注）　**mpls mtu override** *bytes* コマンドは、1580 バイト以下のデフォルト MTU サイズのインターフェイス（イーサネットなど）だけで使用できます。ATM ブリッジ インターフェイスでは使用できません。

- その他の制約事項については、「MPLS VPN に関する注意事項および制約事項」（P.26-16）および「EoMPLS に関する注意事項および制約事項」（P.26-20）を参照してください。

MPLS でサポートされるコマンド

PFC の 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

これらのコマンドの詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html

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*』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t3/feature/guide/rtr_13t.html

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、および MPLS レイヤ 3 VPN のロード バランシング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。PFC では、明示的に設定しなくても MPLS ラベル付きパケットが転送されます。パケットに付加されたラベルが 3 つ以下で、基礎となるパケットが IPv4 の場合、PFC 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 でないか、3 つより多いラベルが存在する場合、PFC は 5 番めまたは最下位の深さまでのラベル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 MAC 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 VC 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 バランシングが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.26-9）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
```

マルチキャスト隣接割り当て

マルチキャスト隣接割り当て機能を使用すると、マルチキャスト ルートに対して隣接エントリの予約ができます。1 つのリージョン内で、またはリージョン単位でマルチキャスト範囲を設定できます。

マルチキャスト隣接割り当ての制限

マルチキャスト隣接割り当てには次の制限が適用されます。

- この機能は、PFC-3A、3B、3BXL、3C、3CXL でサポートされます。
- マルチキャスト隣接エントリを設定した後、新しい隣接割り当て方式をイネーブルにするためにルータを再起動する必要があります。
- 新しい割り当て方式はユニキャスト隣接に制限されます。マルチキャスト隣接の割り当て方式は変更されません。

マルチキャスト隣接割り当ての設定

ここでは、マルチキャスト隣接割り当てを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mls cef adjacency-mcast** {*number* | **region** *region per-region*}
4. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**mls cef adjacency-mcast** {*number*	**region** *region per-region*} **例：** `Router# mls cef adjacency-mcast region 31 2`	マルチキャスト隣接の番号とリージョンを指定します。有効な値は次のとおりです。 *number*：1 ～ 16K *region*：1 ～ 31 *per-region*：1 ～ 16 **（注）** グローバルおよびリージョン単位の設定は共存できます。 **（注）** リージョンに対して設定可能な最大割り当ては 16K です（リージョンが 31 の場合を除く）。リージョンが 31 の場合は、最大割り当ては 13K です。
ステップ 4	**end** **例：** `Router(config-if)# end`	コンフィギュレーション モードを終了します。

設定例

次に、マルチキャスト隣接番号を指定する例を示します。

```
Router# configure terminal
Router(config)#mls cef adjacency-mcast region 31 2
Router(config)# end
```

次に、グローバル レベルで機能を無効にする例を示します。

```
Router# configure terminal
Router(config)#no mls cef adjacency-mcast
Router(config)# end
```

次に、リージョン レベルで機能を無効にする例を示します。

```
Router# configure terminal
Router(config)#no mls cef adjacency-mcast region 31
Router(config)# end
```

設定の確認

次に、マルチキャスト隣接割り当てテーブルを表示する例を示します。

```
Router# show mls cef adjacency list

Region0:
   Head:    1738B928, 16351, 33
   Next:    1738B928, 16351, 33
   Midptr:  0
   Limit:   16384
   Usage:   33
   Start:   0
   End:     16383
   Size:    16384
   MidPt:   8192
   Search:  1
   Stats:   1
   BC[0]:  1
   BC[1]:  0
   BC[2]:  0
   BC[3]:  0
   BC[4]:  0
   BC[5]:  0
   BC[6]:  0
   BC[7]:  0
   BC[8]:  0
   BC[9]:  0
   BC[10]:  0
   BC[11]:  0
   BC[12]:  0
   BC[13]:  0
   BC[14]:  0
   BC[15]:  0
   BC[16]:  0
Region1:
   Head:    1738B904, 16377, 16391
   Next:    1738B904, 16377, 16391
   Midptr:  0
```

```
   Limit:   16057
   Usage:   7
   Start:   16384
   End:     32767
   Size:    16384
   MidPt:   24412
   Search:  1
   Stats:   1
   BC[0]:  1
   BC[1]:  0
   BC[2]:  0
   BC[3]:  0
   BC[4]:  0
   BC[5]:  0
   BC[6]:  0
   BC[7]:  0
   BC[8]:  0
   BC[9]:  0
   BC[10]:  0
   BC[11]:  0
   BC[12]:  0
   BC[13]:  0
   BC[14]:  0
   BC[15]:  0
   BC[16]:  0
Region2:
   Head:    1738B8E0, 16377, 32775
   Next:    1738B8E0, 16377, 32775
   Midptr:  0
   Limit:   16057
   Usage:   7
   Start:   32768
   End:     49151
   Size:    16384
   MidPt:   40796
   Search:  1
   Stats:   1
   BC[0]:  1
   BC[1]:  0
.............................
```

次に、マルチキャスト隣接の使用を表示する例を示します。

```
Router#show mls cef adjacency usage

Adjacency Table Size:     1048576
ACL region usage:         3
Non-stats region usage:   132
Stats region usage:       249
Total adjacency usage:    384
```

次に、マルチキャスト隣接の数を表示する例を示します。

```
Router#show mls cef adjacency count

Region0:         33      Region1:        7
Region2:         7       Region3:        7
Region4:         7       Region5:        7
Region6:         7       Region7:        7
Region8:         7       Region9:        7
Region10:        7       Region11:       7
```

```
Region12:        7       Region13:       7
Region14:        7       Region15:       7
Region16:        7       Region17:       7
Region18:        7       Region19:       7
Region20:        7       Region21:       7
Region22:        7       Region23:       7
Region24:        7       Region25:       7
Region26:        7       Region27:       7
Region28:        7       Region29:       7
Region30:        7       Region31:       6
Region32:        130     Region33:       2
Region34:        0       Region35:       0
Region36:        0       Region37:       0
Region38:        0       Region39:       0
Region40:        0       Region41:       0
Region42:        0       Region43:       0
Region44:        0       Region45:       0
Region46:        0       Region47:       0
```

次に、リージョンでのマルチキャスト隣接割り当てを表示する例を示します。

```
Router#show mls cef adjacency region 22

Region22:
   Head:    1738B610, 16377, 360455
   Next:    1738B610, 16377, 360455
   Midptr:  0
   Limit:   16057
   Usage:   7
   Start:   360448
   End:     376831
   Size:    16384
   MidPt:   368476
   Search:  1
   Stats:   1
   BC[0]:  1
   BC[1]:  0
   BC[2]:  0
   BC[3]:  0
   BC[4]:  0
```

次に、マルチキャスト隣接内部の詳細を表示する例を示します。

```
Router#show mls cef adjacency internal

Alloc req:                  1506
Dealloc req:                1250
Invalid free:               0
Internal alloc fail:        0
Chunk malloc fail:          0
CCC notify:                 0
Num of region:              65
Num of mcast regions:       32
Num of stats regions:       32
Num no-stats regions:       32
Mcast start:                0
Mcast end:                  31
Stats start:                1
Stats end:                  31
No-stats start:             32
No-stats end:               63
ACL region num:             64
```

```
Stats adj req fails:        0
No-stats adj req fails:     0
Stats cur adj req fails:    0
No-stats cur adj req fails: 0
Mcast region req fails:     0
```

PFC の VPN スイッチング

ここでは、PFC の VPN スイッチングについて説明します。

- 「PFC の VPN スイッチングの動作」（P.26-15）
- 「MPLS VPN に関する注意事項および制約事項」（P.26-16）
- 「MPLS VPN でサポートされるコマンド」（P.26-17）
- 「MPLS VPN 設定例」（P.26-17）

PFC の VPN スイッチングの動作

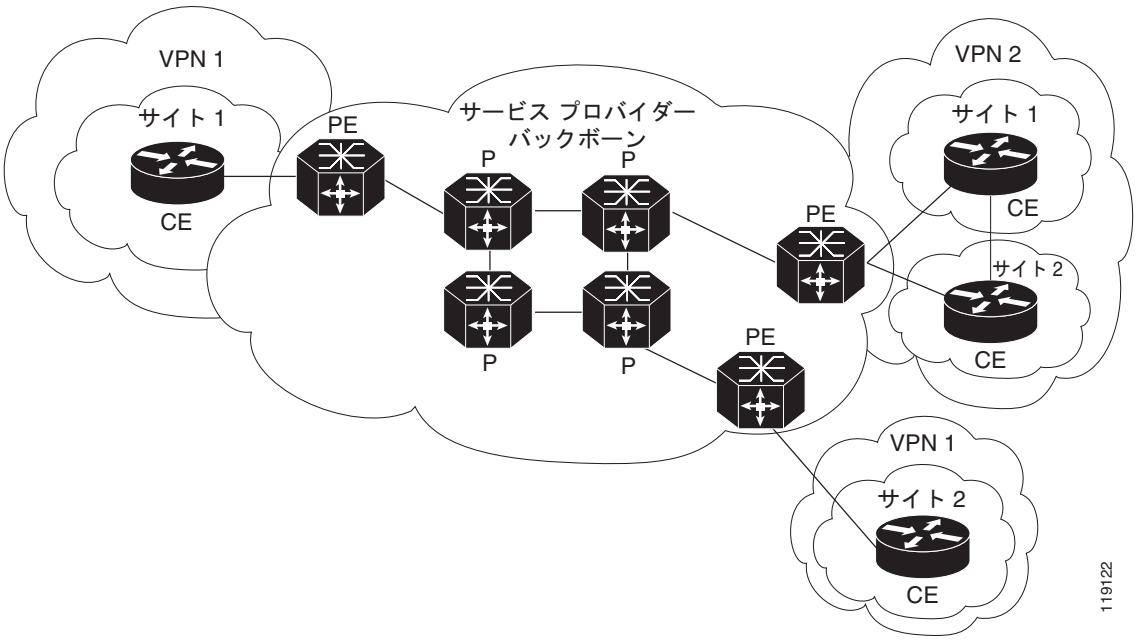
Cisco IOS ネットワークに MPLS の IP VPN 機能を使用すると、スケーラブルな IP レイヤ 3 VPN バックボーン サービスを、共有インフラストラクチャに配置された複数のサイトに導入し、同時にプライベート ネットワークと同じアクセスまたはセキュリティを提供できます。MPLS テクノロジーに基づいた VPN には、ルーティングの隔離、セキュリティの向上、ルーティングの簡素化およびスケーラビリティの向上が実現するという利点があります。

MPLS VPN の概念的な概要および設定の詳細については、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 26-3 に、一般的な MPLS VPN ネットワーク トポロジーを示します。

図 26-3　VPN およびサービス プロバイダー バックボーン



PFC 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。PFC には、VLAN を VPN にマッピングするテーブルが格納されています。Cisco 7600 シリーズ ルータの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 に対応付けられます。PFC 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 内のプレフィックスだけです。(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 ラベルが格納されます。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、そこで書き換えられて、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ッ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。プレフィックス単位のラベルが使用される場合、各 VPN プレフィックスには一意のラベルが対応付けられます。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）　PFC が割り当てるのは、VRF ごとに 1 つの集約ラベルだけです。

出力 PE で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ックスをこのラベルに対応付けることができます。この場合、PFC 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 検索には再循環が必要となる場合があります。

MPLS VPN に関する注意事項および制約事項

MPLS VPN を設定するときは、次の注意事項および制約事項に従ってください。

- PFC では、拡張 OSM でシャーシごとに合計 1024 個の VRF がサポートされます。非拡張 OSM を使用すると、システムのデフォルトは 511 個の VRF になります。
- PFC は、VPN 数が 511 を超えているときに VPN を再循環させます。

MPLS VPN でサポートされるコマンド

PFC では、次の MPLS VPN 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**

これらのコマンドの詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html

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/en/US/docs/ios/12_0st/12_0st21/feature/guide/fs_vpn.html

（注） 別の MPLS デバイスとのレイヤ 2 ポート ピアリングで 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する場合は、別のレイヤ 3 VLAN インターフェイスを VRF インターフェイスとして使用できます。

MPLS VPN 設定例

次の設定例は、LAN、OSM、および拡張 FlexWAN CE 方向インターフェイスを示しています。PFC MPLS スイッチング設定は、別のプラットフォームにおける設定と同じです。

```
!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

Any Transport over MPLS（AToM）は MPLS バックボーン上でレイヤ 2 パケットを転送します。AToM はエッジ ルータ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、転送が生じます。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）で接続を判別する逆多重化ラベルです。

AToM では、PFC において、次の類似転送タイプがサポートされます。

- Ethernet over MPLS（EoMPLS）（VLAN モードおよびポート モード）
- DLCI-to-DLCI 接続による Frame Relay over MPLS
- 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。

PFC では、ハードウェアベースの EoMPLS、および OSM ベースの EoMPLS または拡張 FlexWAN ベースの EoMPLS がサポートされます （Release 12.2SR では FlexWAN ベースの EoMPLS がサポートされません）。詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/docs/general/TD_Trash/lczaplys_trash/mpls.html#wp1128955

http://www.cisco.com/en/US/docs/general/TD_Trash/lczaplys_trash/mpls.html#wp1279824

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。

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.26-19）
- 「EoMPLS の概要」（P.26-19）
- 「EoMPLS に関する注意事項および制約事項」（P.26-20）
- 「EoMPLS の設定」（P.26-25）
- 「LAN カードにおける 7600-MUX-UNI サポートの設定」（P.26-32）

AToM ロード バランシング

PFC の EoMPLS では、トンネル入力でロード バランシングがサポートされません。複数の Interior Gateway Protocol（IGP）パスが使用可能でも、1 つの IGP パスだけが選択されますが、ロード バランシングは MPLS コアで使用可能です。

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

送が生じます。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）で接続を判別する逆多重化ラベルです。

EoMPLS は MPLS パケットに Ethernet 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転送されます。

（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 ベースまたは拡張 Flex WAN ベースの EoMPLS を使用してください。SVI で EoMPLS を設定する必要があり、コア方向カードは OSM モジュールまたは拡張 FlexWAN モジュールにする必要があります。ローカルなレイヤ 2 スイッチングが不要な場合は、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 EoMPLS を使用します。

EoMPLS に関する注意事項および制約事項

EoMPLS を設定するときは、次の注意事項および制約事項を考慮してください。

- 受信された最大のレイヤ 2 パケットを伝達できるように、エンドポイント間のすべての中間リンクの最大伝送単位（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 メンバーシップ情報を挿入する標準方式を確立します。
- VLAN ベース EoMPLS では、デフォルトを超える MTU サイズが物理インターフェイスに指定されている場合、VLAN サブインターフェイスの MTU サイズを 1500（デフォルト）より大きくする必要があります。

（注）　ポートチャネルと xconnect の組み合わせがポート ベースの EoMPLS 上でサポートされます。ただし、一般的な PFC ベースの EoMPLS に関するすべての制約事項がポートチャネルと xconnect にも適用されます。

- QoS がグローバルにディセーブルの場合、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の場合、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。新しいコマンドでは、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 PFC を設定できます。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 45 章「PFC QoS の設定」を参照してください。

（注）　PFC ベース EoMPLS サービスおよび PXF ベース EoMPLS サービスを同じシステムで使用する場合は、**no mls qos rewrite ip dscp** を使用しないでください。

- プライベート VLAN では、EoMPLS が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 ブリッジ プロトコル データ ユニット（BPDU）をサポートするには、Ethernet over MPLS VLAN 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。このようにすると、EoMPLS VLAN のカスタマー ルータ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。スケーラブル EoMPLS（SVI ベース EoMPLS）とポートモード EoMPLS の詳細とそのサンプル設定については、「スケーラブル EoMPLS とポートモード EoMPLS」（P.26-22）と「SwEoMPLS および VPLS のサンプル設定」（P.26-22）を参照してください。
- Cisco 7600 は、次の 3 種類の Ethernet over MPLS（EoMPLS）ソリューションを提供します。
  - ハードウェア ベース EoMPLS とも呼ばれる PFC ベース EoMPLS では、スーパーバイザまたは DFC ベースのラインカード上で Earl が実行されます。
  - ソフトウェア ベース EoMPLS とも呼ばれる LAN ベース EoMPLS では、MPLS コア対向ラインカード上で Earl が実行されます。
  - スケーラブル EoMPLS では、カスタマー デバイス対向ラインカード上で Earl が実行されます。この機能は、SIP400、ES20、および ES40 でカスタマー対向ラインカードとしてサポートされます。さらに、ES20 と ES40 では、このソリューションが EVC ベースの設定でのみサポートされます。
- PFC の場合、すべてのプロトコル（CDP、VTP、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、ISL カプセル化はサポートされません。
- インターフェイス間には一意の VLAN が必要です。異なるインターフェイスで同じ VLAN ID は使用できません。
- PE から PE へ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。
- PFC 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だけです。
- 旧リリースの AToM では、AToM 回路の設定に使用されるコマンドは **mpls l2 transport route** でした。このコマンドは、**xconnect** コマンドに置き換えられました。**xconnect** コマンドは、EoMPLS 回路を設定する場合に使用できます。
- AToM 制御ワードはサポートされていません。
- レイヤ 3 VLAN インターフェイスでは EoMPLS が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携します。

- ES20 など、一部の SPA ベース イーサネット ラインカードは、QinQ トラフィックで外部 VLAN のマッチングをサポートします。詳細については、関連するラインカードのマニュアルを参照してください。

スケーラブル EoMPLS とポートモード EoMPLS

スケーラブル EoMPLS シナリオでは、PE ルータの EVC 上で直接相互接続を設定することができます。ポートモード EoMPLS では、物理インターフェイスまたはサブインターフェイス上で相互接続を設定することができます。スケーラブル EoMPLS とポートモード EoMPLS では、アクセス対向インターフェイスがスパニングツリー プロトコル（STP）に参加しないため、スパニングツリーをディセーブルにする必要がありません。Cisco 7600 シリーズ ルータ上でのスパニングツリー プロトコル（STP）と Multiple Spanning Tree（MST）プロトコルの設定方法については、第 20 章「STP および MST の設定」を参照してください。

（注）　Cisco 7600 シリーズ ルータは複数のバックアップ PW をサポートしません。

イーサネット AC の HSPW サポート

Cisco IOS Release 15.1(01)S 以降、ホット スタンバイ疑似配線（HSPW）機能は、ScEoMPLS、ATM、および TDM の相互接続のアクセス側にインポジションおよびディスポジションを持つ ES+ ラインカードと SIP400 PW でサポートされます。ホット スタンバイ機能により、サービス プロバイダー ネットワーク内の PW のスイッチオーバー時間を短縮できます。この機能は、ハードウェアでバックアップ PW を事前にプログラミングされた状態に保ちます。またスイッチオーバーでは、バックアップ PW はトラフィック通過がイネーブルになっています。

次のセクションで、STP を処理し、BPDU の疑似回線経由の中継を可能にするサンプル設定とシナリオについて説明します。

SwEoMPLS および VPLS のサンプル設定

次に、SVI ベース EoMPLS とも呼ばれる SwEoMPLS 用のサンプル トポロジに関する例を示します。

CE1-----PE1-----P------PE2----CE2

SwEoMPLS では、SVI インターフェイス（インターフェイス VLAN）上で相互接続を設定します。次に、CE 対向インターフェイス上でのサンプル設定を示します。

```
interface FastEthernet1/13
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
end
```

次に、相互接続を使用した SVI インターフェイスのサンプル設定を示します。

```
interface Vlan110
no ip address
xconnect 6.6.6.6 200 encapsulation mpls
end
```

次に、P ルータ向けのコア対向ラインカード上でのサンプル設定を示します。

```
interface GigabitEthernet2/2/0
ip address 53.53.53.1 255.255.255.0
mpls ip
end
```

次に、VPLS 用の CE 対向ラインカード上でのサンプル設定を示します。

```
interface FastEthernet1/13
switchport switchport trunk encapsulation dot1q
switchport trunk allowed vlan 110
switchport mode trunk
end
```

次に、SVI 内部で相互接続が設定されている場合のサンプル設定を示します。

```
interface Vlan110
description VPLS
no ip address
xconnect vfi PE1-VPLS
end
```

これまでのサンプル設定に基づいて、VFI が定義されます。

```
l2 vfi PE1-VPLS manual
vpn id 110
neighbor 6.6.6.6 encapsulation mpls
```

次に、VFI 用の CE 対向ラインカード上でのサンプル設定を示します。

```
interface GigabitEthernet2/2/0
ip address 53.53.53.1 255.255.255.0
mpls ip
end
```

上記トポロジと設定では：

- カスタマー ルータの CE1 と CE2 はイーサネット接続を備えています。
- VLANS にタグ付けされたトラフィックが中継されます。
- CE1-CE2 トラフィックを PE1-PE2 で透過的に通過させるために、ルータの PE1 と PE2 間に EoMPLS 疑似配線が設置されます。

ブリッジ プロトコル データ ユニットを可能にするためのスパニングツリー プロトコルの管理

PE ルータ上のカスタマー対向インターフェイスは STP に参加します。EoMPLS クラウド（PE1-P-PE2）上でイーサネット スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）をサポートするには、下記方法を修正してスーパーバイザ エンジン スパニングツリーをディセーブルにします。

1. スパニングツリー モードが MST の場合は、STP BPDU からタグが外されます。

```
spanning-tree mode mst
```

PE ルータの CE 対向インターフェイス上では：

```
Int Gig 1/1
switchport
switchport trunk allowed vlan 110
switchport mode trunk
```

STP BPDU を中継するように VFI（ここでは mst-1）を設定します。

```
l2 vfi mst-1 manual
vpn id 1
forward permit l2protocol all
```

1 つ前の手順で設定した VFI を SVI に対応付けます。

```
interface Vlan1
no ip address
xconnect vfi mst-1
```

2. スパニングツリー モードが PVST の場合は、STP BPDU にタグが付けられます。たとえば、カスタマー ルータのトラフィックを VLAN110 で受信する場合は、BPDU に VLAN 110 のタグが付けられます。

```
spanning-tree mode pvst
```

アクセス対向インターフェイス上では：

```
Int Gig1/1
switchport
switchport trunk allowed vlan 110
switchport mode trunk
no spanning-tree vlan 110
```

上記シナリオの場合は、**no spanning-tree vlan 110** で十分であり、BPDU を中継するための特別な VFI が必要ありません。

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」（P.26-25）
- 「PFC モードの VLAN ベース EoMPLS の設定」（P.26-25）
- 「PFC のポートベース EoMPLS の設定」（P.26-29）

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 を通して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 ルータ間にラベル 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 Ethernet 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転送されます。PFC で EoMPLS を設定するには、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 トラフィックを転送します。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 がサブインターフェイス（VLAN）ベース 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、PFC の EoMPLS はインターフェイス間で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 設定または拡張 FlexWAN 設定、および PFC モード設定を同時にイネーブルにすることができます。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 または拡張 FlexWAN 対応インターフェイスを経由しない限り、OSM または拡張 FlexWAN ベース 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 または拡張 FlexWAN ベース EoMPLS に対応するパケットは廃棄されます。

PFC は、MPLS をサポートしています。PFC の場合、LAN ポートは、OSM または拡張 FlexWAN モジュールを使用せずに、レイヤ 2 トラフィックを受信したり、ラベルをインポーズしたり、MPLS コアにフレームを切り替えたりすることができます。

PFC では、MPLS ネットワークのコアに向けて OSM または拡張 FlexWAN モジュールを設定し、OSM 設定、拡張 FlexWAN 設定、または PFC モード設定のうちいずれかを使用できます。

EoMPLS over WAN（拡張 FlexWAN および OSM）の詳細については、次の資料を参照してください（Release 12.2SR では FlexWAN ベースの EoMPLS がサポートされません）。

http://www.cisco.com/en/US/docs/general/TD_Trash/lczaplys_trash/mpls.html#wp1128955

PFC モードの VLAN ベース EoMPLS の設定

PFC の VLAN ベース EoMPLS を設定するときは、次の注意事項および制約事項に従ってください。

- 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、およびラント 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。
- VLAN ベース EoMPLS はサブインターフェイスで設定する必要があります。また、デフォルトを超える MTU サイズが物理インターフェイスに指定されている場合、VLAN サブインターフェイスの MTU サイズを 1500（デフォルト）より大きくする必要があります。

PFC の VLAN ベース EoMPLS を設定するには、プロバイダー エッジ（PE）ルータ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)# 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 が稼働している 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なければなりません。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なくてもかまいません。
ステップ 4	`Router(config-if)# xconnect` *peer_router_id vcid* `encapsulation mpls`	接続回路を疑似配線 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、PFC の VLAN ベース EoMPLS 設定の例を示します。

```
!
interface GigabitEthernet6/4
xconnect 13.13.13.13 4 encapsulation mpls
no shut
!
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 デバイスのサブインターフェイスに設定されます。

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 ごとに 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 の 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：現在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：このラベルが付加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：この入ラベルによってスイッチングされるバイト数。
- Outgoing interface：このラベルが付加されたパケットが送信されるときに経由するインターフェイス
- Next Hop：出ラベルに割り当てられたネイバーの IP アドレス

- 現在ルーティング中の 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
```

PFC のポートベース EoMPLS の設定

PFC のポートベース EoMPLS を設定するときは、次の注意事項および制約事項に従ってください。

- 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、およびラント 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は、サブインターフェイスでのコマンド入力も不可能になります。

PFC 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 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`	接続回路を疑似配線 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 ごとに 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 の 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ことを確認するには、**show mpls forwarding-table** コマンドを使用します。

```
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：現在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：このラベルが付加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：この入ラベルによってスイッチングされるバイト数。

  - Outgoing interface：このラベルが付加されたパケットが送信されるときに経由するインターフェイス
  - Next Hop：出ラベルに割り当てられたネイバーの IP アドレス
- 現在ルーティング中の 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
```

LAN カードにおける 7600-MUX-UNI サポートの設定

User Network Interface（UNI）は、カスタマー エッジ（CE）機器が入力 PE に接続するポイントであり、接続 VLAN は UNI ポート上の VLAN です。

LAN カードにおける 7600-MUX-UNI サポート機能では、接続 VLAN の物理ポートを分割でき、複数のレイヤ 2 サービスおよびレイヤ 3 サービスが単一 UNI で提供されます。

LAN カードにおける 7600-MUX-UNI サポートの設定時には、次の注意事項および制約事項に従ってください。

- メイン インターフェイスにおけるカプセル化は、ISL ではなく、dot1Q にする必要があります。
- メイン インターフェイスで dot1q カプセル化を使用する場合は、サブインターフェイスで ISL を設定できません。レイヤ 3 インターフェイスは影響されません。

LAN カードにおける 7600-MUX-UNI サポートを設定するには、プロバイダー エッジ（PE）ルータ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)# interface type number`	設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。イーサネット ポートだけで有効です。
ステップ 3	`Router(config-if)# switchport`	レイヤ 3 モードのインターフェイスをレイヤ 2 コンフィギュレーションに対応するレイヤ 2 モードにします。
ステップ 4	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	802.1Q カプセル化をサポートするようにポートを設定します。 リンクの両端を同一カプセル化タイプで設定する必要があります。 **（注）** MUX-UNI サポートの有効な選択肢は dot1Q です。
ステップ 5	`Router(config-if)# switchport mode trunk`	VLAN トランクとしてポートを設定します。

ステップ 6	`Router(config-if)# switchport trunk allowed vlan vlan-list`	デフォルトでは、すべての VLAN が許可されます。VLAN を明示的に許可するには、このコマンドを使用します。vlan-list の有効な値は、1 ～ 4094 です。 （注）　メイン インターフェイスとサブインターフェイスの間で VLAN を重複して割り当てないでください。メイン インターフェイスとサブインターフェイスの間の VLAN 割り当ては、相互に排他的にする必要があります。
ステップ 7	`Router(config)# interface type slot/port.subinterface-number`	設定するサブインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。イーサネット ポートだけで有効です。
ステップ 8	`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 が稼働している 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なければなりません。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なくてもかまいません。
ステップ 9	`Router(config-if)# xconnect peer_router_id vcid encapsulation mpls`	接続回路を疑似配線 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、LAN カードにおける 7600-MUX-UNI サポート機能の例で、UNI として使用される物理トランク ポートを示します。

```
interface Fastethernet3/1
switchport
switchport encapsulation dot1q
switchport mode trunk
switchport trunk allowed VLAN 200-250

interface Fastethernet3/1.10
encap dot1q 3000
xconnect 10.0.0.1 3000 encapsulation mpls
```

次に、LAN カードにおける 7600-MUX-UNI サポート機能の例で、UNI として使用されるレイヤ 2 ポート チャネルを示します。

```
interface Port-channel100
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk allowed VLAN 100-200
    switchport mode trunk
    no ip address

interface Port-channel100.1
    encapsulation dot1Q 3100
    xconnect 10.0.0.30 100 encapsulation mpls
```

次に、LAN カードにおける 7600-MUX-UNI サポート機能の例で、Muxed UNI ポートのレイヤ 3 終端および VRF を示します。

```
Vlan 200, 300, 400
interface Fastethernet3/1
```

```
switchport
switchport encapsulation dot1q
switchport mode trunk
switchport trunk allowed VLAN 200-500

interface Fastethernet3/1.10
encap dot1q 3000
xconnect 10.0.0.1 3000 encapsulation mpls

interface Vlan 200
ip address 1.1.1.3

interface Vlan 300
ip vpn VRF A
ip address 3.3.3.1

interface Vlan 400
ip address 4.4.4.1
ip ospf network broadcast
mpls label protocol ldp
mpls ip
```

CHAPTER 27

IPv4 マルチキャスト VPN サポートの設定

この章では、Cisco 7600 シリーズ ルータにおいて IPv4 マルチキャスト Virtual Private Network（MVPN）サポートを設定する方法について説明します。MVPN がサポートされるのは、PFC3B、PFC3BXL、PFC3C、PFC3CXL のいずれかをルータにインストールしているときです。

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.27-1）
- 「MVPN 設定時の注意事項および制約事項」（P.27-7）
- 「MVPN の設定」（P.27-8）

MVPN の機能概要

ここでは MVPN について説明します。

- 「MVPN の概要」（P.27-2）
- 「マルチキャスト ルーティング、転送、マルチキャスト ドメイン」（P.27-2）
- 「マルチキャスト配信ツリー」（P.27-2）
- 「Multicast Tunnel Interface」（P.27-5）
- 「MVPN の PE ルータ ルーティング テーブルのサポート」（P.27-6）
- 「Multicast Distributed Switching サポート」（P.27-6）
- 「ハードウェア処理の IPv4 マルチキャスト」（P.27-7）

MVPN の概要

MVPN は規格に基づいた機能であり、IPv4 マルチキャスト トラフィックが MPLS VPN クラウドで送信されます。Cisco 7600 シリーズ ルータの MVPN では IPv4 マルチキャスト トラフィックの既存 PFC ハードウェア サポートを使用して、ワイヤ速度で VPN 上でマルチキャスト トラフィックが転送されます。MVPN では、レイヤ 3 IPv4 VPN 上における IPv4 マルチキャスト トラフィックのサポートが、既存の IPv4 ユニキャスト サポートに追加されます。

MVPN では、VPN ルーティングおよび転送（VRF）インスタンスごとにマルチキャスト パケットのルーティングおよび転送が行われ、サービス プロバイダー バックボーンを横断して VPN トンネルでマルチキャスト パケットが送信されます。

MVPN は IP-in-IP 総称ルーティング カプセル化（GRE）トンネルの代替策です。GRE トンネルは容易にスケールできるソリューションではなく、カスタマーに提供される粒度に制限されます。

マルチキャスト ルーティング、転送、マルチキャスト ドメイン

MVPN では、VPN ルーティング/転送テーブルにマルチキャスト ルーティング情報が追加されます。プロバイダー エッジ（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カスタマー エッジ（CE）ルータから受信すると、マルチキャスト VRF（MVRF）の情報に従って転送が実行されます。

（注）　MVRF は、VRF-Lite 上のマルチキャストとも一般的に呼ばれます。

それぞれの MVRF では、特定 VRF インスタンスに必要となるルーティング情報および転送情報が維持されます。MVRF の作成と設定は既存 VRF と同じ方法で行われますが、それぞれの MVRF ではマルチキャスト ルーティングもイネーブルになります。

マルチキャスト ドメインは、MPLS ネットワークで相互にマルチキャスト トラフィックを送信できるホストのセットで構成されます。たとえば、特定タイプのマルチキャスト トラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャスト ドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

マルチキャスト配信ツリー

MVPN 機能では、最低でも 1 つのマルチキャスト配信ツリー（MDT）がマルチキャスト ドメインごとに確立されます。MDT では、さまざまな PE ルータに存在する同一 MVRF の相互接続に必要となる情報が提供されます。

MVPN では、次の 2 つの MDT タイプがサポートされます。

- デフォルト MDT：特定マルチキャスト ドメインのすべての PE ルータ間における PIM 制御メッセージおよび低帯域幅ストリームの永続チャネルです。デフォルト MDT におけるすべてのマルチキャスト トラフィックは、ドメインのその他すべての PE ルータに複製されます。各 PE ルータは、ドメインのその他すべての PE ルータから、論理的に PIM ネイバー（1 ホップ先）と見なされます。
- データ MDT：これはオプションです。イネーブルにするとダイナミックに作成され、フルモーション ビデオなど、すべての PE ルータに送信する必要がない高帯域幅送信用に最適なパスが提供されます。これにより、PE ルータ間において高帯域幅トラフィックのオンデマンド転送が可能になるので、作成されるすべての高帯域幅ストリームですべての PE ルータがフラッディングされなくなります。

データ MDT を作成するため、バックボーンにマルチキャスト ストリームを定期的に転送する各 PE ルータは、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定期的に検査します。

1. 各 PE ルータはマルチキャスト トラフィックを定期的にサンプル抽出して（ソフトウェア スイッチングの場合は約 10 秒ごと、ハードウェア スイッチングの場合は 90 秒ごと）、マルチキャスト ストリームが設定しきい値を超えているかどうかを判断します。（ストリームのサンプル抽出タイミングにより、最悪の場合は、高帯域幅ストリームが検出されるまでに最大 180 秒かかることがあります）。

（注）　データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルート エントリ専用に作成されます。（*,G）エントリ用には作成されません。

2. 特定マルチキャスト ストリームが定義済みしきい値を超えた場合、送信側 PE ルータは、その特定マルチキャスト トラフィック用にデータ MDT をダイナミックに作成します。
3. 送信側 PE ルータは、その他の PE ルータに DATA-MDT JOIN 要求（ポート 3232 へのユーザ データグラム プロトコル（UDP）メッセージ）を送信し、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 テーブルを調べて、このデータ ストリームの受信に関係するカスタマーがいるかどうかを判断します。そのようなカスタマーがいる場合、受信側 PE ルータは PIM プロトコルを使用し、この特定データ MDT グループの PIM JOIN メッセージ（グローバル テーブル PIM インスタンス）を送信してストリームを受け入れます。このストリームのカスタマーがいないルータは、カスタマーがあとでそのストリームを要求したときのため、情報をキャッシュします。
5. 送信側 PE ルータは、DATA-MDT JOIN メッセージ送信の 3 秒後、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、新しいデータ MDT で送信し始めます。
6. 送信側 PE ルータは、マルチキャスト ストリームが定義済みしきい値を超え続ける限り、60 秒ごとに DATA-MDT JOIN メッセージの送信を続けます。ストリームが 60 秒より長くしきい値を下回った場合、送信側 PE ルータは DATA-MDT JOIN メッセージの送信を停止し、ストリームをデフォルト MDT に戻します。
7. 受信側ルータは、3 分より長く DATA-MDT JOIN メッセージを受信しなかった場合、デフォルト MDT のキャッシュ情報と期限切れにします。

データ MDT では高帯域幅の送信元が VPN 内部で許可されますが、MPLS VPN コアでの最適トラフィック転送が確保されます。

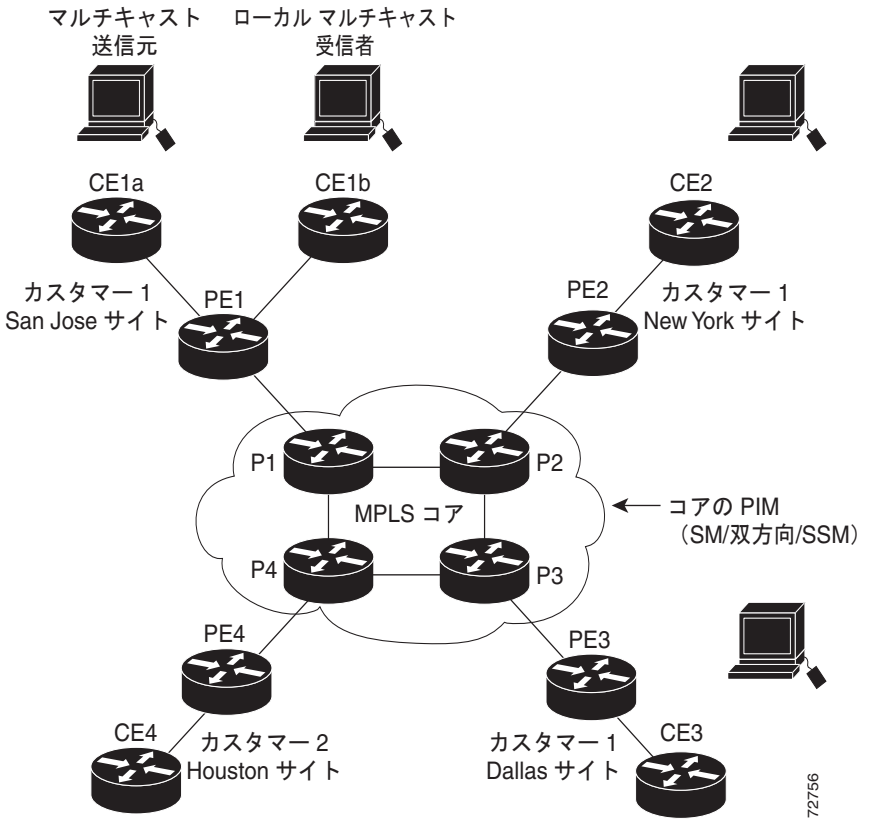
（注）　DATA-MDT JOIN メッセージとその他のデータ MDT 作成および使用法に関する技術情報については、Eric C. Rosen らによる インターネット ドラフト『*Multicast in MPLS/BGP IP VPNs*』を参照してください。

次の例のサービス プロバイダーには、San Jose、New York、Dallas にオフィスがあるマルチキャスト カスタマーがいます。San Jose サイトは、単方向マルチキャスト プレゼンテーションを送信しています。サービス プロバイダー ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズの顧客の Houston サイトがサポートされます。

エンタープライズの顧客のデフォルト MDT は、プロバイダーのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は、MPLS コアのその他のルータに相互接続されていますが、別のカスタマーと関連しているので、デフォルト MDT の一部ではありません。

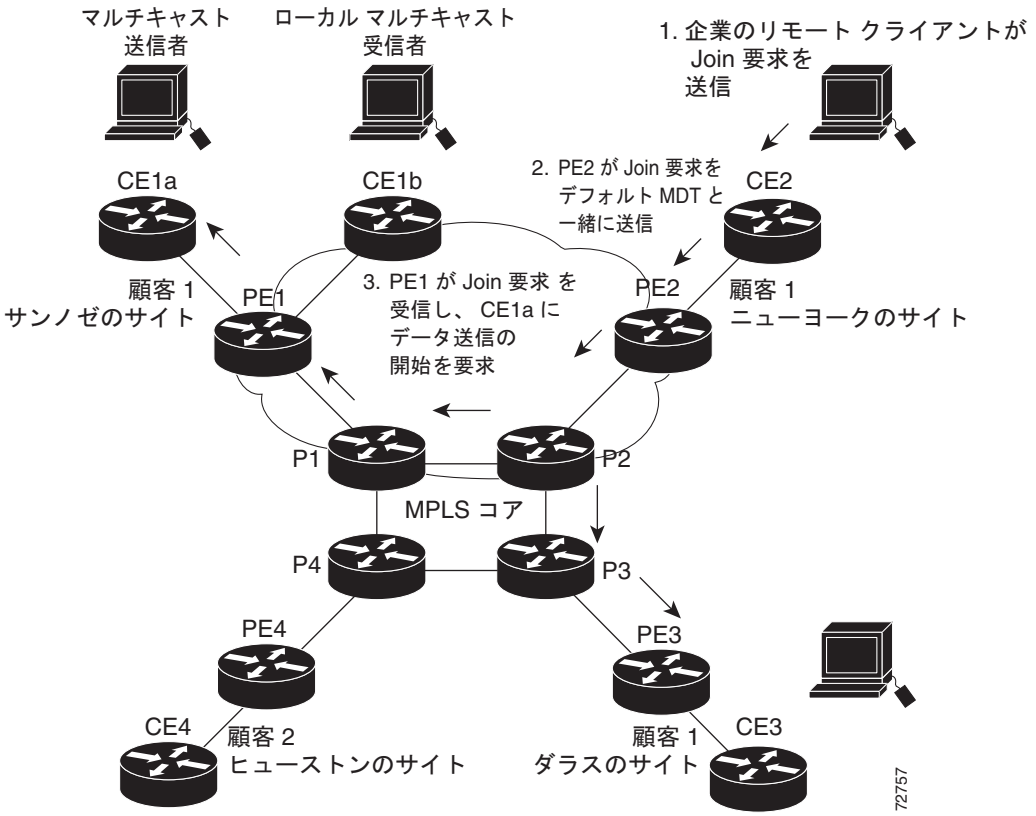
図 27-1 は、San Jose の外側でマルチキャスト ブロードキャストに加入するユーザがいない場合、つまりデフォルト MDT でデータが流れない場合のネットワークの状況を示しています。各 PE ルータはデフォルト MDT 上にあるその他の PE ルータとの PIM 関係を維持し、直接接続している PE ルータとの PIM 関係も維持します。

図 27-1　デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入した場合、ニューヨーク サイトに関連する PE ルータは加入要求を送信します。この加入要求は、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）と関連する PE ルータは、この要求を受信します。図 27-2 は、PE ルータが、マルチキャスト送信元（CE1a）と関連する CE ルータに要求を転送する方法を示しています。

図 27-2　データ MDT の初期化



CE ルータ（CE1a）は関連 PE ルータ（PE1）にマルチキャスト データを送信し始め、PE ルータは、マルチキャスト データが帯域幅しきい値を超えているためにデータ MDT を作成する必要があることを認識します。PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用してすべてのルータにメッセージを送信します。

約 3 秒後、PE1 は、データ MDT を使用してその特定ストリームのマルチキャスト データを送信し始めます。この送信元に関係するレシーバは PE2 だけにいるので、PE2 だけがデータ MDT に加入してデータ MDT でトラフィックを受信します。

Multicast Tunnel Interface

PE ルータは、マルチキャスト ドメインのマルチキャスト VRF Multicast VRF（MVRF）ごとに Multicast Tunnel Interface（MTI）を作成します。MVRF はトンネル 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、MVRF とグローバル MVRF を接続するコンジットを提供します。

ルータの場合、MTI はクラス D マルチキャスト アドレスを含むトンネル インターフェイスです（**interface tunnel** コマンドで作成）。この MVRF 用にデフォルト MDT で設定したすべての PE ルータは論理ネットワークを作成し、この論理ネットワークでは、各 PE ルータが、マルチキャスト ドメインにあるその他すべての PE ルータの PIM ネイバー（1 ホップ先）として表示されます。この場合、各ルータ間の物理的な距離は関係ありません。

MVRF を設定すると、MTI は自動的に作成されます。BGP 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 プロトコルは各 MTI で自動的にイネーブルになります。

ルータは、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、受信する MVRF 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。ルータは、パケットをカプセル化するとき、送信元アドレスを BGP ピアリング インターフェイスの送信元アドレスに、デフォルト MDT のマルチキャスト アドレス、またはデータ MDT の送信元アドレス（設定されている場合）に宛先アドレスを設定します。次にルータは、適切な数の MTI インターフェイスで転送するために、必要に応じてパケットを複製します。

ルータは、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、適切な MVRF を識別します。次にパケットのカプセル化を解除し、必要なだけ複製して適切なインターフェイスに転送します。

（注）
- MVPN MTI は、Cisco ルータで一般的に使用されるその他のトンネル インターフェイスと異なり、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可能でありませんが、**show interface tunnel** コマンドを使用してそのステータスを表示できます。
- MTI インターフェイスは、VPN トンネル上のマルチキャスト トラフィックに排他的に使用されます。
- このトンネルは、ユニキャストでルーティングされたトラフィックを搬送しません。

MVPN の PE ルータ ルーティング テーブルのサポート

MVPN フィーチャをサポートする各 PE ルータは、次のルーティング テーブルを使用して、VPN トラフィックおよび MVPN トラフィックを正しくルーティングします。

- デフォルト ルーティング テーブル：すべての Cisco 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、および MPLS 以外の VPN ユニキャスト トラフィックとマルチキャスト トラフィック（総称ルーティング カプセル化（GRE）マルチキャスト トラフィックを含む）に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：VRF インスタンスごとに作成されるルーティング テーブル。MPLS ネットワークの VPN 間でユニキャスト トラフィックをルーティングします。
- マルチキャスト VRF（MVRF）テーブル：VRF インスタンスごとに作成されるマルチキャスト 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 ドメインでマルチキャスト トラフィックをルーティングします。このテーブルには、マルチキャスト ドメインへのアクセスに使用される Multicast Tunnel Interface も含まれます。

Multicast Distributed Switching サポート

MVPN では、インターフェイス単位および VRF 単位でマルチキャストをサポートするため、Multicast Distributed Switching（MDS）がサポートされます。MDS を設定するときには、ループバック インターフェイスも含めたすべてのインターフェイスに **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

PFC では、VPN トラフィック上の IPv4 マルチキャスト用にハードウェア アクセラレーションがサポートされ、MSFC3 CPU の使用率を上げずにワイヤ速度で適切な VPN にマルチキャスト トラフィックが転送されます。

カスタマー VRF の場合は、PFC ハードウェア アクセラレーションにより、PIM dense（密）モード、PIM sparse（疎）モード、PIM 双方向モード、PIM Source Specific Multicast（SSM; 送信元固有マルチキャスト）モードのマルチキャスト トラフィックがサポートされます。

サービス プロバイダー コアの場合は、PFC ハードウェア アクセラレーションにより、PIM sparse モード、PIM 双方向モード、PIM SSM モードでマルチキャスト トラフィックがサポートされます。サービス プロバイダー コアの場合は、PFC ハードウェア アクセラレーションは PIM デンス モードでマルチキャスト 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 を設定する場合は、次の注意事項および制約事項に従ってください。

- Cisco 7600 シリーズ ルータで MVPN を実行するには、PFC3B、PFC3BXL、PFC3C、PFC3CXL のいずれかをインストールする必要があります。
- マルチキャスト ドメインのすべての PE ルータでは、MVPN 機能をサポートする Cisco IOS ソフトウェア イメージを実行する必要があります。P ルータおよび CE ルータには、MVPN をサポートするための要件がありません。
- すべてのバックボーン ルータでは、IPv4 マルチキャスト トラフィックのサポートもイネーブルにする必要があります。
- 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では、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロトコルを設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。
- MVPN を設定した場合は、入力複製だけがサポートされます。出力複製用にルータを設定している場合は、最初の MVRF を設定したとき、強制的に入力複製になります。
- ルータが PE として動作しており、存続可能時間（TTL）値が 2 であるカスタマー ルータからマルチキャスト パケットを受信した場合、そのパケットは、カプセル化されて MVPN リンクを横断して転送される代わりにドロップされます。MVPN リンクの反対側の PE がこのようなパケットを正常にドロップするので、トラフィック フローは影響されません。
- コア マルチキャスト ルーティングが SSM を使用する場合は、データ マルチキャスト配信ツリー（MDT）グループおよびデフォルト マルチキャスト配信ツリー（MDT）グループを IPv4 アドレスの SSM 範囲内で設定する必要があります。
- BGP ピアリングの更新送信元インターフェイスは、ルータで設定されているすべての BGP ピアリングで同一でないと、デフォルト MDT は適切に設定されません。BGP ピアリングにループバック アドレスを使用する場合は、ループバック アドレスで PIM スパース モードをイネーブルにする必要があります。
- 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 **ip mroute-cache** コマンドをイネーブルにしないと、分散マルチキャスト スイッチングは、それをサポートするプラットフォームで機能しません。**no ip mroute-cache** コマンドは、これらのインターフェイスでは使用 *できません*。

- デンス モード マルチキャスト フローにはフラッディングとプルーニングという性質があり、データ MDT の周期的な始動および分解という結果になるので、データ MDT は VRF PIM デンス モード マルチキャスト ストリームで作成されません。
- 送信元情報が使用できないので、VRF PIM 双方向モードではデータ MDT が作成されません。
- MVPN では複数の BGP ピアリング更新送信元がサポートされず、これを設定すると、MVPN RPF チェックが中断することがあります。MVPN トンネルの送信元 IPv4 アドレスは、BGP ピアリング更新送信元に使用される最高の IPv4 アドレスによって決まります。この IPv4 アドレスが、リモート PE ルータを含む BGP ピアリング アドレスとして使用される IPv4 アドレスでない場合、MVPN は適切に機能しません。
- MDT トンネルではユニキャスト トラフィックが搬送されません。
- MVPN は MPLS VPN ネットワークのインフラストラクチャを使用しますが、MPLS タグやラベルは、VPN 上のマルチキャスト トラフィックに適用できません。
- デフォルト MDT で設定されている各 MVRF は、ユーザに表示される外部 VLAN に加えて、3 つの非表示 VLAN（カプセル化、カプセル化解除、インターフェイスに 1 つずつ）を使用します。つまり各ルータでは、絶対最大値の 1,000 MVRF がサポートされます（MDT が設定されていない MVRF では 1 つの内部 VLAN が使用されるので、未使用 MVRF を削除して VLAN 割り当てを維持する必要があります）。
- MVPN では MPLS が使用されるので、MVPN では RPR および RPR+ の冗長モードだけがサポートされます。MPLS は Stateful Switchover（SSO）冗長モードの Nonstop Forwarding（NSF）と共存できますが、ステートフル MPLS スイッチオーバーはサポートされません。
- MPLS VPN ネットワークに VRF のネットワークがすでに含まれている場合は、そのネットワークを削除したり再作成したりしなくても、MVRF トラフィックをサポートできます。その代わりに次の手順に示すように **mdt default** コマンドおよび **mdt data** コマンドを設定し、VRF 上でマルチキャスト トラフィックをイネーブルにしてください。
- マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。
- 特定 VPN 接続をサポートする各 PE ルータでは、同一 MVRF を設定する必要があります。
- 特定 MVRF をサポートする各 PE ルータは、同じ **mdt default** コマンドで設定する必要があります。
- Cisco IOS Release 15.0(1)S では、Cisco 7600 シリーズ ルータで MVPN が設定されている場合、出力および入力レプリケーション モードがサポートされています。ルータは、入力または出力レプリケーション モードに設定できます。
- ネイティブ マルチキャストに対してサポートされている最大スケールは 20k です。

MVPN の設定

ここでは、MVPN の設定手順について説明します。

- 「出力および入力マルチキャスト レプリケーション モードの設定」（P.27-9）
- 「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.27-10）
- 「マルチキャスト VRF ルーティングの設定」（P.27-16）
- 「MVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定」（P.27-21）

（注）　この設定タスクでは、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で BGP がすでに設定されていて動作していることを想定しています。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

出力および入力マルチキャスト レプリケーション モードの設定

出力または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、次のコマンドを使用します。

	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)# **ip multicast hardware-switching replication-mode** {**egress** | **ingress**} または	入力マルチキャスト レプリケーション モードを設定し、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（デフォルトではイネーブル）。
	Router(config)# **no ip multicast hardware-switching replication-mode** {**egress** | **ingress**}	システムを自動検出モードに戻します。
ステップ 3	Router(config)# **show platform software multicast ip capability**	設定を確認します。

次に、入力レプリケーション モードが出力レプリケーション モードにされた場合の実行コンフィギュレーションのサンプル出力を示します。

```
Router(config)# ip multicast hardware-switching replication-mode ingress
Warning: This command will change the replication mode for all address families.

Router(config)# do sh runn | i ingress
ip multicast hardware-switching replication-mode ingress
ipv6 multicast hardware-switching replication-mode ingress

Router(config)# ip multicast hardware-switching replication-mode egress
Warning: This command will change the replication mode for all address families.
Warning: Egress replication-mode forced by CLI in presence of an egress-incapable card
*Apr 19 05:07:30.180: %CONST_MFIB_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change
Detected.
Current system replication mode is Egress

Router(config)# do sh runn | i egress
ip multicast hardware-switching replication-mode egress
```

次に、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 platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
```

現在のレプリケーション モードが出力である場合、またはいずれかのスイッチング モジュールで出力レプリケーション モードが可能になっている場合は、スケジュールされているメンテナンス期間中に入力レプリケーション モードを設定し、カスタマー トラフィックの混乱を最低限に抑えてください。

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)# ip multicast hardware-switching replication-mode {egress | 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、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（デフォルトではイネーブル）。
	`Router(config)# no ip multicast hardware-switching 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)# show platform software multicast ip capability`	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、設定を確認する例を示します。

```
Router(config)# ip multicast hardware-switching replication-mode ingress
Router(config)# show platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
Router#
```

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、マルチキャスト トラフィックの送受信を行う特定 VPN 接続ごとに、トラフィックを処理する各 PE ルータでそれぞれの VPN 接続用にマルチキャスト VPN ルーティング/転送（MVRF）インスタンスを設定する方法について説明します。

- 「VRF エントリの設定」（P.27-11）
- 「ルート識別子の設定」（P.27-11）
- 「ルートターゲット拡張コミュニティの設定」（P.27-12）
- 「デフォルト MDT の設定」（P.27-12）
- 「データ MDT の設定（任意）」（P.27-13）
- 「データ MDT ロギングのイネーブル化」（P.27-14）
- 「設定例」（P.27-14）
- 「VRF 情報の表示」（P.27-14）

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 エントリおよびシスコ エクスプレス フォワーディング（CEF）テーブル エントリを設定し、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、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 プレフィッ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。

ルート識別子の設定時には、次のうちいずれかの形式でルート識別子を入力してください。

- 16 ビット AS 番号：32 ビット番号（101:3）
- 32 ビット IPv4 アドレス：16 ビット番号（192.168.122.15:1）

次に、ルート識別子として 55:1111 を設定し、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`	ルートターゲット拡張コミュニティを VRF 用に設定します。
	`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の設定時には、次に注意してください。

- **import**：ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
- **export**：ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。
- **both**：インポートおよびエクスポートを行います。
- *route_target_ext_community*：48 ビット ルートターゲット拡張コミュニティを VRF に追加します。次のうちいずれかの形式で数値を入力してください。
  - 16 ビット AS 番号：32 ビット番号（101:3）
  - 32 ビット IPv4 アドレス：16 ビット番号（192.168.122.15:1）

次に、インポートおよびエクスポートの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、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 の設定時には、次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。このアドレスは MVRF コミュニティの識別子として動作します。この同一グループ アドレスで設定したすべてのプロバイダー エッジ（PE）ルータはグループのメンバーになり、メンバーは、グループの他のメンバーが送信した PIM 制御メッセージおよびマルチキャスト トラフィックを受信します。
- これと同じデフォルト MDT を各 PE ルータで設定しないと、PE ルータは、この特定 MVRF のマルチキャスト トラフィックを受信できません。

次に、デフォルト MDT として 239.1.1.1 を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）マルチキャスト アドレスの指定範囲にデータ MDT を設定します。
Router(config-vrf)# **no mdt data**	データ MDT を削除します。

任意のデータ MDT の設定時には、次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 の範囲にすることができますが、デフォルト MDT に割り当てたアドレスと重複させることはできません。
- *wildcard_bits*：可能なアドレスの範囲を作成するため、マルチキャスト グループ アドレスに適用するワイルドカード 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）しきい値をキロビット単位で定義します。このしきい値を超えると、マルチキャスト トラフィックはデフォルト MDT からデータ MDT に切り替わります。*threshold_value* パラメータの範囲は 1 ～ 4294967 キロビットです。
- **list** *access_list*：（任意）このトラフィックに適用するアクセス 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 ロギングのイネーブル化

データ MDT ロギ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-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 が頻繁に再利用される場合は、**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、データ MDT の許可数を増やす必要があります。
`Router(config-vrf)# no log-reuse`	データ MDT ロギングをディセーブルにします。

次に、データ MDT ロギングをイネーブルにする例を示します。

```
Router(config-vrf)# mdt log-reuse
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲の典型的な VRF 設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
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

ルータで設定されているすべての 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 用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、このコマンドの典型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 インターフェイスの IPv4 アドレスは、MVRF のデフォルト MDT のマルチキャスト グループ アドレスです。

特定の VRF に関するエントリを表示するには、**show platform software multicast ip vrf** コマンドを使用します。次に、このコマンドの典型的な出力例を示します。

```
Router# show platform software multicast ip vrf

  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 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 MVRF のマルチキャスト ルーティング テーブルおよびトンネル 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 の典型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** コマンドによって、VRF が使用している MDT Tunnel Interface（MTI）が Tunnel1 であることが示されます。

マルチキャスト VRF ルーティングの設定

ここでは、MVPN をサポートするマルチキャスト ルーティングの設定方法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.27-17）
- 「IPv4 マルチキャスト VRF ルーティングのイネーブル化」（P.27-17）
- 「PIM VRF 登録メッセージ送信元アドレスの設定」（P.27-18）
- 「PIM VRF ランデブー ポイント（RP）アドレスの指定」（P.27-18）
- 「Multicast Source Discovery Protocol（MSDP）ピアの設定」（P.27-19）
- 「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.27-19）
- 「マルチキャスト ルートの最大数の設定」（P.27-20）
- 「設定例」（P.27-20）
- 「IPv4 マルチキャスト VRF ルーティング情報の表示」（P.27-21）

（注）　マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

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ときは、次の情報に注意してください。

- *vrf_name*：マルチキャスト ルーティングの特定 VRF を指定します。*vrf_name* には、「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.27-10）で指定したように、以前作成した VRF を指定する必要があります。
- **distributed**：（任意）Multicast Distributed Switching（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 登録メッセージ送信元アドレスの設定

PIM VRF 登録メッセージ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 登録メッセージ送信元アドレスを設定します。登録メッセージの送信元としてループバック インターフェイスを設定できます。
`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 登録メッセージ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]`	PIM RP IPv4 アドレスを指定します（スパース PIM ネットワークの場合必須）。
`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 アドレスの指定時には、次の情報に注意してください。

- **vrf** *vrf_name*：（任意）使用する特定 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 アドレスが競合する場合は、この特定 RP により、Auto-RP で学習した RP を上書きします。
- **bidir**：（任意）*access_list* 引数で指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定しない場合、グループは PIM スパース モードで動作します。
- できるだけ双方向モードを使用してください。拡張性がより適切になります。

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 Souce 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 ピアの設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：使用する特定 VRF インスタンスを指定します。
- {*peer_name* | *peer_address*}：MSDP ピア ルータのドメイン ネーム システム（DNS）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るインターフェイスのインターフェイス名および番号。
- **remote-as** *ASN*：（任意）MSDP ピアの自律システム番号。これは表示専用です。

次に、MSDP ピアを設定する例を示します。

```
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ときは、次の情報に注意してください。

- **vrf** *vrf_name*：指定した VRF にバッファが割り当てられます。
- **rtp**：（任意）Real-Time Transport Protocol（RTP）ヘッダーもキャッシュします。
- バッファは **show ip mpacket** コマンドで表示できます。

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]`	設定されているルートの最大数をクリアします。

ルートの最大数の設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：指定した 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 ルートの数。範囲は 1 ～ 2147483647 であり、デフォルトは 2147483647 です。
- *threshold*：（任意）警告メッセージが発生する前に追加できるマルチキャスト ルートの数。有効範囲は、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 リストで 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* パラメータは、アクセス リストの名前または番号にすることができます。
`Router(config)# no ip multicast mrinfo-filter`	設定されている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
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲でマルチキャスト ルーティングをサポートするために必要となる最低限の設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
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 MVRF の既知の PIM ネイバーを表示するには、**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方法について説明します。

- 「マルチキャスト ルーティング設定の概要」（P.27-21）
- 「インターフェイスでの PIM の設定」（P.27-22）
- 「IPv4 VRF 転送用インターフェイスの設定」（P.27-23）
- 「設定例」（P.27-23）

マルチキャスト ルーティング設定の概要

IPv4 マルチキャスト トラフィック用に使用されているすべてのインターフェイスでは、Protocol Independent Multicast（PIM）を設定する必要があります。VPN マルチキャスト環境では、最低でも次のインターフェイスのすべてで 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 ピアリングに使用されているループバック インターフェイス。
- スパース 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ているループバック インターフェイス。

マルチキャスト トラフィックを転送する予定のインターフェイスと MVRF を関連付ける必要もあります。

マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

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の PIM の設定時には、次の情報に注意してください。

- 次のうちいずれかのインターフェイス タイプを使用できます。
  - 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 ピアリングに使用されているループバック インターフェイス。
  - sparse PIM ネットワーク Rendezvous Point（RP; ランデブー ポイント）アドレスの送信元として使用されているループバック インターフェイス
- PIM モードは次のとおりです。
  - **dense-mode**：動作のデンス モードをイネーブルにします。
  - **sparse-mode**：動作のスパース モードをイネーブルにします。
  - **sparse-dense-mode**：マルチキャスト グループで RP ルータが定義されている場合はスパース モード、RP ルータが定義されていない場合はデンス モードをイネーブルにします。
- バックボーンに接続されているすべての PE ルータの物理インターフェイス、および BGP ピアリングに使用されるか RP アドレス指定の送信元として使用されるすべてのループバック インターフェイスには、**sparse-mode** を使用してください。

次に、物理インターフェイス上で PIM スパース モードを設定する例を示します。

```
Router# configure terminal
interface gigabitethernet 10/1
Router(config-if)# ip pim sparse-mode
```

次に、ループバック インターフェイス上で PIM スパース 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 テーブルおよび転送テーブルをインターフェイスと関連付けます。指定しない場合、インターフェイスのデフォルトはグローバル ルーティング テーブルの使用になります。 **（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てください。
`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、VRF blue 転送用インターフェイスを設定する例を示します。

```
Router(config-if)# ip vrf forwarding blue
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、単一 MVRF 上でマルチキャスト トラフィックをイネーブルにするインターフェイス設定、および関連 MVRF 設定を示しています。

```
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 の設定例

ここには、次の MVPN 機能の設定例が含まれています。

- 「デフォルト MDT だけの MVPN 設定」（P.27-24）
- 「デフォルト MDT およびデータ MDT を含む MVPN 設定」（P.27-25）

デフォルト MDT だけの MVPN 設定

次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 設定に関連する行を示しています。（必須 BGP 設定は表示されていません）。

```
!
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
ip multicast hardware-switching 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 およびデータ MDT を含む MVPN 設定

次の設定例には、デフォルト MDT とデータ MDT の両方で設定された 3 つの MVRF が含まれています。MVPN 設定に関連する設定だけを表示しています。

```
...
!
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
ip multicast hardware-switching 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 28

マルチキャスト VPN エクストラネット サポートの設定

この章では、Cisco 7600 シリーズ ルータにおいて 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）エクストラネット サポートを設定する方法について説明します。MVPN がサポートされるのは、PFC3B、PFC3BXL、PFC3C、PFC3CXL のいずれかをルータにインストールしているときです。

この章の内容は、次のとおりです。

- 概要
- エクストラネット MVPN アーキテクチャ
- MVPN エクストラネットの設定
- 制約事項および使用上の注意事項

概要

エクストラネットは、外部ユーザに組織のイントラネットへのアクセスを許可するバーチャル プライベート ネットワークです。外部ユーザは、その組織のビジネス パートナー、カスタマー、サプライヤである可能性があります。MVPN エクストラネット機能により、サービス プロバイダーは、ある企業サイトから他の企業サイトへ、あるいは異なる VRF 設定間で送信されたマルチキャスト コンテンツを配信できます。これにより、異なる非公開ユーザ グループが、複数の VPN カスタマー間でマルチキャスト情報を共有できます。この機能により、サービス プロバイダーは、企業間のビジネス パートナーシップの実現に役立つ高度で柔軟なエクストラネット サービスを提供できます。MVPN エクストラネット機能を使用すると、サービス プロバイダーは次のものに対して効率的なコンテンツ配信を提供できます。

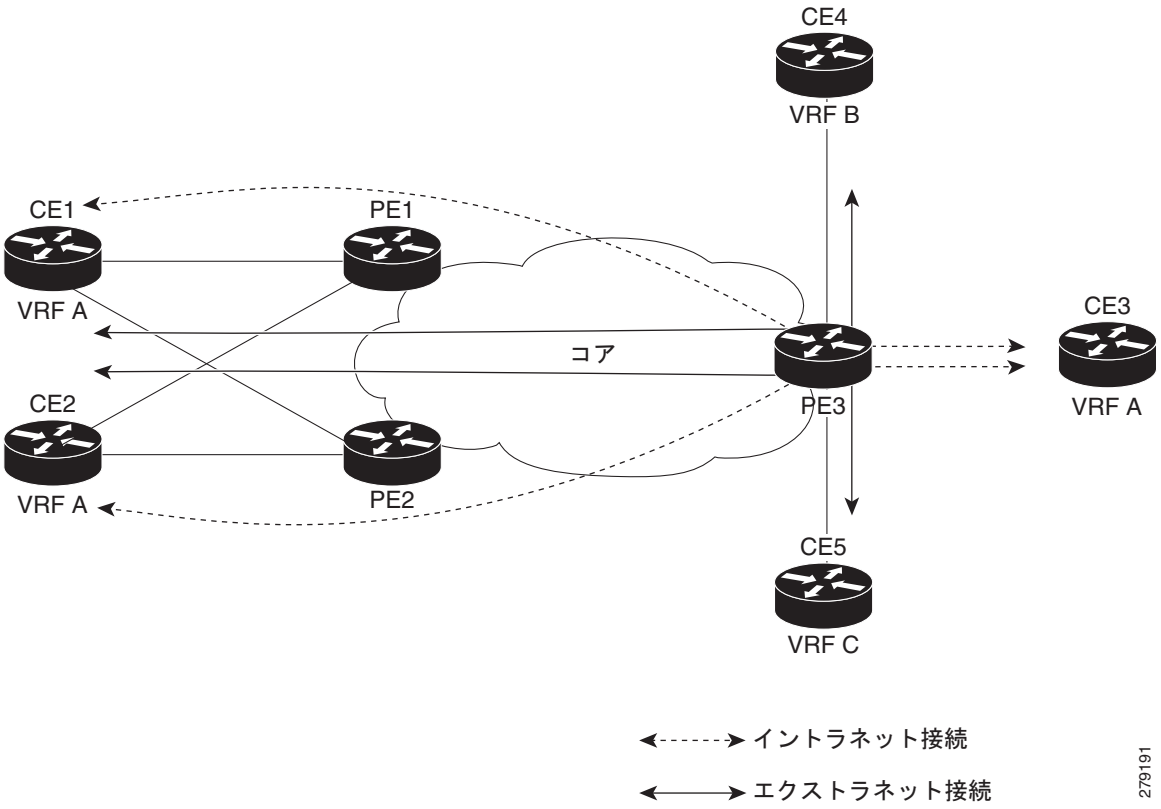
- さまざまな企業。
- サービス プロバイダーまたはコンテンツ プロバイダーと VPN カスタマー。

MPLS VPN により、ユーザが許可された情報にのみアクセスすることが保証されます。MPLS VPN エクストラネット サービスは、エクストラネット ユーザにセキュリティおよび機密データの整合性のないユニキャストおよびマルチキャスト接続を提供します。マルチキャスト VPN エクストラネット サポート機能では、この機能を拡張してエクストラネット ユーザへのマルチキャスト接続も追加されます。

エクストラネット MVPN アーキテクチャ

図 28-1 に、エクストラネット MVPN アーキテクチャを示します。

図 28-1　エクストラネット MVPN アーキテクチャ



MVPN エクストラネットの設定

企業 VPN カスタマーにエクストラネット MVPN サービスを提供するには、次の手順を使用して受信プロバイダー エッジ（PE）ルータに、発信元 Multicast Virtual Routing and Forwarding（MVRF; マルチキャスト仮想ルーティングおよびフォワーディング）を設定する必要があります。

- 直接接続された CE ルータの背後のエクストラネット サイトに 1 つ以上の受信先が存在する受信 PE ルータで、追加 MVRF を設定します（MVRF が設定されていない場合）。この MVRF には、マルチキャスト発信元に接続されたサイトと同じデフォルトの Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）グループが存在します。
- 受信 PE ルータで、発信元 MVRF から受信 MVRF へのルートのインポートに使用されるルーティング ポリシーと同様のユニキャスト ルーティング ポリシーを設定します。

MVPN エクストラネットは、入力レプリケーション モードおよび出力レプリケーション モードの両方で動作します。プラットフォームでは、両方のモードで Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）通知に基づきハードウェア エントリをプログラミングします。エンド ユーザに対しては、エクストラネットはプラットフォームが使用するモードに関係なく、同様に動作してパケットをスイッチします。

（注）　MVPN エクストラネット サポートの設定の詳細については、『Configuring Multicast VPN Extranet Support』を参照してください。

制約事項および使用上の注意事項

Cisco 7600 シリーズ ルータでマルチキャスト VPN エクストラネット サポートを設定する場合は、次の制約事項および使用上のガイドラインに従ってください。

- IPV6 ベースの MVPN エクストラネットは、Cisco 7600 シリーズ ルータでサポートされていません。
- データ トラフィックのパフォーマンス、遅延、およびコンバージェンスは、MVPN エクストラネットおよび MVPN イントラネットで同じです。
- MVPN エクストラネットの拡張に関するデータは次のとおりです。
  - サポートされている MVRF の最大数は 100 です。
  - 各 MVRF でサポートされている mroute の最大数は 100 です。
- エクストラネット コンテンツ グループ モードは、すべての VRF で一貫している必要があり、次のモードがサポートされています。
  - MVPN エクストラネット機能は、Protocol Independent Multicast（PIM）スパース モード（PIM-SM）と Source Specific Multicast（SSM）トラフィックをサポートします。PIM デンス モード（PIM-DM）および双方向 PIM（Bidir-PIM）トラフィックはサポートされません。
  - PIM スパース モードは、RP が（CE 上の）PE ルータの背後に設定されていて、発信元が同じイントラネット MVPN で CE ルータの背後にある場合にのみサポートされています。
- *fallback-lookup* オプションを指定したスタティック mroute だけが、RPF 検索でサポートされています。
- MVPN エクストラネット サポートを設定するには、レシーバ PE でソース MVRF を設定します。発信元 PE で受信 MVRF の設定によって、MVPN エクストラネット サポートを実装することはできません。

CHAPTER 29

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、Cisco 7600 シリーズ ルータに 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、次の資料を参照してください。

- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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

この章の内容は、次のとおりです。

- 「レイヤ 3 スイッチングの機能概要」（P.29-1）
- 「ハードウェア レイヤ 3 スイッチングのデフォルト設定」（P.29-4）
- 「設定時の注意事項および制約事項」（P.29-4）
- 「ハードウェア レイヤ 3 スイッチングの設定」（P.29-5）
- 「ハードウェア レイヤ 3 スイッチング統計情報の表示」（P.29-6）

（注）
- Internetwork Packet Exchange（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 31 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」（P.29-2）

• 「レイヤ 3 スイッチド パケットの書き換え」（P.29-2）

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 PFC および 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 上で等しく稼働します。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 アクセス コントロール リスト（ACL）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; シスコ エクスプレス フォワーディング）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）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。パケットが Cisco 7600 シリーズ ルータから送信されるときに、出力ポート上で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 52 章「NetFlow および 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

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、Cisco 7600 シリーズ ルータは 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な形になります。

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（MAC）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 へルーティングさせる場合、ルータはそのパケットが MSFC のレイヤ 2（MAC）アドレスに送信されたことを認識します。

レイヤ 3 スイッチングを実行するため、ルータはレイヤ 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、ルータはレイヤ 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。ルータはレイヤ 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 パケットは次のようにフォーマットされます（概念上）。

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	*Source A MAC*	*Destination B IP*	*Source A IP*	*n*	*calculation1*		

ルータが 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。

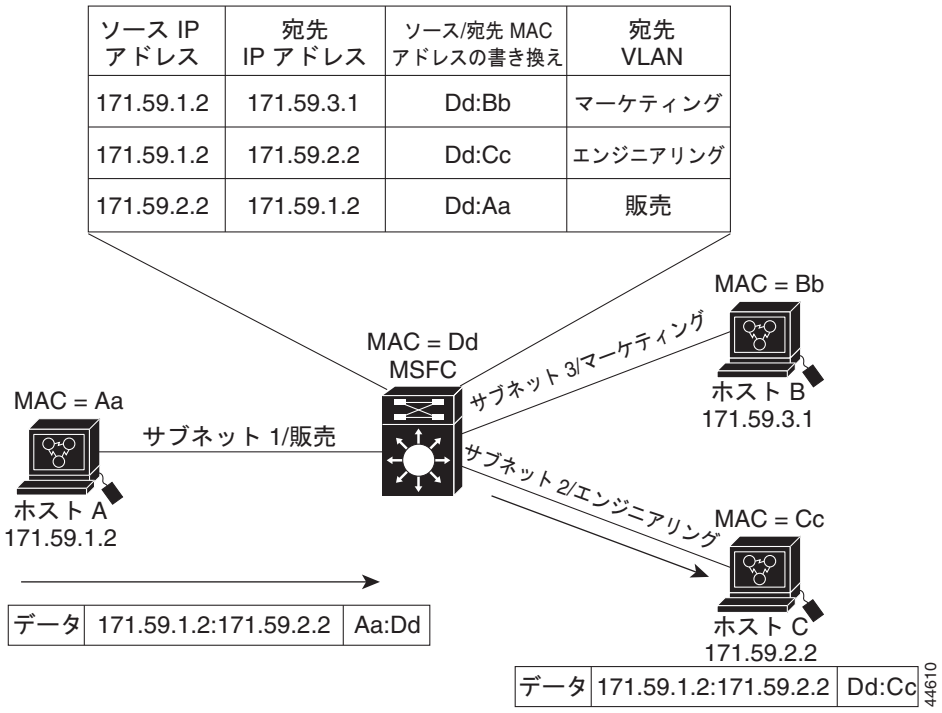
レイヤ 2 フレーム ヘッダー		**レイヤ 3 IP ヘッダー**				**データ**	**FCS**
宛先	送信元	宛先	送信元	TTL	チェックサム		
Destination B MAC	*MSFC MAC*	*Destination B IP*	*Source A IP*	*n-1*	*calculation2*		

ハードウェア レイヤ 3 スイッチングの例

図 29-1（P.29-4）に、単純なネットワーク トポロジーを示します。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 29-1　ハードウェア レイヤ 3 スイッチングのトポロジー例



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 29-1 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 29-1　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（分散 CEF）

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際、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 バイト制御を使用する 802.2 対応の 802.3（SAP1）
  - 802.2 対応の 802.3 および 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。設定は必要ありません。

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スを 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スは、パケットごとのロードバランス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スの判断を行うので、結果としてロードバランスがランダムにならない場合があります。

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 C7600 シリーズ ルータではサポートされません。

MSFC 上の Cisco IOS CEF および dCEF の詳細については、次の資料を参照してください。

- 次の URL の「Cisco Express Forwarding」の項
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt1/index.htm
- 次の URL の『*Cisco IOS Switching Services Command Reference*』
  http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html

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 30

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

PFC3 および DFC3 では、IPv6 マルチキャスト トラフィックがハードウェアでサポートされます。Cisco 7600 シリーズ ルータで IPv6 マルチキャストを設定するには、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/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html
- 『*Cisco IOS IPv6 Command Reference*』
  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

ここでは、Cisco 7600 シリーズ ルータにおける IPv6 マルチキャストのサポートについて詳しく説明します。

- 「IPv6 マルチキャストをサポートする機能」（P.30-1）
- 「IPv6 マルチキャストの注意事項および制約事項」（P.30-2）
- 「IPv6 マルチキャスト レイヤ 3 スイッチングの設定」（P.30-3）
- 「show コマンドを使用した IPv6 マルチキャスト レイヤ 3 スイッチングの確認」（P.30-3）

IPv6 マルチキャストをサポートする機能

次の機能で IPv6 マルチキャストがサポートされます。

- RPR および RPR+ 冗長モード：第 7 章「RPR および RPR+ スーパーバイザ エンジンの冗長設定」を参照してください。
- Multicast Listener Discovery version 2（MLDv2）スヌーピング：第 32 章「IPv6 マルチキャスト トラフィック用 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ません。

- IPv6 マルチキャスト レート リミッタ：第 40 章「サービス拒絶保護の設定」を参照してください。
- ブートストラップ ルータ（BSP）：『*Cisco IOS IPv6 Configuration Library*』および『*Cisco IOS IPv6 Command Reference*』の BSR の情報を参照してください。
- IPv6 アクセス サービス：DHCPv6 プレフィックス委任：次の資料を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html

- IPv6 の SSM マッピング：次の資料を参照してください。
  http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html

IPv6 マルチキャストの注意事項および制約事項

次の注意事項および制約事項は、Cisco 7600 シリーズ ルータにおける IPv6 マルチキャストのサポートに適用されます。

- PFC3 および DFC3 では、以下がハードウェアでサポートされます。
  - 完全にスイッチングされた IPv6 マルチキャスト フロー
  - IPv6 PIM-Sparse Mode（PIM-SM; PIM sparse（疎）モード）（S,G）転送
  - NetFlow テーブルを使用した 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 チェックでエラーになった 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 の SSM Mapping（PIM-SSM）
  - NetFlow テーブルを使用した IPv6 マルチキャスト転送情報ベース（MFIB）
  - NetFlow テーブルを使用した IPv6 Distributed MFIB（dMFIB）
  - 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複製
  - マルチキャスト ルートの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使用不可）
  - RPR および RPR+ 冗長モード（第 7 章「RPR および RPR+ スーパーバイザ エンジンの冗長設定」を参照）
  - 入力および出力 PFC QoS（第 45 章「PFC QoS の設定」を参照）
  - 入力および出力の Cisco アクセス コントロール リスト（ACL）
- PFC3 および DFC3 では、以下がハードウェアでサポートされません。
  - 部分的にスイッチングされた 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
  - 6to4 トンネルを組み込んだ ISATAP トンネル

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 インターフェイスで PIM-SM をイネーブルにします。

show コマンドを使用した IPv6 マルチキャスト レイヤ 3 スイッチングの確認

ここでは、**show** コマンドを使用して、IPv6 マルチキャスト レイヤ 3 スイッチングを確認する方法について説明します。

- 「MFIB クライアントの確認」（P.30-3）
- 「スイッチング機能の表示」（P.30-4）
- 「(S,G) 転送機能の確認」（P.30-4）
- 「(*,G) 転送機能の確認」（P.30-4）
- 「サブネット エントリ サポート ステータスの確認」（P.30-4）
- 「レプリケーション モード機能の表示」（P.30-5）
- 「サブネット エントリの表示」（P.30-5）
- 「IPv6 マルチキャスト概要の表示」（P.30-5）
- 「NetFlow ハードウェア転送カウントの表示」（P.30-5）
- 「FIB ハードウェア ブリッジングおよびドロップ カウントの表示」（P.30-6）
- 「共有および well-known ハードウェア隣接カウンタの表示」（P.30-6）

（注）　以降で使用する show コマンドは、DFC3 をスロット 1 に装備したスイッチング モジュールを搭載したルータ、および PFC3 をスロット 6 に装備した Supervisor Engine 720 用です。

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 上で動作している 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 および任意の DFC3 上で動作している 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)
```

スイッチング機能の表示

次に、**show platform software multicast ipv6 capability** コマンドの全出力例を示します。

```
Router# show platform software multicast ipv6 capability | i switching
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 : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress

PE1-7600#
```

（S,G）転送機能の確認

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）転送機能の確認

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 サポート ステータスの確認

次に、サブネット エントリ 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.
```

レプリケーション モード機能の表示

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 モード機能を表示する例を示します。

```
Router# show platform software multicast ipv6 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 : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
```

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 multicast ipv6 connected
IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception
```

IPv6 マルチキャスト概要の表示

次に、IPv6 マルチキャスト概要を表示する例を示します。

```
Router# show platform software multicast ipv6 summary module 4
IPv6 Multicast Netflow SC summary on Slot[4]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      0
(*, G)                      0

IPv6 Multicast FIB SC summary on Slot[4]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  0
(*, G/m)                    3
```

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）　Netflow（*,G）カウントは常にゼロです。MSFC3 では PIM-SM（*,G）転送がソフトウェアでサポートされるからです。

FIB ハードウェア ブリッジングおよびドロップ カウントの表示

次に、FIB ハードウェア ブリッジング カウントおよびドロップ 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）の値は、ハードウェア ブリッジ エントリ カウントです。
- （*,G/m）の値は、ハードウェア ブリッジ/ドロップ 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 multicast ipv6 shared-adjacencies コマンドでは、FIB および ACL-TCAM のエントリによって IPv6 マルチキャストに使用される、共有および well-known のハードウェア隣接カウンタが表示されます。

```
Router# show platform software multicast ipv6 shared-adjacencies module 4

---- SLOT [4] ----

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      0            0
StarG (spt == INF) adjacency  0xB      0            0
StarG (spt != INF) adjacency  0xC      0            0
Router
```

CHAPTER 31

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、Cisco 7600 シリーズ ルータで IPv4 マルチキャスト レイヤ 3 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、次の資料を参照してください。

- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.31-1）
- 「IPv4 双方向 PIM の機能概要」（P.31-7）
- 「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」（P.31-7）
- 「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」（P.31-8）
- 「IPv4 マルチキャスト レイヤ 3 スイッチングの設定」（P.31-9）
- 「IPv4 双方向 PIM の設定」（P.31-23）

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概要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」（P.31-2）
- 「マルチキャスト レイヤ 3 スイッチング キャッシュ」（P.31-2）
- 「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」（P.31-3）
- 「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」（P.31-4）
- 「非 RPF トラフィックの処理」（P.31-5）
- 「IPv4 双方向 PIM の機能概要」（P.31-7）

IPv4 マルチキャスト レイヤ 3 スイッチングの概要

ポリシー フィーチャ カード（PFC）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 シスコ エクスプレス フォワーディング（CEF）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。CEF は、PFC の転送情報ベース（FIB）および隣接関係テーブルを使用します。分散型フォワーディング カード（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リバース パス転送（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。

ハードウェア スイッチングとも呼ばれるマルチキャスト 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、ネットワーク ルータのプロセッサを中心としたマルチキャスト転送および複製の負荷が軽減されます。

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。Protocol Independent Multicast（PIM）がルート決定に使用され、mcast レート リミッタがルート プロセッサにリレーされるトラフィックを制限します。

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 33 章「IPv4 マルチキャスト トラフィック用 IGMP スヌーピングの設定」を参照）。

7600 内の最新の IPV4 マルチキャスト実装では、ルート プロセッサ（RP）からスイッチ プロセッサ（SP）へのプラットフォーム固有の分散メカニズムが使用されます。MFIB の導入によって、プラットフォームに依存しない方法で情報をスイッチ プロセッサ（SP）とラインカード（LC）に分散させることができるようになります。12.2(33)SRE では、この機能が SUP720、Sup32、RSP720、および互換性のある DFC でサポートされます。

MFIB 実装の前に使用されていた Multicast Distributed Switching Services（MDSS）実装の詳細については、http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdmdc.html を参照してください。

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 により、レイヤ 3 スイッチング情報をハードウェア テーブルに維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。隣接関係テーブルには、書き換え情報と Multicast Expansion Table（MET）テーブルへのポインタが格納されています。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。

MSFC 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 グループへの発信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 テーブルをクリアすると、すべてのマルチキャスト レイヤ 3 スイッチング キャッシュ エントリがクリアされます。
- **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 上のすべてのマルチキャスト レイヤ 3 スイッチング キャッシュ エントリが消去されます。

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場合を想定します。送信元 VLAN 以外の VLAN 上にグループ G1 のメンバーが存在する場合、PFC は送信元以外の 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（ルータはさらに、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、パケットは、次のようにフォーマットされます（概念上）。

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		
Group G1 MAC[1]	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

1. この例では、宛先 B はグループ G1 のメンバーです。

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 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、すべての発信インターフェイス用のアドレスと同じであり、変更することができません）。
- IP ヘッダーの存続可能時間（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、書き換えられた IP マルチキャスト パケットは、ルーティングされたような外見になります。PFC は書き換えたパケットを該当する宛先 VLAN に複製し、その VLAN 上でパケットが IP マルチキャスト グループ G1 のメンバーに転送されます。

PFC がパケットの書き換えを行ったあと、パケットは、次のようにフォーマットされます（概念上）。

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		
Group G1 MAC	*MSFC MAC*	*Group G1 IP*	*Source A IP*	*n-1*	*calculation2*		

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

あるフローの 1 つ以上の発信レイヤ 3 インターフェイスがハードウェア スイッチングされ、1 つ以上の発信インターフェイスがハードウェア スイッチングされない場合は、そのフローが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たフローが形成されると、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、ソフトウェアによって、ハードウェア スイッチングされない発信インターフェイスに転送されます。

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.31-4）
- 「フローの完全スイッチング」（P.31-5）

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、ルータが IP マルチキャスト グループのメンバー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 スパース モードで、ルータが送信元への最初のホップ ルータである場合（この場合、ルータはランデブー ポイント（RP）に PIM 登録メッセージを送信する必要があります）。
- フローの発信インターフェイスで、マルチキャスト TTL しきい値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、かつ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。
- 発信インターフェイスがディスタンス ベクトル マルチキャスト ルーティング プロトコル（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ネットワーク アドレス変換（NAT）が設定されていて、発信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。
- 発信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 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 Shortest-Path-Tree（SPT）へのしきい値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。

- 最低 1 つの（S,G）エントリに（*,g）エントリと同じ RPF が含まれていても、次のうちいずれかが真である場合、（*,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）が設定されていない。
  - SPT フラグ（T ビット）が設定されていない。
  - プルーニングフラグ（P ビット）が設定されていない。
- DVMRP ネイバーが（*,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。
- インターフェイスおよびマスク エントリが（*,G）エントリの RPF インターフェイス用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、すべての発信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 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。

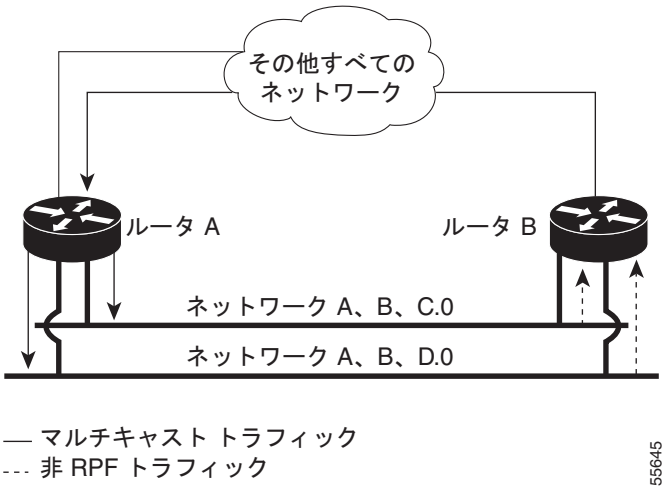
- 「非 RPF トラフィックの概要」（P.31-5）
- 「スタブ ネットワークのための RPF 障害のフィルタリング」（P.31-6）
- 「RPF 障害トラフィックのレート制限」（P.31-6）

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、発信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レシーバまで転送します（図 31-1 を参照）。このようなトポロジでは、PIM 指定ルータ（PIM DR）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ドロップ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。

Cisco 7600 シリーズ ルータは、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 31-1　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、スパース モードのスタブ ネットワーク用に、RPF 障害の ACL 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ドロップされるため、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、スパース モードのスタブ ネットワークにかぎって使用してください。デンス 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。デンス モードのネットワーク、およびスパース 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.31-16）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ドロップされます。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、ルータは非 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ドロップ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。

最初の非 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。その後 NetFlow エントリは、パケットを MSFC ではなくブリッジド ポートだけに送信して、送信元およびグループのパケットをすべて処理します。

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 スパース 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、デフォルトでイネーブルに設定されています。

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がサポートされます。IPv4 双方向 PIM グループをサポートするために、PFC3 は指定フォワーダ（DF）モードという新しいモードを実装しています。指定フォワーダは、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、グループはデンス 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.31-23）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 31-1 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 31-1　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	すべてのインターフェイス上でディセーブル
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	すべてのインターフェイス上でディセーブル
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、かつ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、イネーブル

Internet Group Management Protocol（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ングすると、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 33 章「IPv4 マルチキャスト トラフィック用 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」（P.31-8）
- 「サポートされていない機能」（P.31-9）

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 フローに実行されません。

- 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制御パケット専用で、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）にマッピングされます。

- 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、フロー内で IP オプションを指定されていないパケットは、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した送信元トラフィック（MBONE トラフィックなど）
- スパース 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。
- （*,G）エントリが IPv4 双方向 PIM エントリでルータがグループの RP である場合を除き、（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。
- 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。
- Supervisor Engine 32 では出力マルチキャスト複製がサポートされず、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。
- MFIB 実装では、片方向のデータ パケット数を制限する**ip multicast rate-limit** コマンドがハードウェア設定内でサポートされません。
- MFIB 実装では、**ip multicast ttl-threshold** コマンドがハードウェア設定内でサポートされません。
- MFIB 実装では、ネットワーク アドレス変換（NAT）がハードウェア設定内でサポートされません。
- MFIB IPv4 実装以降で次の MDSS コマンドが無効になっています。
  - **debug mdss [vrf <vrf-name>] [all | error | events | mdt | p2p | packet]**
  - **mls ip multicast [vrf <name>] connected {config command - global and interface-level}**

  - **mls ip multicast consistency-check {config command - global and interface-level}**
  - **show mls ip multicast consistency-check**
  - **show mls ip multicast rp-mapping**
- MFIB 実装以降で次のコマンドが廃止予定になっています。
  - **mls ip multicast non-rpf aging fast**
  - **mls ip multicast non-rpf aging global**
  - **ip multicast replication-mode egress**
  - **mls ip multicast replication-mode ingress**
  - mls ip multicast flow-stat timer

サポートされていない機能

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。

マルチキャスト ストリーミングは、Cat6500 および 7600 上の DMVPN 全体でサポートされません。ルーティング プロトコルなどのローカル コントロール プレーンからのマルチキャスト パケットだけがサポートされます。

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方法について説明します。

- 「IGMPv3、IGMP v3lite、および URD を使用した Source Specific Multicast」（P.31-10）
- 「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.31-10）
- 「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.31-10）
- 「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」（P.31-11）
- 「レプリケーション モードの設定」（P.31-12）
- 「ローカル出力レプリケーションのイネーブル化」（P.31-14）
- 「レイヤ 3 スイッチングのグローバルしきい値の設定」（P.31-15）
- 「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」（P.31-15）
- 「フロー統計情報メッセージ インターバルの指定」（P.31-16）
- 「IPv4 双方向 PIM の設定」（P.31-23）
- 「IPv4 双方向 PIM スキャン インターバルの設定」（P.31-24）
- 「RPF 障害に対する ACL ベースのフィルタリングの設定」（P.31-16）
- 「レート リミッタ ステータスの確認」（P.31-17）
- 「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」（P.31-18）
- 「IPv4 マルチキャスト ルーティング テーブルの表示」（P.31-21）
- 「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.31-22）

- 「IPv4 双方向 PIM 情報の表示」（P.31-25）
- 「IPv4 デバッグ コマンドの使用」（P.31-26）

（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、EXEC モード 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）を使用した送信元固有マルチキャスト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、次の資料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/iproute/command/reference/fiprrp_r.html
- 次の URL の『*Cisco IOS IP and IP Routing Command Reference*, Release 12.1』
  http://www.cisco.com/en/US/docs/ios/12_1/iproute/command/reference/ip_r.html

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 スパース 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 platform software multicast ip**	システム内のパケット フローに関する概要を表示します。

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)# show platform software multicast ip
(40.0.0.2, 232.0.1.4) Incoming interface: Lspvif0, Packets Switched: 119954142
Hardware switched outgoing interfaces:
GigabitEthernet3/6
Total hardware switched flows: 1
```

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限り行います。

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.31-10）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 では、入力レプリケーション モードだけがサポートされます。

Supervisor Engine 720 では **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「マルチキャストの強化：レプリケーション モード検出」と呼ばれています。

デフォルトの場合、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できる場合、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できないモジュールを検出した場合、レプリケーション モードは入力レプリケーションに自動的に変更されます。ip multicast hardware-switching replication-mode **egress** コマンドを入力してこの処理を無効にすることができるため、OSM などの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がインストールされている場合でも、システムは出力レプリケーション モードで動作し続けます。入力レプリケーション モードだけで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している場合に、出力レプリケーションを実行できないモジュールを搭載すると、次のようになります。

- システムは入力モードに戻ります。
- システム ログが生成される
- 元の設定に戻すために、システム リロードが発生します。

システムが強制出力モードで機能している場合はシステム ログが作成され、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が表示されます。

（注）　出力レプリケーションに対応していないファブリック対応モジュールを含むシステムに強制出力モードを設定する場合は、このようなモジュールがマルチキャスト トラフィックを発信したり受信したりしないことを確認する必要があります。

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 モードへの変更中、ショートカットが削除され再インストールされるためトラフィックの中断が発生する場合があります。トラフィック転送の中断を回避するには、グローバル コンフィギュレーション モードで ip multicast hardware-switching replication-mode **ingress** コマンドを入力します。このコマンドにより、システムは入力レプリケーション モードで動作します。

ip multicast hardware-switching replication-mode **ingress** コマンドの **no** 形式は、システムを自動検出モードに戻します。

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 multicast hardware-switching replication-mode** [**egress** | **ingress**]	レプリケーション モードを指定します。
ステップ 2	Router# **show platform software multicast ip 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 platform software multicast ip 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または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)# ip multicast hardware-switching replication-mode egress
Router# show platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
Router#

Router# show platform software multicast ip summary

IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type               Shortcut count
--------------------------+--------------
(S, G)                      0

IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type               Shortcut count
--------------------------+--------------
(*, G/128)                  0
(*, G/m)                    0
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 では、入力レプリケーション モードだけがサポートされます。

Supervisor Engine 720 では、ローカル出力レプリケーションを無条件でイネーブルにすることができます。この機能は、リリース ノートおよび Feature Navigator で「マルチキャストの強化：出力レプリケーション パフォーマンスの改善」と呼ばれています。

デュアル スイッチファブリック接続を含む DFC を装備したモジュールには、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 エンジンがあります。それぞれのレプリケーション エンジンは、スイッチファブリック接続と関連したインターフェイスにパケットを転送したり、そのインターフェイスからパケットを転送したりします。スイッチファブリック接続と関連するインターフェイスは、パケット レプリケーション エンジン側から見て「ローカル」と見なされます。

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と関連するローカル インターフェイスだけにパケットを転送するように、モジュールの 2 つのレプリケーション エンジンに指示するコマンドを入力することで、スイッチファブリック接続間でマルチキャスト パケットの複製の重複を防止できます。

この機能をイネーブルにすると、レプリケーション エンジンごとの Multicast Expansion Table（MET）にローカル レイヤ 3 インターフェイスだけが入力されます。この処理により、レプリケーション エンジンによってサポートされないインターフェイス（ローカル以外のインターフェイス）の複製が防止され、複製のパフォーマンスが向上します。

ローカル出力レプリケーションは、次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 装備モジュール
- ポート チャネルの一部でないレイヤ 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、次の内部 VLAN でサポートされません。

- 出力内部 VLAN
- 部分ショートカット内部 VLAN
- マルチキャスト VPN マルチキャスト配信ツリー（MDT）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 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、または IPv4 と IPv6 マルチキャストの混在がイネーブルになっているシステムで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）　このコマンドでは、システムをリセットしないと、設定が有効になりません。

	コマンド	目的
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 platform software multicast ip 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。

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 platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
```

レイヤ 3 スイッチングのグローバルしきい値の設定

グローバル マルチキャスト レートしきい値（パケット数/秒で指定）を設定し、これを下回るとすべてのマルチキャスト トラフィックが MSFC によってルーティングされるようにすることができます。この設定により、低レート レイヤ 3 フローのスイッチング キャッシュ エントリの作成が防止されます。

（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。既存のルートにしきい値を適用するには、ルートをいったん消去して、再び確立させます。

レイヤ 3 スイッチングしきい値を設定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls ip multicast threshold` *ppsec*	IP MMLS しきい値を設定します。
`Router(config)# no mls ip multicast threshold`	デフォルトの IP MMLS しきい値に戻します。

次に、レイヤ 3 スイッチングしきい値を 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 スパース モードでは、インターフェイスの指定ルータである最初のホップ 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、それをランデブー ポイント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 によって完全にハードウェアでスイッチング フローのままになる、(*,G) フローおよび新たに直接接続された送信元の両方が正常

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 platform software multicast ip 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 へ転送する手順を指定します。
`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)#
```

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、特定の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、特定の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**

レート リミッタ ステータスの確認

レート リミッタ ステータスを確認するには、次の作業を行います。

コマンド	目的
Router# **show mls rate-limit | i RPF**	RPF 障害レート制限情報とレート リミッタの現在の状態を表示します。

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 rate-limit | i RPF
IP RPF FAILURE         100      10
Router-1# sh mls rate-limit usage
                            Rate Limiter Type     Packets/s   Burst
                          ----------------------   ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                          -           -       -
             RL# 1: Free                          -           -       -
             RL# 2: Free                          -           -       -
             RL# 3: Free                          -           -       -
             RL# 4: Free                          -           -       -
             RL# 5: Used
                                   MCAST DFLT ADJ          10      10
             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-1# sh 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                  10      10  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                  -       -     -
    DHCP Snooping IN    Off                  -       -     -
   DHCP Snooping OUT    Off                  -       -     -
       ARP Inspection   Off                  -       -     -
      LAYER_2 PORTSEC   Off                  -       -     -
   LAYER_2 MiniProto    Off                  -       -     -
            IP ERRORS   On                 100      10  Group:0 S
          CAPTURE PKT   Off                  -       -     -
           MCAST IGMP   Off                  -       -     -
MCAST IPv6 DIRECT CON   Off                  -       -     -
MCAST IPv6 ROUTE CNTL   Off                  -       -     -
MCAST IPv6 *G M BRIDG   Off                  -       -     -
 MCAST IPv6 SG BRIDGE   Off                  -       -     -
 MCAST IPv6 DFLT DROP   Off                  -       -     -
MCAST IPv6 SECOND. DR   Off                  -       -     -
 MCAST IPv6 *G BRIDGE   Off                  -       -     -
       MCAST IPv6 MLD   Off                  -       -     -
 IP ADMIS. ON L2 PORT   Off                  -       -     -
       LAYER_2 MACSEC   Off                  -       -     -
       MCAST IPv4 PIM   Off                  -       -     -
Router-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発信インターフェイス 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、フローが発信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 platform software multicast ip コマンドは、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します。

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、次のうちいずれかの作業を行います。

コマンド	目的
Router# **show platform software multicast ip group** *group-id*	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 platform software multicast ip interface** [**gigabitethernet** *1-6* | **port-channel** *1-256* | **tengigabitethernet** *1-6* | **vlan** *1-4094*] | **source** *A.B.C.D.*]	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 platform software multicast ip source** *source-ip*	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 platform software multicast ip 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 platform software multicast ip statistics** [**group** *group-id*]	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。

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 platform software multicast ip group 232.0.1.4
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 8069027
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

PE1-7600
```

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 platform software multicast ip source 40.0.0.2
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 8778143
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

Router#
```

次に、gigabitethernet interface 3/2/1 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例を示します。

```
Router# show platform software multicast ip interface gigabitethernet 3/2/1
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 8206582
Hardware switched outgoing interfaces:
```

```
     Tunnel10

Total hardware switched flows: 1
```

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 platform software multicast ip statistics group 232.0.1.4

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

ここでは、IPv4 双方向 Protocol Independent Multicast（PIM）の設定方法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」（P.31-23）
- 「IPv4 双方向 PIM グループのランデブー ポイントの設定」（P.31-24）
- 「IPv4 双方向 PIM スキャン インターバルの設定」（P.31-24）
- 「IPv4 双方向 PIM 情報の表示」（P.31-25）

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`	ルータ上で IPv4 双方向 PIM をグローバルにイネーブル化します。
`Router(config)# no ip pim bidir-enable`	ルータ上で IPv4 双方向 PIM をグローバルにディセーブルにします。

次に、ルータ上で 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 グループのランデブー ポイントの設定

IPv4 双方向 PIM グループのランデブー ポイント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]***	グループのランデブー ポイントの 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 ランデブー ポイントを使用します。
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 ランデブー ポイント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 リバース パス転送（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、次のうちいずれかの作業を行います。

コマンド	目的
Router# **show ip pim rp mapping** [**in-use**]	PIM グループとランデブー ポイントの間のマッピングを表示し、使用中の学習したランデブー ポイントを表示します。
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 グループとランデブー ポイントとのマッピングに関する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、余白の矢印はショートカットの一部の情報を指定します。

```
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 platform software multicast ip group 232.0.1.4
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: Lspvif0, Packets Switched: 120181613
Hardware switched outgoing interfaces:
GigabitEthernet3/6

Total hardware switched flows: 1
```

IPv4 デバッグ コマンドの使用

表 31-2 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。

（注）　旧来のデバッグ コマンドは利用できなくなります。

表 31-2　IP マルチキャスト レイヤ 3 スイッチングの debug コマンド

コマンド	説明
[no] debug ip multicast hardware-switching {control *group-name* | error *A.B.C.D* | event *A.B.C.D* | ha-error *A.B.C.D* | ha-event *A.B.C.D}*	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。
debug platform software multicast [all | assert]	すべてのログ イベント、パケット情報、およびアサート イベントを表示します。
debug platform software multicast	マルチキャストのデバッグ情報を表示します。
debug platform software multicast ha l2-sso [all |error |event |pak]	レイヤ 2 ハイ アベイラビリティ マルチキャスト ショートカットのデバッグ エラー、イベント、およびパケット情報を表示します。
debug platform software multicast lc	レイヤ 2 ラインカード マルチキャスト イベントを表示します。
debug platform software multicast cgmp [event | pak]	CGMP のデバッグ イベントおよびパケット情報を表示します。
debug platform software multicast ha [error | event]	ハイ アベイラビリティ マルチキャスト ショートカットのデバッグ エラーおよびイベントを表示します。
debug platform software multicast ip hal [error | event |pak | timer]	マルチキャスト HAL のエラー、イベント、タイマー、およびパケット情報を表示します。

表 31-2　IP マルチキャスト レイヤ 3 スイッチングの debug コマンド （続き）

コマンド	説明
debug platform software multicast igmp [**event** | **pak**]	IGMP のデバッグ イベントおよびパケット情報を表示します。
debug platform software multicast mld [**event** | **pak**]	MLD のデバッグのイベントおよびパケット情報を表示します。
debug platform software multicast mrouter [**event** |**pak**]	マルチキャスト ルータのイベントおよびパケット情報を表示します。
debug platform software multicast msc [**error** | **event** |**pak**]	マルチキャスト ショートカットのデバッグ情報を表示します。
debug platform software multicast rgmp [event|pak]	マルチキャスト RGMP のデバッグ情報を表示します。
debug platform software multicast rpdf [error|event]	マルチキャスト双方向 DF のデバッグ情報を表示します。
debug platform software multicast titan [error|event]	マルチキャスト Titan のデバッグ情報を表示します。
debug platform software multicast ipv6 [cmfib | hal]	MFIB IPv6 プラットフォーム コードのデバッグおよびマルチキャスト HAL IPv6 のデバッグ コマンド情報を表示します。
debug platform software multicast ip cmfib [error|event|stats]	マルチキャスト IP CMFIB のエラー、ショートカット イベント、およびハードウェア統計情報のエクスポートを表示します。
debug platform software multicast ip cmfib error [***A.B.C.D*** **| pending]**	送信元またはグループ IP アドレスおよび MFIB IPv4 の保留中のエントリのエラー情報を表示します。
debug platform software multicast ip cmfib event [**A.B.C.D | ctrl | hwapi | mdt | pending | table]**	送信元またはグループ IP アドレス､MFIB IPv4 Ctrl エントリ イベント、MFIB HW-API イベント、MFIB IPv4 テーブル イベント、MFIB IPv4 の保留中のエントリのイベント、および MFIB IPv4 テーブル イベントを表示します。
debug platform software multicast ipv6 cmfib [error|event|stats]	マルチキャスト IPv6 MFIB エラー、ショートカット イベント、およびハードウェア統計エクスポート情報を表示します。
debug platform software multicast ipv6 hal [error| event]	マルチキャスト IPv6 HAL のエラーおよびイベントを表示します。

CHAPTER 32

IPv6 マルチキャスト トラフィック用 MLDv2 スヌーピングの設定

この章では、Cisco 7600 シリーズ ルータで IPv6 マルチキャスト トラフィック用に Multicast Listener Discovery version 2（MLDv2）スヌーピングを設定する方法について説明します。MLDv2 スヌーピングは、すべてのバージョンの PFC3 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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- IPv4 マルチキャスト トラフィックを抑制する場合は、第 33 章「IPv4 マルチキャスト トラフィック用 IGMP 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。

- 「MLDv2 スヌーピングの機能概要」（P.32-1）
- 「デフォルト MLDv2 スヌーピング設定」（P.32-8）
- 「MLDv2 スヌーピング設定時の注意事項および制約事項」（P.32-8）
- 「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」（P.32-8）
- 「MLDv2 スヌーピング クエリアのイネーブル化」（P.32-9）
- 「MLDv2 スヌーピングの設定」（P.32-10）

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」（P.32-2）
- 「MLDv2 メッセージ」（P.32-2）
- 「送信元ベース フィルタリング」（P.32-3）
- 「明示的ホスト トラッキング」（P.32-3）
- 「MLDv2 スヌーピング プロキシ レポート機能」（P.32-3）
- 「IPv6 マルチキャスト グループへの加入」（P.32-4）
- 「マルチキャスト グループからの脱退」（P.32-6）

- 「MLDv2 スヌーピング クエリアの概要」（P.32-7）

MLDv2 スヌーピングの概要

MLDv2 スヌーピングにより、Cisco 7600 シリーズ ルータで 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することができます。

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、ルータを設定できます。MLDv2 スヌーピングは、IPv6 マルチキャスト トラフィックを受信するポートだけにそのトラフィックをダイナミックに転送するように、レイヤ 2 LAN ポートを設定することにより、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 で稼働し、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 スヌーピング クエリアをルータで設定し、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で 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.32-9）を参照してください。

（マルチキャスト ルータ上の）MLDv2 または（スーパーバイザ エンジン上の）MLDv2 スヌーピング クエリアは、ルータが VLAN のすべてのポートを経由して転送し、ホストが応答する一般的な MLDv2 クエリーを定期的に送信します。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）　マルチキャスト グループで、VLAN 中に送信元だけ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 ポート宛てだけに抑制します。

MLDv2 メッセージ

MLDv2 では次のメッセージが使用されます。

- 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あるかを学習するために、マルチキャスト ルータが送信します。
  - マルチキャスト アドレス固有クエリー：特定マルチキャスト アドレスにリスナーがあるかどうかを学習するために、マルチキャスト ルータが送信します。
  - マルチキャスト アドレスおよび送信元固有クエリー：特定マルチキャスト アドレスの指定リストからの送信元にリスナーがあるかどうかを学習するために、マルチキャスト ルータが送信します。
- マルチキャスト リスナー レポート
  - 現行状態レコード（送信請求）：クエリーに応答してホストが送信し、ホストが関係するマルチキャスト グループごとに INCLUDE モードまたは EXCLUDE モードを指定します。
  - フィルタ モード変更レコード（非送信請求）：1 つ以上のマルチキャスト グループの INCLUDE モードまたは EXCLUDE モードを変更するため、ホストが送信します。
  - 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、ホストが送信します。

送信元ベース フィルタリング

MLDv2 では送信元ベース フィルタリングが使用されます。送信元ベース フィルタリングでは、特定マルチキャスト グループでどのマルチキャスト送信元を許可するかブロックするかをホストおよびルータによって特定できるようにします。送信元ベース フィルタリングでは、MLDv2 メッセージの次の情報に基づいてトラフィックの許可またはブロックが行われます。

- 送信元リスト
- INCLUDE モードまたは EXCLUDE モード

レイヤ 2 テーブルが（MAC 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 フィルタリングはハードウェアで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。

明示的ホスト トラッキング

MLDv2 では、ポート上のメンバーシップ情報の明示的な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 レポートを処理し、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
- ホストによって報告されたチャネル
- ホストによって報告された各グループのフィルタ モード
- ホストによって報告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 レポート機能はディセーブルになります。
- 明示的トラッキングがイネーブル化されていて、ルータがレポート抑制モードになっている場合、マルチキャスト ルータは VLAN インターフェイス経由でアクセスするすべてのホストを追跡できないことがあります。

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答して詳細なマルチキャスト グループ メンバーシップ情報をマルチキャスト ルータに送信します。ルータはこれらの応答を調べて、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ことを防止するため、MLDv2 スヌーピングはプロキシ レポートを実行します。

プロキシ レポート機能では、マルチキャスト グループの最初のレポートだけがルータに転送され、同一マルチキャスト グループのその他すべてのレポートが抑制されます。

プロキシ レポート機能では、送信請求レポートおよび非送信請求レポートが処理されます。プロキシ レポート機能はイネーブルになっており、ディセーブルにすることはできません。

（注）　明示的ホスト 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 レポート機能は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答して、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 グループに加入します（ルータが、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）。ルータはこれらのレポートをスヌーピングします。

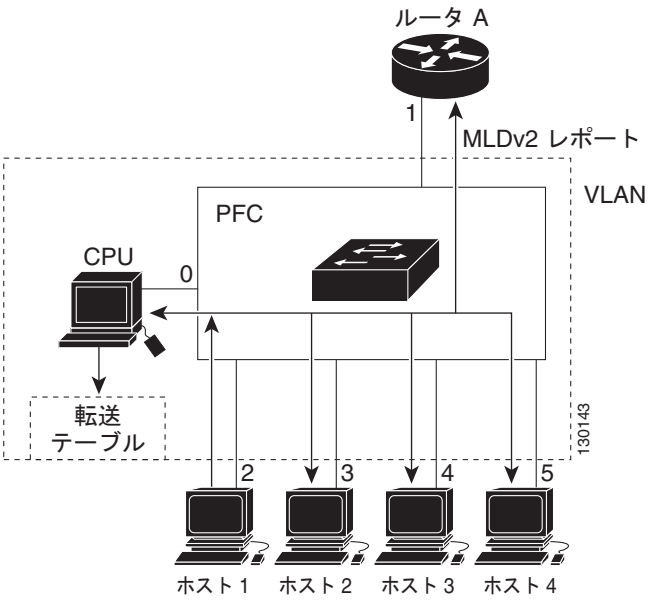
ルータは、調べた MLDv2 レポートに応答して、レポートを受信する VLAN のレイヤ 2 転送テーブルにエントリを作成します。このマルチキャスト トラフィックに関係する別のホストが MLDv2 レポートを送信する場合、ルータはレポートをスヌーピングして、既存のレイヤ 2 転送テーブル エントリにそれを追加します。ルータは、MLDv2 レポートをスヌーピングするマルチキャスト グループごとに、レイヤ 2 転送テーブルで VLAN ごとに 1 つのエントリだけを生成します。

MLDv2 スヌーピングは、マルチキャスト グループごとに 1 つを残して他のすべてのホスト レポートを抑制し、この 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。

ルータは、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 32-1 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 メンバー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 メンバーシップのリストは、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 32-1　初期 MLDv2 リスナー レポート



マルチキャスト ルータ A がルータに MLDv2 の一般的なクエリーを送信し、ルータがそのクエリーをポート 2 ～ 5（同じ VLAN 内のすべてのメンバー）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必要があり、MAC 宛先アドレスが 0x0100.5E01.0203 であるグループに MLDv2 レポートをマルチキャストします。ホスト 1 による MLDv2 レポート マルチキャストをルータがスヌーピングすると、ルータは MLDv2 レポート内の情報を使用して、表 32-1 のような転送テーブル エントリを作成します。このエントリには、ホスト 1 のポート番号、マルチキャスト ルータ、ルータが含まれています。

表 32-1　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

ルータのハードウェアは、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、ルータに対して、MLDv2 パケットだけを CPU に送信するように指示します。これによって、ルータ 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 番めのエントリは、ルータに、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、およびグループに加入しているホスト宛ての MLDv2 パケット（!MLDv2）ではありません。

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 レポートを送信する場合（図 32-2 を参照）、ルータがそのメッセージをスヌーピングして、ホスト 4 のポート番号を転送テーブルに追加します（表 32-2 を参照）。転送テーブルはルータ宛てだけに 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、ルータ宛てではなくグループ宛てに転送されます。

図 32-2　2 番めのホストのマルチキャスト グループへの加入

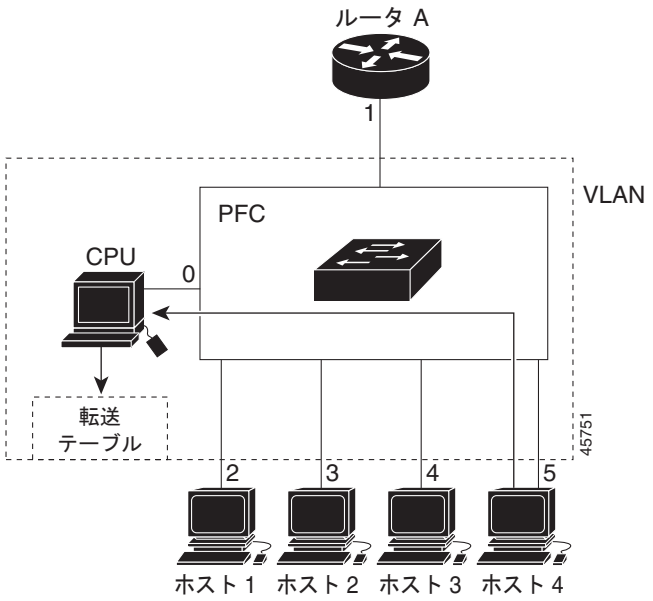


表 32-2　MLDv2 スヌーピング転送テーブルの更新

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」（P.32-6）
- 「高速脱退処理」（P.32-7）

通常の脱退処理

関係するホストは、MLDv2 一般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 MLDv2 一般クエリーに定期的に応答している限り、マルチキャスト ルータはマルチキャスト トラフィックを VLAN に転送し続けます。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 MLDv2 一般クエリーを無視するか（「暗黙的脱退」と言います）、または MLDv2 フィルタ モード変更レコードを送信します。

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 MLDv2 スヌーピングが受信すると、MLDv2 スヌーピングは MAC アドレス付き一般クエリーを送信し、そのインターフェイスに接続されているその他のホストが、指定マルチキャスト グループのトラフィックに関係するかどうかを判断します。

MLDv2 スヌーピングは、この一般クエリーの応答で 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は、指定マルチキャスト グループのトラフィックの受信に関係していないと見なし、指定マルチキャスト グループのレイヤ 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。

ホストがグループに関係する残りのインターフェイスのみからフィルタ モード変更レコードを受信し、MLDv2 スヌーピングが一般クエリーに応答して MLDv2 レポートを受信しなかった場合、MLDv2 スヌーピングはグループ エントリを削除し、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ルータが待機する時間は、「最終メンバ クエリー時間」と言います。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なっています。高速脱退処理をディセーブルにするには、明示的ホスト トラッキングをオフにします。

高速脱退処理は、ソフトウェアで送信元グループ ベースのメンバー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たく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。このようなメッセージをホストから受信すると、ルータは所定のグループに対応する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脱退メッセージで受信された送信元リストとまったく同じである場合、ルータはこのホストを LTL インデックスから削除し、ホストへのマルチキャスト グループ トラフィックの転送を停止します。

送信元リストが一致しない場合、このホストがど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、ルータは LTL インデックスからホストを削除しません。

（注） 明示的ホスト 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 レポート機能は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ているネットワークでは、IP マルチキャスト ルータは MLDv2 クエリアとして機能します。VLAN 内の IP マルチキャスト トラフィックにレイヤ 2 スイッチングだけを行う必要があり、IP マルチキャスト ルータが不要で、VLAN 上に IP マルチキャスト ルータが存在しない場合は、別のルータを MLDv2 クエリアに設定し、このルータからクエリーを送信できるように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 クエリアは定期的に MLDv2 クエリーを送信し、IP マルチキャスト トラフィックを受信するルータからの MLDv2 レポート メッセージをトリガーします。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。

VLAN 内のすべての Cisco 7600 シリーズ ルータで MLDv2 スヌーピング クエリアをイネーブルにできます。ただし、MLDv2 を使用して IP マルチキャスト トラフィックとの関係をレポートするスイッチがある場合は、これらのスイッチに接続された VLAN ごとに、少なくとも 1 つのルータを 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関係なくルータを設定して VLAN 上に MLDv2 クエリーを生成することができます。

デフォルト MLDv2 スヌーピング設定

表 32-3 は、デフォルト MLDv2 スヌーピング設定を示しています。

表 32-3　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	未設定
MLDv2 レポート抑制	イネーブル
MLDv2 スヌーピング ルータの学習方式	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ときは、次の注意事項および制約事項に従ってください。

- MLDv2 は Internet Group Management Protocol version 3（IGMPv3）から派生しています。MLDv2 のプロトコル動作とステート遷移、ホストとルータの動作、クエリーとレポートのメッセージ処理、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 メッセージの形式は、IGMPv3 メッセージとほとんど同じです。
- Cisco IOS ソフトウェアの IPv6 マルチキャストでは MLD バージョン 2 が使用されます。このバージョンの MLD には、MLD バージョン 1 との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 だけ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 ホストおよび MLD バージョン 2 ホストの両方を含む混在 LAN がサポートされます。
- MLDv2 スヌーピングではプライベート VLAN がサポートされます。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ときは、次の注意事項および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 を設定してください（第 14 章「VLAN の設定」を参照）。
- VLAN インターフェイスに IPv6 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）。MLDv2 スヌーピング クエリアをイネーブルにすると、MLDv2 スヌーピング クエリアはクエリー送信元アドレスとして IPv6 アドレスを使用します。
- 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。IPv6 アドレスがクリアされると、MLDv2 スヌーピング クエリアはディセーブルになります。MLDv2 スヌーピング クエリアをイネーブルにすると、IPv6 アドレスを設定した場合、MLDv2 スヌーピング クエリアが再起動されます。
- MLDv2 スヌーピング クエリアをイネーブルにしても、MLDv2 スヌーピング クエリアが 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、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ければ、MLDv2 スヌーピング クエリアは 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、MLDv2 スヌーピング クエリアが 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、MLDv2 スヌーピング クエリアはディセーブルになります。
- MLDv2 スヌーピングがイネーブルである場合、QoS では MLDv2 パケットがサポートされません。
- MLDv2 スヌーピング クエリアをサポートする VLAN 内のすべての Cisco 7600 シリーズ ルータで、MLDv2 スヌーピング クエリアをイネーブルにできます。ルータの 1 つがクエリアとして選定されます。

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。

特定の 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、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.32-9）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.32-10）
- 「マルチキャスト レシーバへのスタティック接続の設定」（P.32-11）
- 「高速脱退処理のイネーブル化」（P.32-13）
- 「明示的ホスト トラッキングの設定」（P.32-13）
- 「レポート抑制の設定」（P.32-14）
- 「MLDv6 スヌーピング情報の表示」（P.32-14）

（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

MLDv2 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)# 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 レシーバへのスタティック接続の設定

マルチキャスト レシーバ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** キーワードを入力して、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 内の別のポートへ送信されるのを防止します。

次に、マルチキャスト レシーバ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 内である必要があります。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、ルータ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。

ルータによって送信される MLD 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)# ipv6 mld snooping last-member-query-interval interval`	ルータによって送信される IGMP 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 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

特定の 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#
```

SSM セーフ レポート機能のイネーブル化

Source-Specific Multicast（SSM）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 レポート機能をイネーブルにする例を示します。

```
Router(config)# interface vlan 10
Router(config-if)# ipv6 mld snooping ssm-safe-reporting
```

明示的ホスト トラッキングの設定

（注）　明示的ホスト 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 レポート機能はディセーブルになります。

特定の VLAN で明示的ホスト 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`	明示的ホスト トラッキングの設定を消去します。
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 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
```

MLDv6 スヌーピング情報の表示

ここでは、MLDv6 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.32-15）
- 「MAC アドレス マルチキャスト エントリの表示」（P.32-15）

- 「VLAN インターフェイスの MLDv2 スヌーピング情報の表示」（P.32-16）

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、ルータはマルチキャスト 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、特定の 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 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 インターフェイスで MLDv2 スヌーピング情報を表示します。

次に、VLAN 25 の明示的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 33

IPv4 マルチキャスト トラフィック用 IGMP スヌーピングの設定

この章では、Cisco 7600 シリーズ ルータにおいて IPv4 マルチキャスト トラフィック用 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。

（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 7600 Series Routers Command References』を参照してください。
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- IPv6 マルチキャスト トラフィックを抑制する場合は、第 32 章「IPv6 マルチキャスト トラフィック用 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」（P.33-1）
- 「IGMP スヌーピングのデフォルト設定」（P.33-8）
- 「IGMP スヌーピング設定時の注意事項および制約事項」（P.33-8）
- 「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」（P.33-8）
- 「IGMP スヌーピング クエリアのイネーブル化」（P.33-9）
- 「IGMP スヌーピングの設定」（P.33-10）
- 「MVR の概要」（P.33-17）
- 「MVR の設定」（P.33-19）

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」（P.33-2）
- 「マルチキャスト グループへの加入」（P.33-2）
- 「マルチキャスト グループからの脱退」（P.33-4）
- 「IGMP スヌーピング クエリアの概要」（P.33-5）
- 「IGMP バージョン 3 サポートの概要」（P.33-5）

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、ルータを設定できます。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ダイナミックに転送するようにレイヤ 2 LAN ポートを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 で稼働し、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 については、第 31 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 クエリアをルータで設定し、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で 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.33-9）を参照してください。

（マルチキャスト ルータ上の）IGMP または（スーパーバイザ エンジン上の）IGMP スヌーピング クエリアは、ルータが VLAN のすべてのポートを経由して転送し、ホストが応答する一般的な 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 中に送信元だけがありレシーバがない場合は、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 ポート宛てだけに抑制します。

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（ルータは、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）。

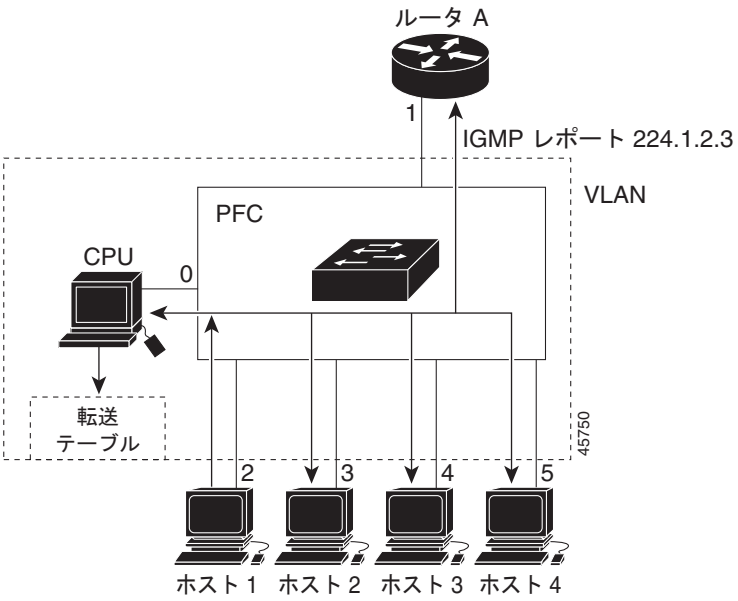
IGMP Join 要求の応答で、ルータは、Join 要求を受信した VLAN のレイヤ 2 転送テーブルにエントリを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが IGMP Join 要求を送信する場合、ルータは、既存のレイヤ 2 転送テーブル エントリに要求を追加します。ルータは、IGMP Join 要求を受信する各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリだけを生成します。

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応答を抑制し、その 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。

ルータは、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 33-1 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 メンバー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 メンバーシップのリストは、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 33-1　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、ルータがそのクエリーを、同じ VLAN の全メンバーのポート 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 への加入を希望し、IGMP メンバーシップ レポート（IGMP Join メッセージ）を同等の MAC 宛先アドレス 0x0100.5E01.0203 を持つグループにマルチキャストします。CPU は、ホスト 1 による IGMP レポート マルチキャストを受け取ると、IGMP レポート内の情報を使用して、転送テーブルのエントリを設定します（表 33-1 を参照）。このエントリには、ホスト 1 のポート番号、マルチキャスト ルータ、およびルータ内蔵 CPU が含まれています。

表 33-1　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

ルータのハードウェアは、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 パケットだけを 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 番めのエントリは、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、およびグループに加入しているホスト宛ての IGMP 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）が同じグループに非送信請求 IGMP Join メッセージを送信する場合（図 33-2 を参照）、CPU はそのメッセージを受信して、転送テーブルにホスト 4 のポート番号を追加します（表 33-2 を参照）。転送テーブルは CPU 宛てだけに 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 33-2　2 番めのホストのマルチキャスト グループへの加入

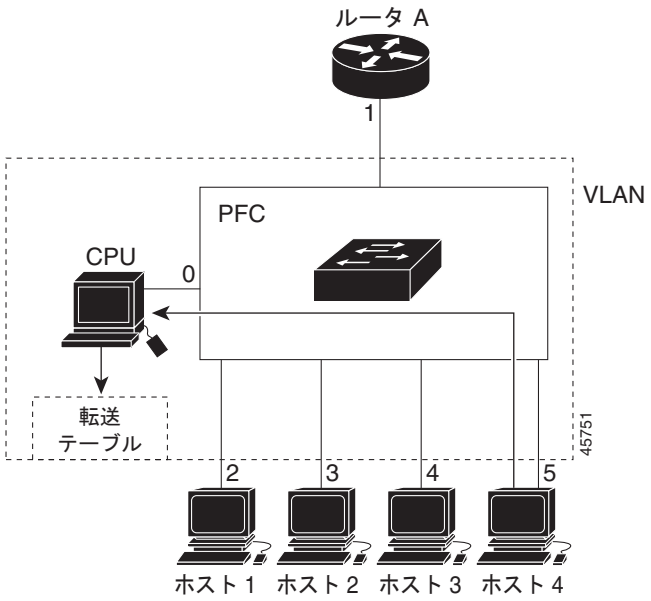


表 33-2　更新された IGMP スヌーピング転送テーブル

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」（P.33-4）
- 「高速脱退処理」（P.33-5）

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 ルータはマルチキャスト トラフィックを VLAN に転送し続けます。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 IGMP クエリーを無視するか（「暗黙的脱退」と呼びます）、またはグループ固有の IGMPv2 Leave メッセージを送信します。

IGMP スヌーピングは、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デバイスが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、この一般的なクエリーに応答して 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デバイスの中に、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係しているデバイスはないと見なし、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だけから 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ルータが待機する時間は、「最終メンバー クエリー時間」と言います。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、最初にレイヤ 2 LAN インターフェイスに IGMP グループ対象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。グループ特定の 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ドロップ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 のホストについてだけサポートされます。

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ているネットワークでは、IP マルチキャスト ルータは IGMP クエリアとして機能します。VLAN 内の IP マルチキャスト トラフィックにレイヤ 2 スイッチングだけを行う必要があり、IP マルチキャスト ルータが不要で、VLAN 上に IP マルチキャスト ルータが存在しない場合は、別のルータを IGMP クエリアに設定し、このルータからクエリーを送信できるようにする必要があります。

IGMP スヌーピング クエリアは、イネーブルの場合、定期的に IGMPv3 クエリーを送信し、IP マルチキャスト トラフィックを受信するルータからの IGMP レポート メッセージをトリガーします。IGMP スヌーピングはこれらの IGMP レポートをリッスンして、適切な転送を確立します。

VLAN 内のすべての Cisco 7600 シリーズ ルータで IGMP スヌーピング クエリアをイネーブルにできます。ただし、IGMP を使用して IP マルチキャスト トラフィックとの関係をレポートするスイッチがある場合は、これらのスイッチに接続された VLAN ごとに、少なくとも 1 台のルータを IGMP 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関係なくルータを設定して VLAN 上に IGMP クエリーを生成することができます。

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」（P.33-6）
- 「IGMPv3 高速脱退処理」（P.33-6）

- 「プロキシ レポート機能」（P.33-6）
- 「明示的ホスト トラッキング」（P.33-7）

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 では送信元ベース フィルタリングが使用されます。送信元ベース フィルタリングでは、特定マルチキャスト グループでどの送信元アドレスを許可するかブロックするかをホストおよびルータによって特定できるようにします。Cisco 7600 シリーズ ルータで 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。送信元専用エントリは 5 分ごとに削除されて再学習され、そのエントリが有効であることが確認されます。

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 ベースのメンバー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たく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。このようなメッセージをホストから受信すると、ルータは所定のグループに対応する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脱退メッセージで受信された送信元リストとまったく同じである場合、ルータはこのホストを LTL インデックスから削除し、ホストへのマルチキャスト グループ トラフィックの転送を停止します。

送信元リストが一致しない場合、このホストがど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、ルータは LTL インデックスからホストを削除しません。

プロキシ レポート機能

IGMP では、IGMPv1 メッセージおよび IGMPv2 メッセージでプロキシ レポート機能がサポートされ、グループ固有のクエリーが処理されます。このクエリーはダウンストリームに送信されませんが、スイッチはクエリーに直接応答します。スイッチは、グループ固有のクエリーを受信すると、グループのレシーバがある場合、クエリーを終了して 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 レポート機能がありません。IGMPv3 の場合は、グループ固有のクエリーまたはグループ送信元固有のクエリーが、すべての VLAN メンバ ポートにフラッディングされます。IGMPv3 メンバーシップ レポートのデータベースは、受信した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って抑制できます。レポート抑制は、IGMPv1、IGMPv2、IGMPv3 のメッセージでサポートされます。レポート抑制がイネーブルな状態では（デフォルト）、スイッチが、一般クエリーを受信したとき、すべてのホストから各グループまたはチャネル（S,G）へのレポート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だけが転送されます。残りのレポートは抑制されます。IGMPv1 および IGMPv2 の場合、抑制の時間は、一般的なクエリー メッセージに示されているレポート応答時間です。IGMPv3 の場合、抑制は一般的なクエリー間隔全体で行われます。

（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。送信元専用エントリは 5 分ごとに削除されて再学習され、そのエントリが有効であることが確認されます。
- 明示的ホスト 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 レポート機能はディセーブルになります。

明示的ホスト トラッキング

IGMPv3 では、ポート上のメンバーシップ情報の明示的な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、および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 レポートを処理し、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
- ホストによって報告されたチャネル
- ホストによって報告された各グループのフィルタ モード
- ホストによって報告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 レポート機能はディセーブルになります。
- 明示的なトラッキングがイネーブル化されていて、ルータがプロキシレポート 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背後にあるホストの一部を追跡できないことがあります。

IGMP スヌーピングのデフォルト設定

表 33-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 33-3　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	未設定
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 SSM セーフ レポート機能	ディセーブル

IGMP スヌーピング設定時の注意事項および制約事項

IGMP スヌーピングの設定時には、次の注意事項および制約事項に従ってください。

- Cisco Group Management Protocol（CGMP）クライアント デバイス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」の「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 クエリアの設定時には、次の注意事項および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 を設定してください（第 14 章「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 スヌーピング クエリアは、イネーブルになっている場合、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 クエリアは、イネーブルの場合でも、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起動しません。
- IGMP スヌーピング クエリアは、イネーブルの場合、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、60 秒後に起動します。
- IGMP スヌーピング クエリアは、イネーブルの場合でも、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、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、QoS は IGMP パケットをサポートしません。
- VLAN 内のすべての Cisco 7600 シリーズ ルータで、IGMP スヌーピング クエリアをイネーブルにできます。ルータの 1 つがクエリアとして選定されます。

（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。

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 querier is enabled on this interface
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 31 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.33-9）を参照）。

IGMP スヌーピングにより、Cisco 7600 シリーズ ルータで 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することができます。

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.33-10）
- 「マルチキャスト レシーバへのスタティック接続の設定」（P.33-11）
- 「マルチキャスト ルータ ポートのスタティックな設定」（P.33-12）
- 「IGMP スヌーピング クエリー時間の設定」（P.33-12）
- 「IGMP 高速脱退処理のイネーブル化」（P.33-13）
- 「送信元固有マルチキャスト（SSM）マッピングの設定」（P.33-13）
- 「SSM セーフ レポート機能のイネーブル化」（P.33-13）
- 「IGMPv3 明示的ホスト トラッキングの設定」（P.33-14）
- 「IGMP スヌーピング情報の表示」（P.33-14）

（注）　グローバルなイネーブル 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 レシーバへのスタティック接続の設定

マルチキャスト レシーバ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** キーワードを入力して、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 内の別のポートへ送信されるのを防止します。

次に、マルチキャスト レシーバ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 内である必要があります。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、ルータ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。

ルータ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*	ルータ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）
- IGMPv3 マルチキャスト レシーバをサポートする 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、次の資料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）Source-specific Multicast（SSM）セーフ レポート機能は、現在は推奨していません。

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 になります。

ルータが同じ VLAN 内で IGMPv1、IGMPv2、および IGMPv3 ホストを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 ホストを両方サポートするようにルータ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 明示的ホスト トラッキングの設定

特定の VLAN で明示的ホスト 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」（P.33-15）
- 「MAC アドレス マルチキャスト エントリの表示」（P.33-15）
- 「VLAN インターフェイスの IGMP スヌーピング情報の表示」（P.33-15）
- 「IGMP スヌーピング統計情報の表示」（P.33-16）

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、ルータはマルチキャスト 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、特定の 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のリスト
- フィルタ モード
- ポートの下位の reporter-address
- 最後に **clear ip igmp snooping statistics** コマンドを入力した以降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#
```

MVR の概要

マルチキャスト VLAN レジストレーション（MVR）は、イーサネット リングベースのサービス プロバイダー ネットワークでマルチキャスト トラフィックを展開するために使用されます。たとえば、サービスプロバイダー ネットワークによる複数のテレビ チャネルのブロードキャストなどが挙げられます。

MVR は次のことを実行します。

- MVR IP マルチキャスト ストリームとそれに関連するレイヤ 2 転送テーブルの IP マルチキャスト グループを識別します。
- IGMP メッセージを代行受信します。
- ポートの加入者をマルチキャスト VLAN のマルチキャスト ストリームに加入させたり、そこから脱退させることができます。
- 加入者は別個の VLAN 上に存続しながら、ネットワークで単一のマルチキャスト VLAN を共有できます。
- マルチキャスト VLAN でマルチキャスト ストリームを継続的に送信しながら、帯域幅とセキュリティを確保するために、ストリームと加入者の VLAN を分離できます。
- 受信者が送信元とは別の VLAN に存在する場合でも、レイヤ 2 転送テーブルで、マルチキャスト ストリームの受信者として加入者を含めるか、または削除するよう変更します。この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

ルータは、MVR IP マルチキャスト ストリームのマルチキャスト データを、IGMP レポートまたは MVR の静的設定のいずれかを使用して、ホストが加入した MVR ポートに対してのみ転送します。ルータは、MVR ホストから受信した IGMP レポートを送信元（アップリンク）ポートに対してだけ転送します。これにより、MVR データ ポート リンク上で不要な帯域幅が使用されなくなります。

（注）　MVR に参加するのは、レイヤ 2 ポートだけです。ポートを MVR 受信ポートとして設定する必要があります。ルータ 1 台につき MVR マルチキャスト VLAN を 1 つのみ使用できます。

MVR の実行時には、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退を行います。これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能は相互に独立して動作します。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

マルチキャスト TV アプリケーションでの MVR の使用

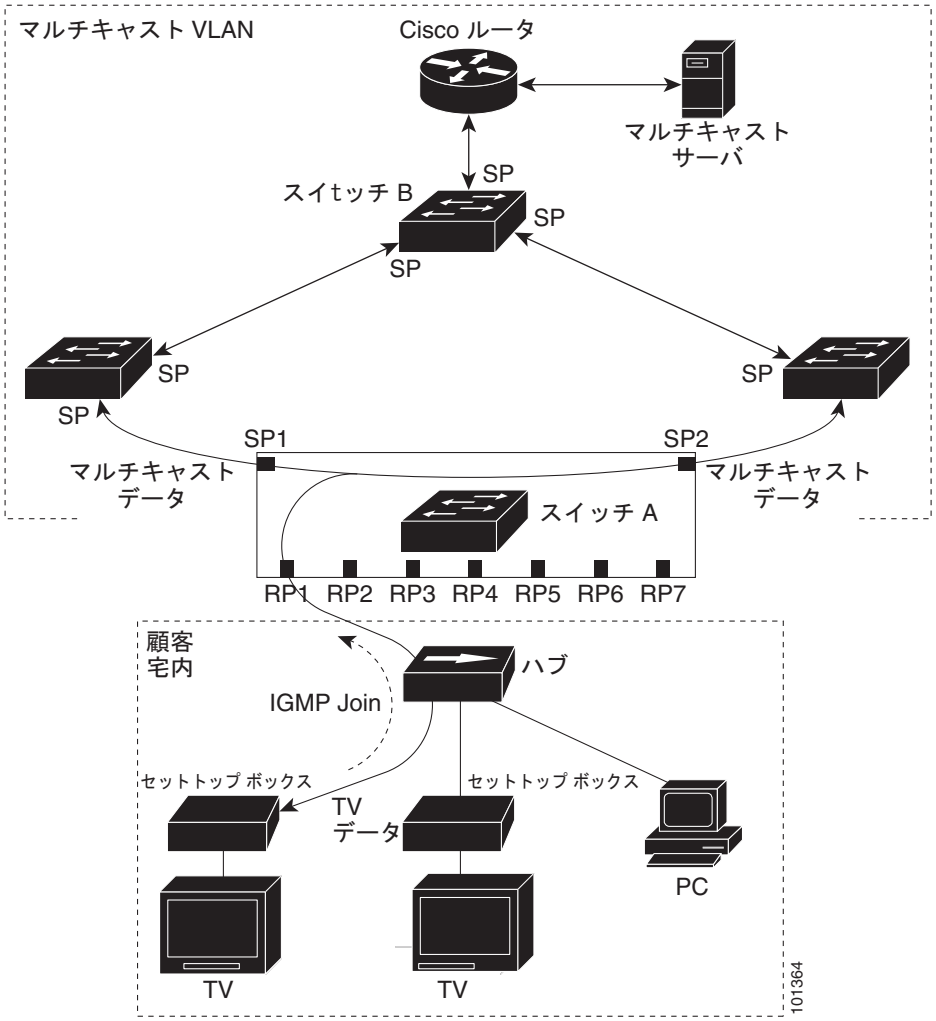
マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信します。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR 受信ポートとして設定されたスイッチ ポートです。図 33-3 に、この設定を示します。

マルチキャスト TV アプリケーションにおける MVR 機能は、次の順序で機能します。

- Dynamic Host Configuration Protocol（DHCP）によって、セットトップ ボックスまたは PC に IP アドレスが割り当てられます。加入者がチャネルを選択すると、適切なマルチキャストに加入するために、セットトップ ボックスまたは PC からスイッチ A に IGMP レポートが送信されます。IGMP レポートが設定済みの IP マルチキャスト グループ アドレスのいずれかと一致した場合、

Source Port（SP; 送信元ポート）の CPU は、この受信ポートと VLAN が、指定のマルチキャスト ストリームをマルチキャスト VLAN から受信した際の転送先として含まれるように、ハードウェア アドレス テーブルを変更します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

図 33-3　　マルチキャスト VLAN レジストレーション



RP = レシーバー ポート
SP = 送信元ポート

注：　すべての送信元ポートは
マルチキャスト VLAN に所属します。

- 加入者がチャネルを切り替えるか、テレビのスイッチを切ると、セットトップ ボックスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。SP CPU は、受信ポートの VLAN を介して MAC ベースの一般クエリーを送信します。VLAN に、このグループに加入している別のセットトップ ボックスがある場合、そのセットトップ ボックスはクエリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はこのグループの転送先としての受信ポートを除外します。
- 即時脱退機能がイネーブルでない場合、ルータは受信ポートの加入者から IGMP Leave メッセージを受信すると、そのポートに IGMP クエリーを送信し、IGMP グループ メンバーシップ レポートを待ちます。設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバーシップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信した受信ポートから、IGMP クエリーは送信されません。Leave メッセージの受信後ただちに、

受信ポートがマルチキャスト グループ メンバーシップから削除されるので、脱退遅延時間が短縮されます。即時脱退機能は、1 つの受信デバイスが接続された受信ポートでのみイネーブルにしてください。

- MVR を使用すると、各 VLAN の加入者に対してテレビ チャネルのマルチキャスト トラフィックを重複して送信する必要がなくなります。すべてのチャネル用のマルチキャスト トラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランクに 1 回だけ送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN で送信されます。これらのメッセージにより、レイヤ 3 デバイス（スイッチ B）上のマルチキャスト VLAN 内のマルチキャスト トラフィック ストリームが、ダイナミックに登録されます。アクセス レイヤ スイッチ（スイッチ A）は、2 つの VLAN 間でのトラフィック伝送を選択的に許可し、マルチキャスト VLAN から別の VLAN 上の加入者ポートにトラフィックが転送されるように転送動作を変更します。
- IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されます。スイッチ A の CPU は、受信ポートからのすべての IGMP Join および Leave メッセージを取り込んで、送信元（アップリンク）ポートのマルチキャスト VLAN に転送する必要があります。

MVR の設定

ここでは、MVR の設定情報について説明します。

- MVR のデフォルト設定
- MVR 設定の制約事項
- MVR グローバル パラメータの設定
- MVR インターフェイスの設定
- MVR 情報の表示
- MVR カウンタのクリア

MVR のデフォルト設定

表 33-4 に、MVR のデフォルト設定を示します。

表 33-4　MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
MVR 最大グループ数	最大 1000 グループ
マルチキャスト アドレス	未設定
クエリーの応答時間	1 秒
マルチキャスト VLAN	VLAN 1
インターフェイスのデフォルト（ポート単位）	受信ポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定の制約事項

MVR には、次の制約事項が適用されます。

- ルータ 上に存在できる MVR VLAN は 1 つだけで、同一ネットワーク内のすべてのルータで MVR VLAN と同じ VLAN を設定する必要があります。
- 送信元ポートは、MVR VLAN 内に存在できません。
- ルータの受信ポートは別の VLAN 内に存在できますが、MVR VLAN 内には存在できません。
- 受信ポートはアクセス ポートでなければなりません。トランク ポートにはできません。
- VLAN の受信ポートには、その VLAN 上で IGMP クエリーを生成するためにスヌーピング クエリアまたは L3 SVI のいずれかが必要です。
- プライベート VLAN を使用する場合、プライマリまたはセカンダリ VLAN を MVR VLAN として設定することはできません。
- マルチキャスト ルータを受信ポートに接続しないでください。
- MVR VLAN を、マルチキャスト ルートの RPF インターフェイスにしないでください。
- MVR 受信ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- ルータのマルチキャスト エントリ（MVR グループ アドレス）の最大数（受信したテレビ チャネルの最大数）は 8000 です。
- MVR は、ネイティブ システムだけで使用できます。
- MVR VLAN の数が 1 ～ 1000 である場合は、VTP プルーニングをディセーブルにする必要があります。
- MVR はルータで IGMP スヌーピングと共存できます。
- MVR は、IGMPv3 メッセージをサポートします。
- MVR は ES-20 ポートのストーム制御と共存できません。
- レイヤ 2 ポート チャネルが MVR 受信ポートとして設定されている場合、MVR グループからのマルチキャスト データ トラフィックはメンバー リンクの外には転送されません。

MVR グローバル パラメータの設定

デフォルト設定を使用して、MVR のグローバル パラメータを設定できます。個別のアクションについては、必要に応じてオプション設定を使用します。デフォルトのパラメータ（MVR VLAN を除く）を変更する前に、まず MVR をイネーブルにする必要があります。

MVR 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
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)# mvr`	ルータで MVR をイネーブルにします。
ステップ 3	`Router(config)# mvr max-groups` *max-groups*	MVR グループの最大数を指定します。範囲は 1 ～ 8000 です。デフォルト値は 1000 です。

	コマンド	目的
ステップ 4	Router(config)# **mvr group** *ip-address* [**count** *count* | [**mask** *mask*]]	ルータ上で IP マルチキャスト アドレスを設定するか、または count パラメータを使用して、連続する MVR グループ アドレスを設定します。count の範囲は 1 ～（max-groups 現在カウント）で、デフォルトは 1 です。このアドレスに送信されたマルチキャスト データは、ルータ上のすべての送信元ポート、およびそのマルチキャスト アドレスのデータを受信することを選択したすべての受信ポートに送信されます。各マルチキャスト アドレスは 1 つのテレビ チャネルに対応します。mask は、MVR グループ アドレスの IP マスクを指定します。
ステップ 5	Router(config)# **mvr querytime** *value*	（任意）マルチキャスト グループ メンバーシップからポートを削除する前に、受信ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は 10 分の 1 秒単位で設定します。範囲は 1 ～ 100 で、デフォルトは 10 分の 10 秒、つまり 1 秒です。
ステップ 6	Router(config)# **mvr vlan** *vlan-id*	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。VLAN の範囲は 1 ～ 1001 および 1006 ～ 4094 です。デフォルトは 1 です。
ステップ 7	outer(config)# **end**	特権 EXEC モードに戻ります。
ステップ 8	Router# **show mvr**	設定を確認します。

デフォルト設定に戻すには、**no mvr** [**group** *ip-address* | **querytime** | **vlan**] グローバル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにし、グループ アドレスを設定し、クエリー時間を 1 秒（10/10）に設定し、MVR マルチキャスト VLAN を VLAN 22 に指定する例を示します。

```
Router(config)# mvr
Router(config)# mvr group 228.1.23.4 256
Router(config)# mvr querytime 10
Router(config)# mvr vlan 22
Router(config)# end
```

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、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)# mvr`	ルータで MVR をイネーブルにします。
ステップ 3	`Router(config)# interface interface-id`	設定するレイヤ 2 ポートを指定して、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 4	`Router(config-if)# mvr type {source | receiver}`	MVR ポートを、次のポート タイプのいずれかに設定します。 • source：マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。ルータ上のすべての送信元ポートは、単一マルチキャスト VLAN に属します。 • receiver：ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合には、ポートを受信ポートとして設定します。受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。受信ポートをマルチキャスト VLAN に所属させることはできません。 非 MVR ポートに MVR 設定を行おうとしても、エラーになります。デフォルトでは、非 MVR ポートとして設定されます。
ステップ 5	`Router(config-if)# mvr immediate`	（任意）ポート上で MVR の即時脱退機能をイネーブルにします。この機能は、デフォルトでディセーブルです。 このコマンドが適用されるのは、受信ポートだけです。また、イネーブルにするのは、単一の受信デバイスが接続されている受信ポートに限定してください。
ステップ 6	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router# show mvr`	設定を確認します。

デフォルト設定に戻すには、**no mvr [type | immediate]** インターフェイス コンフィギュレーション コマンドを使用します。

次に、送信元ポートおよび受信ポートを設定し、受信ポート上で即時脱退機能を設定する例を示します。

```
Router(config)# mvr
Router(config)# interface gigabitethernet 3/48
Router(config-if)# switchport
Router(config-if)# switchport access vlan 22
Router(config-if)# mvr type source
Router(config-if)# exit
Router(config)# interface gigabitethernet 3/47
```

```
Router(config-if)# switchport
Router(config-if)# switchport access vlan 30
Router(config-if)# mvr type receiver
Router(config-if)# mvr immediate
Router(config-if)# exit
```

MVR 情報の表示

ルータまたは指定されたインターフェイスの MVR 情報を表示できます。MVR 設定を表示するには、次の作業の 1 つ以上を実行します。

コマンド	目的
`Router# show mvr`	MVR ステータスを次の情報とともに表示します。 • MVR（True または False） • マルチキャスト VLAN • マルチキャスト グループの設定最大値および現在の数 • クエリー応答時間
`Router# show mvr groups`	MVR グループの設定を、マルチキャスト グループの最大および現在の情報とともに表示します。
`Router# show mvr interface` [*type module/port*]	すべての MVR インターフェイスおよびその MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。 • Type：Receiver または Source • Status：次のいずれか – Active：ポート上の MVR グループに対して、少なくとも 1 つの IGMP Join メッセージが受信されている。 – Inactive：ポートはいずれの MVR グループにも参加していない。 – Up/Down：ポートは転送中（Up）または非転送中（Down）である。 • Immediate Leave：Enabled または Disabled
`Router# show mvr members` [[**vlan** *vlan-id*] | [*type module/port*]] **count**	すべての MVR メンバーの詳細、およびすべてのアクティブな MVR グループ内、または指定された VLAN あるいはポート上の MVR メンバーの数（カウント）を表示します。
`Router# show mvr` {**receiver-ports** | **source-ports**} [*type module/port*]	いずれかの IP マルチキャスト グループのメンバーであるか、指定されたインターフェイス ポート上にある受信ポートまたは送信元ポートをすべて表示します。

次に、ルータの MVR ステータスおよび値を表示する例を示します。

```
Router# show mvr
MVR Running: TRUE
MVR multicast vlan: 22
MVR Max Multicast Groups: 1000
MVR Current multicast groups: 256
MVR Global query response time: 10 (tenths of sec)
```

次に、MVR グループの設定を表示する例を示します。

```
Router# show mvr groups
MVR max Multicast Groups allowed: 8000
MVR current multicast groups: 8000
MVR groups:
        Group start     Group end       Type  Count/Mask
        --------------- --------------- ----- ---------------
        225.0.7.226     225.0.7.226     count 1
        225.0.7.227     225.0.7.227     count 1
        225.0.7.228     225.0.7.228     count 1
        225.0.7.229     225.0.7.229     count 1
        225.0.7.230     225.0.7.230     count 1
        225.0.7.231     225.0.7.231     count 1
        236.8.7.0       236.8.7.255     mask  255.255.255.0
        237.8.7.0       237.8.7.255     mask  255.255.255.0
        237.8.8.0       237.8.8.255     mask  255.255.255.0
```

次に、すべての MVR インターフェイスおよび設定を表示する例を示します。

```
Router# show mvr interface
Port      VLAN  Type       Status           Immediate Leave
----      ----  ----       ------           ---------------
Gi1/20       2  RECEIVER   ACTIVE/UP        DISABLED
Gi1/21       2  SOURCE     ACTIVE/UP        DISABLED
```

次に、VLAN 2 上のすべての MVR メンバーを表示する例を示します。

```
Router# show mvr members vlan 2
MVR Group IP      Status     Members             VLAN
------------      ------     -------             -----
224.000.001.001   ACTIVE     Gi1/20(u),Gi1/21(u)  2
224.000.001.002   ACTIVE     Fa3/2(d),Gi1/12(u)   2
```

次に、すべての MVR VLAN 上の MVR メンバー数を表示する例を示します。

```
Router# show mvr members count
Count of active MVR groups:
Vlan 490: 400
Vlan 600: 400
Vlan 700: 0
Vlan 950: 0
```

次に、いずれかの IP マルチキャスト グループのメンバーである受信ポートすべてを表示する例を示します。

```
Router# show mvr receiver-ports
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port   VLAN Status          Immediate            Joins
                              Leave          (v1,v2,v3)     (v3)
----   ---- -------------  ----------   ---------- -----------
Gi1/7   202 INACTIVE/UP    ENABLED           305336             0
Gi1/8   202 ACTIVE/UP     DISABLED             4005             0
Gi1/9   203 INACTIVE/DOWN DISABLED           53007            0
Gi1/10  203 ACTIVE/UP      DISABLED             6204             0
Gi1/11  204 ACTIVE/UP      DISABLED                0           940
```

```
Gi1/12   205 INACTIVE/UP     ENABLED              8623              0
```

MVR カウンタのクリア

ルータ、送信元ポートまたは受信ポート、あるいは指定されたインターフェイスの MVR Join カウンタをクリアできます。

MVR 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 mvr counters [[receiver-ports | source-ports]** [*type module/port*]]	すべての MVR ポート、送信元ポートまたは受信ポート、あるいは指定された MVR インターフェイス ポートの Join カウンタをクリアします。

次に、ギガビット イーサネット ポート 1/7 の受信ポートの Join カウンタをクリアする例を示します。

```
Router# clear mvr receiver-ports GigabitEthernet 1/7
Router# show mvr receiver-ports GigabitEthernet 1/7
Joins: v1,v2,v3 counter shows total IGMP joins
       v3 counter shows IGMP joins received with both MVR and non-MVR groups
Port    VLAN Status           Immediate             Joins
                                 Leave          (v1,v2,v3)      (v3)
----    ---- -------------   -----------    ---------- -----------
Gi1/7    202 INACTIVE/UP     ENABLED                 0             0
```

トラブルシューティング

表 33-5 では、MVR の設定時に発生する問題のトラブルシューティングについて示します。

表 33-5　MVR の問題のトラブルシューティング

問題	ソリューション
MVR 受信ポートがトラフィックを受信しない、または MVR グループからのデータ トラフィックが MVR VLAN 上で送信されない場合。	• **show mac-address table vlan** *mvr vlan* コマンドを使用して、MAC アドレスのエントリを確認します。 • **show mvr receiver ports** コマンドを使用して、MVR 受信ポートのステータスを確認します。 • 次のデバッグ コマンドを使用して、MVR 受信ポート上の MVR グループに対する IGMP Join が MVR VLAN にリダイレクトされているかどうかを確認します。 – **debug mvr all** – **debug platform software multicast igmp event** – **debug platform software multicast igmp pak**

CHAPTER 34

PIM スヌーピングの設定

この章では、Cisco 7600 シリーズ ルータに 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。

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.34-1）
- 「PIM スヌーピングのデフォルト設定」（P.34-4）
- 「PIM スヌーピング設定時の注意事項および制約事項」（P.34-4）
- 「PIM スヌーピングの設定」（P.34-4）

PIM スヌーピングの機能概要

レイヤ 2 ルータが Internet Exchange Point（IXP）など複数のルータと相互接続しているネットワークでは、マルチキャスト レシーバ ダウンストリームが存在しない場合でも、ルータはデフォルトで、すべてのマルチキャスト ルータ ポートで 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、ルータは各 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、そのグループに加入しているダウンストリーム レシーバが接続されたマルチキャスト ルータ ポートに限定します。PIM スヌーピングをイネーブルにすると、ルータは PIM Hello メッセージ、PIM Join と Prune メッセージ、および双方向 PIM 指定フォワーダ選定メッセージをリッスンして、特定の VLAN 内でマルチキャスト 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、Cisco 7600 シリーズ ルータ上で 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 34-1 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 34-1　PIM スヌーピングがない場合の PIM Join メッセージ フロー

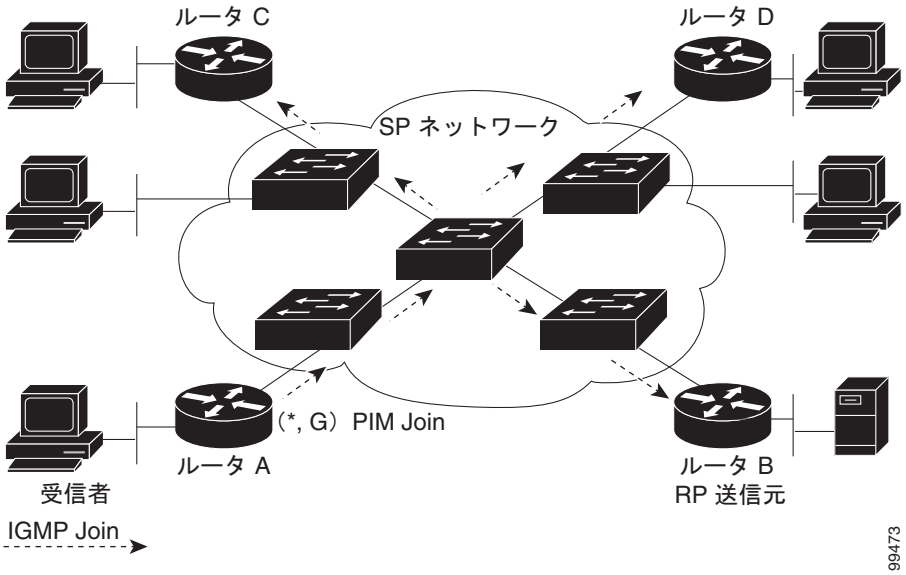


図 34-2 では、PIM スヌーピングがイネーブルの場合の PIM Join メッセージ フローを示します。この図では、スイッチは PIM Join メッセージを制限し、このメッセージを受信する必要があるルータ（ルータ B）だけに転送します。

図 34-2　PIM スヌーピングがある場合の PIM Join メッセージ フロー

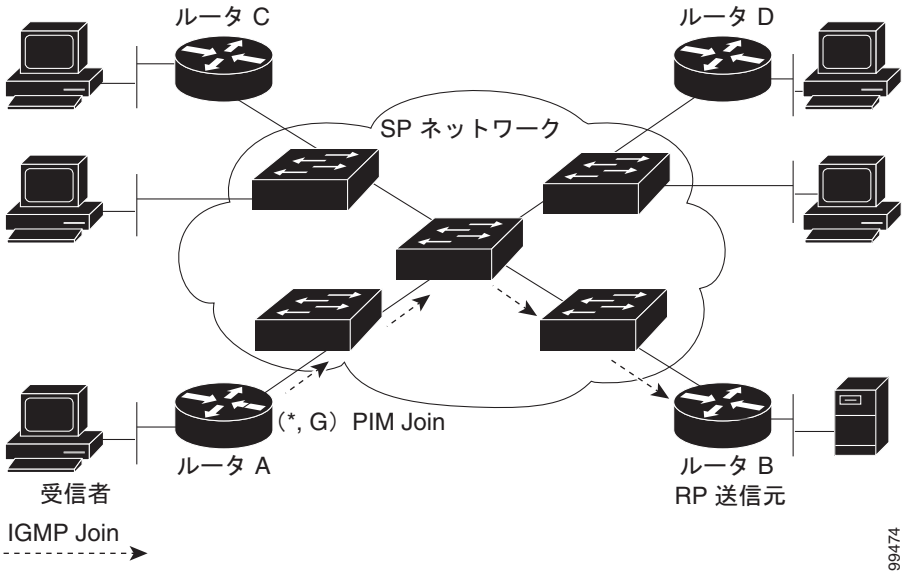


図 34-3 では、PIM スヌーピングがイネーブルでない場合のデータ トラフィック フローを示します。この図では、スイッチはルータ A を対象としたデータ トラフィックを接続されたすべてのルータにフラッディングします。

図 34-3　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

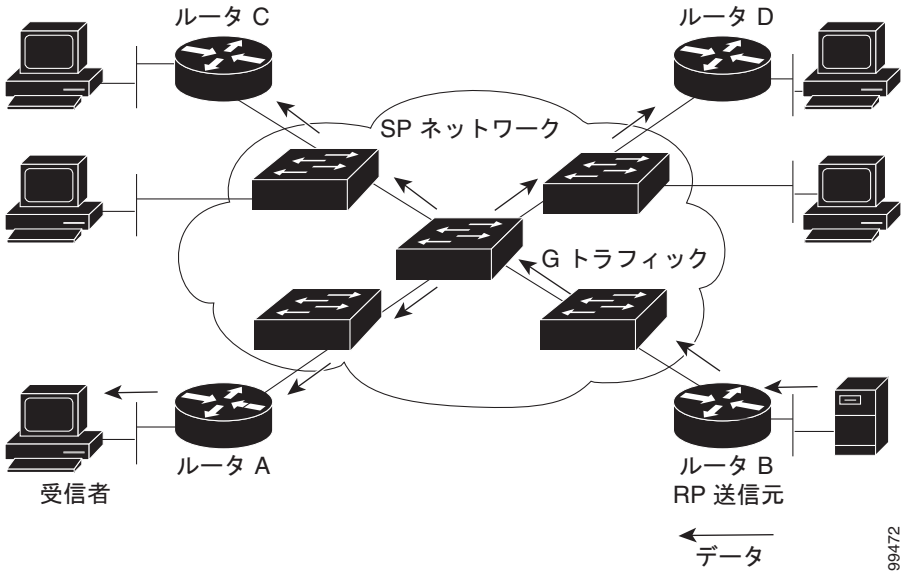
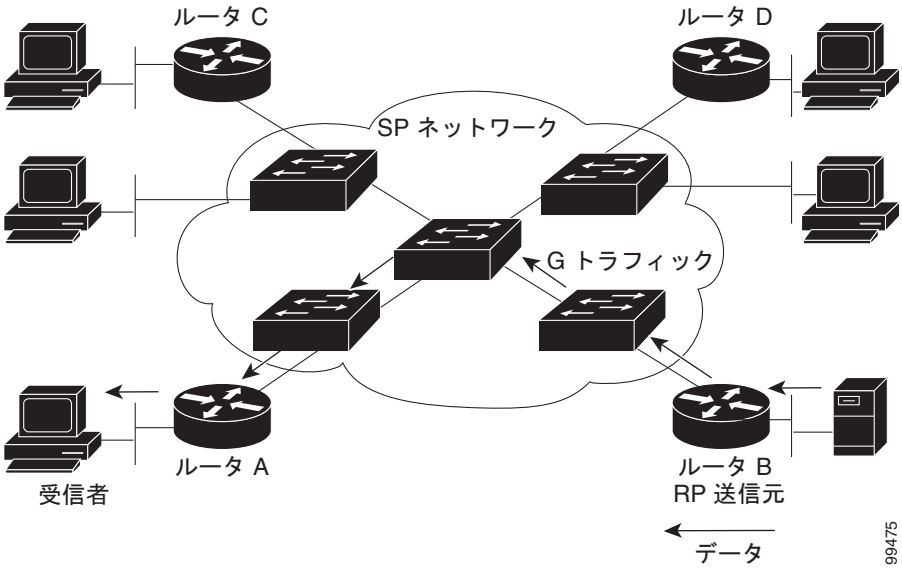


図 34-4 では、PIM スヌーピングがイネーブルの場合のデータ トラフィック フローを示します。この図では、スイッチはデータ トラフィックを受信する必要があるルータ（ルータ A）だけに転送します。

図 34-4　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 スヌーピングの設定時には、次の注意事項および制約事項に従ってください。

- PIM スパース 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係を示す場合、トラフィックだけを監視します。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、トラフィックだけを監視します。
- 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だけ、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。送信元だけ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だけに転送されます。
- 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ドロップされます。
- 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。
- ルータは指定フォワーダ選定時にスヌーピングし、VLAN の各 RP についてすべての指定フォワーダ ルータ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。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することができます。
- 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ー情報はすべて 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.34-5）
- 「VLAN における PIM スヌーピングのイネーブル化」（P.34-5）
- 「PIM スヌーピング指定ルータ フラッディングのディセーブル化」（P.34-6）

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 における 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 スヌーピング指定ルータ フラッディングのディセーブル化

（注）
- PIM スヌーピング DR フラッディング拡張機能は、Supervisor Engine 720 でサポートされます。
- 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 ドメインのルータにおいて、指定ルータ フラッディングをディセーブルにしないでください。

デフォルトの場合、PIM スヌーピングをイネーブルにしているルータは、指定ルータ（DR）にマルチキャスト トラフィックをフラッディングします。この方法による動作では、不必要なマルチキャスト パケットが指定ルータに送信されることがあります。ネットワークは不必要なトラフィックを搬送する必要があり、指定ルータは不必要なトラフィックを処理してドロップする必要があります。

ネットワークで指定ルータに送信されるトラフィックを減らすには、指定ルータ フラッディングをディセーブルにします。指定ルータ 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、PIM スヌーピングが指定ルータへのリンクから明示的な Join を受信するマルチキャスト グループ内にあるトラフィックだけを指定ルータに渡します。

PIM スヌーピング指定ルータ 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 スヌーピング指定ルータ 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 スヌーピング指定ルータ 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 35

ネットワーク セキュリティの設定

この章では、Cisco 7600 シリーズ ルータ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 の『*Cisco IOS Security Configuration Guide*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html
- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

(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、次の資料を参照してください。

- 次の URL の『*Cisco 7600 Series Router Cisco IOS Command Reference*』
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.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

この章の内容は、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」（P.35-1）
- 「TCP インターセプトの設定」（P.35-2）
- 「ユニキャスト RPF チェックの設定」（P.35-2）

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 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 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、次の 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/en/US/docs/ios/12_2/security/configuration/guide/scfdenl.html

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; リバース パス転送）チェック（ユニキャスト RPF チェック）について説明します。

- 「PFC3 ユニキャスト RPF チェックのサポートの概要」（P.35-2）
- 「ユニキャスト RPF チェックに関する注意事項および制約事項」（P.35-3）
- 「ユニキャスト RPF チェックの設定」（P.35-3）

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 チェックの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/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

PFC3 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ックスすべてに対し 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（インターフェイス グループごとに 4 つのインターフェイスを収容可能）のいずれかを通じて到達したプレフィックスに対し最大 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。

ユニキャスト RPF チェックに関する注意事項および制約事項

ユニキャスト RPF チェックの設定時には、次の注意事項および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、ACL 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、MSFC がユニキャスト 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（CSCdz35099）を行わずにハードウェアで転送されます。
- 通常、DoS 攻撃のパケットは拒否 ACE と一致し、ユニキャスト RPF チェックを行うため MSFC に送信されます。そのため、送信されたパケットが MSFC を過負荷状態にす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.35-3）
- 「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.35-5）
- 「self-ping のイネーブル化」（P.35-6）

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 FIB 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 モードを設定する際、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 モードがルータ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 mpath {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 mpath {punt | interface-group}`	デフォルト値に戻します（**mls ip cef rpf mpath 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）：プレフィックスごとに最大 2 つのインターフェイスに対して、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。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** : パスが 1 つまたは 2 つのプレフィックスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。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 プレフィッ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** : パスが 1 つまたは 2 つのプレフィックスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。PFC3 はプレフィックス単位で最大 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 プレフィッ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 mpath 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、ルータはデフォルトで 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** Router(config-if)# **no 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、ルータをイネーブルにします。 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 36

Cisco IOS ACL サポートの概要

この章では、Cisco 7600 シリーズ ルータの Cisco IOS ACL サポートについて説明します。

- 「Cisco IOS ACL 設定時の注意事項および制約事項」（P.36-1）
- 「ハードウェアおよびソフトウェア ACL のサポート」（P.36-2）
- 「PFC3 での最適化 ACL ロギング」（P.36-3）
- 「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」（P.36-5）

Cisco IOS ACL の設定方法については、次の URL にある『*Cisco IOS Security Configuration Guide*, Release 12.2』を参照してください。

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

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 VLAN 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 37 章「VACL の設定」を参照）。
- 各タイプの ACL（IP、IPX、および MAC）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 トラフィックを照合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。
- アクセス コントロール エントリ（ACE）の一致 IP オプションは、ハードウェア転送パスではサポートされません。

ハードウェアおよびソフトウェア ACL のサポート

アクセス コントロール リスト（ACL）は、ハードウェアの場合には Policy Feature Card（PFC; ポリシー フィーチャ カード）、Distributed Forwarding Card（DFC; 分散型フォワーディング カード）で、ソフトウェアの場合には Multilayer Switch Feature Card（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。

- PFC では、番号付き ACL より名前付き ACL の方がより効率的にハードウェアでサポートされます。
- 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、「ip unreachables」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ドロップされます。
- 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。
- VLAN ACL（VACL）フローはハードウェアで処理されます。VACL で指定されたフィールドのハードウェア処理がサポートされていない場合、このフィールドは無視されるか（ACL の **log** キーワードなど）、または設定全体が拒否されます（IPX ACL パラメータを含む VACL など）。
- VACL ロギング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。Cisco 7600 シリーズ ルータでは **access-enable host timeout** コマンドがサポートされません。

- 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 コントロールされません。

- 最適化 ACL ロギング（OAL）を設定しない限り、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 での最適化 ACL ロギング」（P.36-3）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一致カウントには、ハードウェアで処理されたパケットは含まれません。

PFC3 での最適化 ACL ロギング

ここでは OAL について説明します。

- 「OAL の概要」（P.36-3）
- 「OAL に関する注意事項および制約事項」（P.36-3）
- 「OAL の設定」（P.36-4）

OAL の概要

Optimized ACL Logging（OAL; 最適化 ACL ロギング）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。

- OAL キャプチャと VACL キャプチャには互換性がありません。ルータで両方の機能を一緒に設定しないでください。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 だけでサポートされます。
- OAL は IPv4 ユニキャスト パケットだけ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、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
  - 例外パケット（存続可能時間（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。

- 「OAL グローバル パラメータの設定」（P.36-4）
- 「インターフェイスでの OAL の設定」（P.36-5）
- 「OAL 情報の表示」（P.36-5）
- 「キャッシュされた OAL エントリのクリア」（P.36-5）

（注）
- このセクション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 7600 Series Router Cisco IOS Command Reference*』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（カンマを含めないで入力）。
  - デフォルト：8000
- **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、カンマを含めないで入力）。
  - 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（カンマを含めないで入力）。
  - 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（カンマを含めないで入力）。
- 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」（P.36-6）
- 「論理演算ユニットの使用」（P.36-6）

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（geater 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、*9* つより多くの*異なる*演算を指定しないよう推奨します。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」演算子は論理演算ユニット（LOU）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、「論理演算ユニットの使用」（P.36-6）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
```

論理演算ユニットの使用

論理演算ユニット（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。

- LOU1 に、「gt 10」および「lt 9」が保存されます。
- LOU2 に、「gt 11」および「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（range は 1 LOU を使用）。

CHAPTER 37

VACL の設定

この章では、Cisco 7600 シリーズ ルータで VLAN ACL（VACL）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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- OAL キャプチャと VACL キャプチャには互換性がありません。ルータで両方の機能を一緒に設定しないでください。OAL が設定されている場合は（「PFC3 での最適化 ACL ロギング」（P.36-3）を参照）、SPAN 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」（P.37-1）
- 「VACL の設定」（P.37-4）
- 「VACL ロギングの設定」（P.37-10）

VACL の概要

ここでは VACL について説明します。

- 「VACL の概要」（P.37-1）
- 「ブリッジド パケット」（P.37-2）
- 「ルーティング対象パケット」（P.37-2）
- 「マルチキャスト パケット」（P.37-3）

VACL の概要

VACL は、VLAN 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 コントロールを行います。ルータ インターフェイスでのみ設定され、ルーティング対象パケットだけに適用される通常の 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、IPX、および MAC 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。

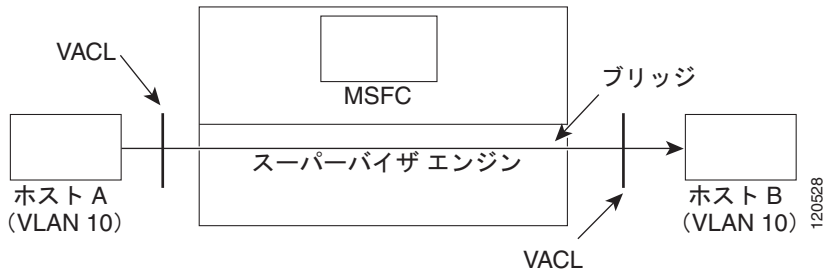
（注）

- 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 CBAC は、同じインターフェイス上に設定できません。
- IGMP パケットは VACL と照合されません。

ブリッジド パケット

図 37-1 に、ブリッジド パケットに適用される VACL を示します。

図 37-1　ブリッジド パケットへの VACL の適用

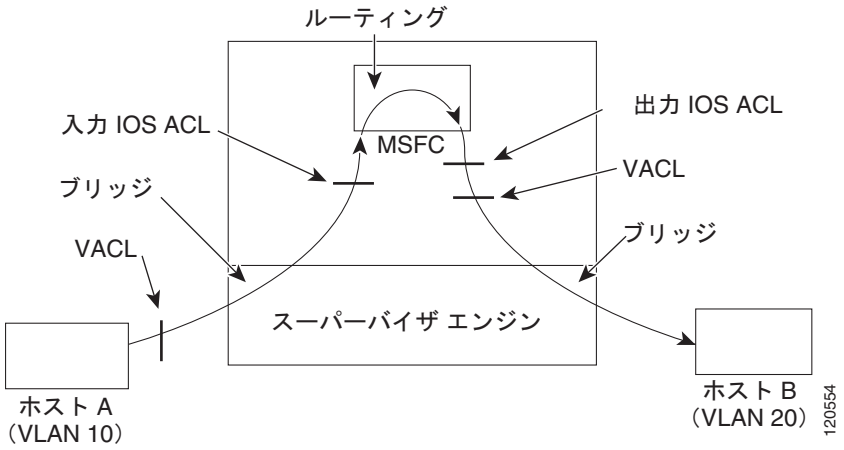


ルーティング対象パケット

図 37-2 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 37-2　ルーティング対象パケットへの VACL の適用

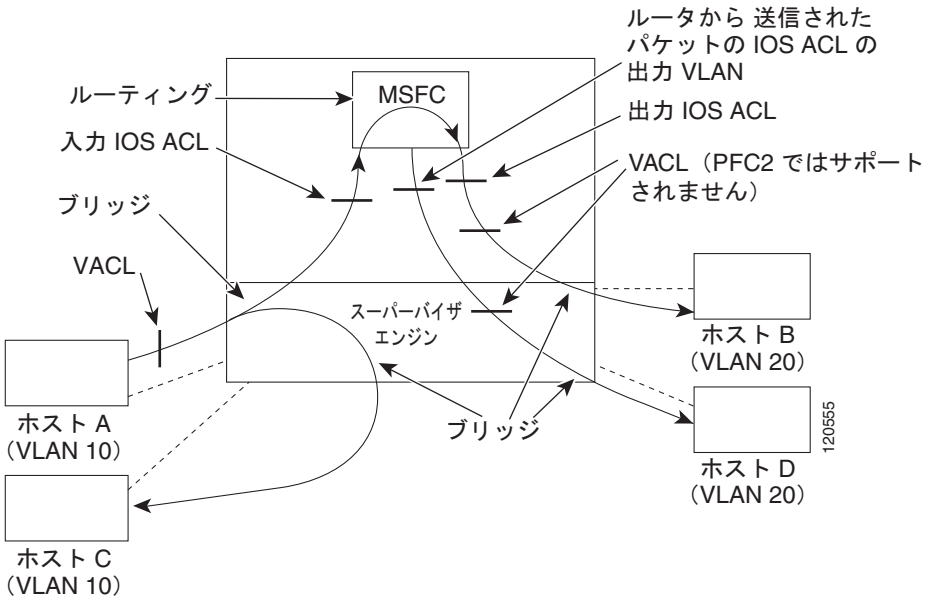


マルチキャスト パケット

図 37-3 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 37-3　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」（P.37-4）
- 「VLAN アクセス マップの定義」（P.37-5）
- 「VLAN アクセス マップ シーケンスでの match 句の設定」（P.37-6）
- 「VLAN アクセス マップ シーケンスでの action 句の設定」（P.37-6）
- 「VLAN アクセス マップの適用」（P.37-7）
- 「VLAN アクセス マップの設定の確認」（P.37-8）
- 「VLAN アクセス マップの設定および確認の例」（P.37-8）
- 「キャプチャ ポートの設定」（P.37-9）

VACL の設定の概要

VACL は標準および拡張 Cisco IOS IP と IPX ACL、MAC レイヤの名前付き ACL（「MAC ACL の設定」（P.45-58）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ッド トラフィックの両方にアクセス コントロールを使用するには、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ッド 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 コントロールを使用します。

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 でのロギング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 NAT 変換前のパケットに適用されます。アクセス コントロール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 コントロールされる場合があります。

VACL の action 句には、転送（forward）、ドロップ（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 マップを定義する際、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 句および action 句をそれぞれ 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。

（注）　VLAN アクセスマップを定義するときに、アクセスマップ名とスペースはアクセスマップ名で許可されないため、単語のみを使用する必要があります。たとえば、アクセスマップの命名に「map_name」は使用できますが、「map name」などの複数の単語を使用することはできません。

「VLAN アクセス マップの設定および確認の例」（P.37-8）を参照してください。

VLAN アクセス マップ シーケンスでの match 句の設定

VLAN アクセス マップ シーケンスに match 句を設定するには、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 句を設定します。
`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 句を削除します。

VLAN アクセス マップ シーケンスに match 句を設定する際、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 句を削除したり、match 句内の特定の 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 については、「MAC ACL の設定」（P.45-58）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/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html

「VLAN アクセス マップの設定および確認の例」（P.37-8）を参照してください。

VLAN アクセス マップ シーケンスでの action 句の設定

VLAN アクセス マップ シーケンスに action 句を設定するには、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 句を設定します。
`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 句を削除します。

VLAN アクセス マップ シーケンスに action 句を設定する際、次の情報に注意してください。

- パケットをドロップ、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、ドロップ、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.37-9）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、ドロップ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、ドロップされた 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 メンバーまたは 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。
- PFC3 を使用した場合、VACL がトラフィックを出力 SPAN 送信元ポートにリダイレクトすると、SPAN は VACL リダイレクトされたトラフィックをコピーしません。
- SPAN および RSPAN 宛先ポートは、VACL リダイレクトされたトラフィックを送信します。
- action 句を削除するか、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.37-8）を参照してください。

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。
`Router(config)# no vlan filter map_name [vlan-list vlan_list | interface type[1] number[2]]`	指定した VLAN または WAN インターフェイスから VLAN アクセス マップを削除します。

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 マップを適用する際、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 リスト、または VLAN ID 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備えていない 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。
- レイヤ 2 VLAN が存在しないか動作していない場合、VLAN に適用される VACL 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.37-8）を参照してください。

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ドロップ アクションによってドロップされます。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 パケットをドロップ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 トラフィックはドロップおよび記録され、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 パケットはドロップされます。

```
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 IEEE 802.1Q または 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.10-8）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.10-9）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 ポートを設定する際、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 リスト、または VLAN ID 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.10-8）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.10-13）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 ポートからルータ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 ロギングの設定

VACL ロギング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 分経過する前にしきい値に達している場合

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（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 ロギング 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 ロギングを設定するには、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.37-4）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 ロギング 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ドロップされます。
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ドロップされます。
ステップ 3	`Router(config)# vlan access-log threshold pkt_count`	ロギングしきい値を設定します。5 分経過する前にフローのしきい値に達すると、ロギング メッセージが生成されます。デフォルトでは、しきい値は設定されません。
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 ロギング 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 ロギング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 38

Private Hosts（PACL の使用）

この章では、Private Hosts 機能について説明します。この機能は、Cisco 7600 シリーズ ルータ用に Cisco IOS Release 12.2SRB で導入されています。この章の内容は、次のとおりです。

- 「概要」（P.38-1）
- 「設定時の注意事項および制限事項」（P.38-5）
- 「Private Hosts の設定」（P.38-9）
- 「コマンド リファレンス」（P.38-13）

概要

Private Hosts 機能を使用すると、VLAN のホスト間での Layer 2（L2; レイヤ 2）の分離を行うことができます。Private Hosts は、現在は Cisco 7600 ルータで使用できないプライベート VLAN 独立トランク機能に代わるものとして使用できます。

世界各国のサービス プロバイダー（SP）は、単一の物理インターフェイス（銅製またはファイバ）でトリプル プレイ サービス（音声、ビデオ、およびデータ）を顧客に提供するよう求められています。通常、トリプル プレイ サービスは、3 つの異なる VLAN で各ユーザに配信されます。ただし、ビデオ トラフィック用の VLAN については、複数のエンド ユーザによって共有される場合もあります。

Private Hosts 機能の主な利点として、次の機能があります。

- 同じ VLAN ID を共有するホスト（加入者）間でのトラフィックの分離
- 異なる加入者間での VLAN ID の再利用（使用可能な 4096 VLAN の効率的な使用による VLAN スケーラビリティの向上）
- MAC スプーフィングの防止による Denial of Service（DoS; サービス拒絶）攻撃の防止

プライベート ホスト機能は、Port-based Access Control List（PACL; ポートベース アクセス コントロール リスト）を使用して、純粋なレイヤ 2 ドメイン内部の信頼できるポート上でのホスト間のレイヤ 2 分離を可能にします。PACL では、ルータ ポートにレイヤ 2 フォワーディング制約を課すことによって、ホストが分離されます。

（注） Release 12.2SRB では、PACL は Private Hosts の一部としてだけサポートされます。独自の PACL は設定できません。代わりに、Private Hosts 設定に基づき、ルータにより PACL が作成されて適用されます。

以降のセクションでは、次の Private Hosts の概念について詳細に説明します。

- 「VLAN でのホストの分離」（P.38-2）

- 「トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）」（P.38-3）
- 「ポート ACL」（P.38-5）

VLAN でのホストの分離

通常、トリプル プレイ サービス（音声、ビデオ、およびデータ）は、3 つの異なる VLAN で各ユーザに配信されます。ただし、同じサービス セットの VLAN が複数のエンド ユーザ間で共有される場合もあります。たとえば、10 人のエンド ユーザすべてが同じサービス セットを受信する場合、Private Hosts を使用して、単一の VLAN セットで 10 人のエンド ユーザすべてにサービスを配信できます。ただし、VLAN を共有するには、サービス プロバイダーはレイヤ 2 で、ユーザ（ホスト）間でトラフィックを分離できる必要があります。

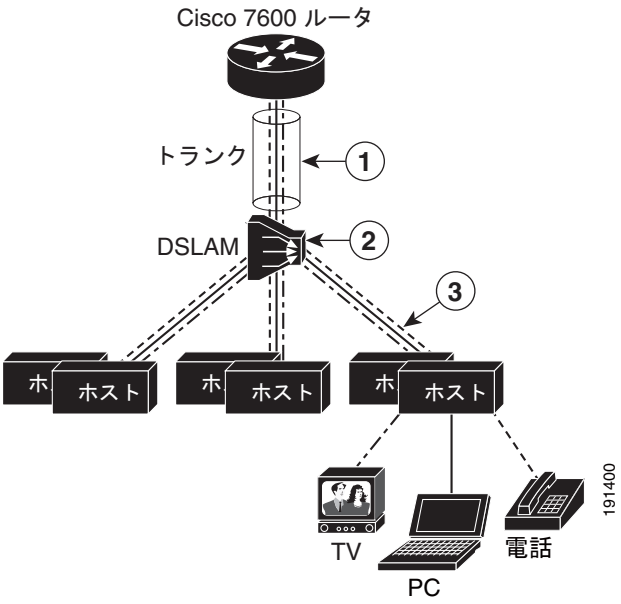
Private Hosts 機能を使用すると、VLAN のホスト（エンド ユーザ）間でのレイヤ 2 の分離を行うことができます。ホストを分離すると、サービス プロバイダーは同じセットのブロードバンド、またはメトロ イーサネット サービスを複数のエンド ユーザに配信する場合、1 セットの VLAN を使用できます。また、その VLAN 内でホスト同士が直接接続することもなくなります。たとえば、VLAN 10 を音声トラフィック、VLAN 20 をビデオ トラフィック、VLAN 30 をデータ トラフィックに使用できます。

Cisco 7600 ルータを DSLAM Gigabit Ethernet（GE; ギガビット イーサネット）集約器として使用する場合、DSLAM は複数の VLAN 向けにデータ伝送可能なトランク ポートを介してルータに接続されます。サービス プロバイダーは、1 つの物理ポートと 1 セットの VLAN を使って、サービスの同じセットを異なるエンド ユーザ（独立ホスト）に配信できます。それぞれの VLAN は個別のサービス（音声、ビデオ、データ）に使用できます。

図 38-1 に、Cisco 7600 ルータから DSLAM に接続している複数のエンド ユーザにトリプルプレイ サービスを配信する例を示します。この図では、次の点に注意してください。

- 単一のトランク リンク（ルータと DSLAM 間）によって、3 つの VLAN すべてのトラフィックが伝送されます。
- 仮想回線によって、DSLAM から個々のエンド ユーザへ VLAN トラフィックが配信されます。

図 38-1　　VC から VLAN へのマッピング



A	トランク リンクによる伝送： • 音声 VLAN × 1 • ビデオ VLAN × 1 • データ VLAN × 1	B	DSLAM により、音声、ビデオ、およびデータ トラフィックは VLAN と VC 間でマッピングされます。
		C	個別の VC により、音声、ビデオ、およびデータ トラフィックは DSLAM と各ホスト間で伝送されます。

トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）

Private Hosts 機能では、PACL を使用して、Private Hosts 用に設定された各ポートを通過できるトラフィックのタイプを制限します。ポートのモード（ポートで Private Hosts をイネーブルにするときに指定）によって、ポートに適用される PACL のタイプが決まります。各タイプの PACL は、それぞれ異なるタイプのトラフィックのトラフィック フローを制限します（たとえば、コンテンツ サーバから独立ホスト、独立ホストからサーバ、独立ホスト間のトラフィックなど）。

次に、Private Hosts 機能で使用されるポート モードについて説明します（図 38-2 を参照）。

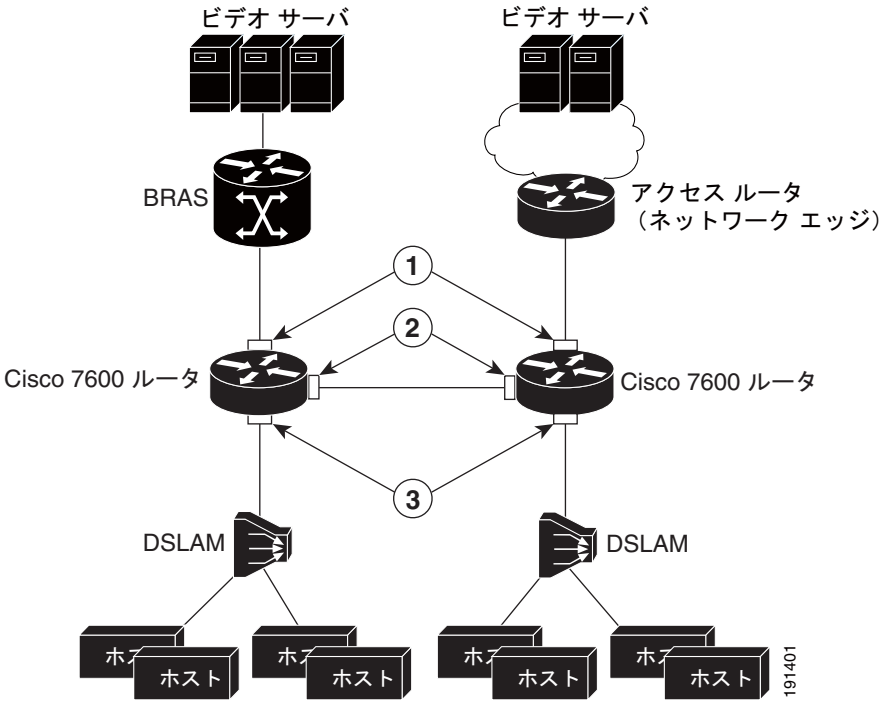
- 独立：エンド ユーザ（独立ホスト）が接続される DSLAM に接続されるポート。この場合ポートにおける VLAN 上のホストは、それぞれが独立している必要があります。このタイプのポートに接続されているホストは、アップストリーム デバイスだけにユニキャスト トラフィックを通過させることができます。
- 無差別：コア ネットワーク側か、Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）デバイス側にあるポート、およびブロードバンド サービスを提供するマルチキャスト サーバ。
- 混合：Cisco 7600 ルータを相互接続するポート。これらのポートは、スパニングツリー プロトコル（STP）トポロジの変更に応じて、独立ポートまたは無差別ポートとして機能します。これらのポートでは、アップストリーム デバイス（BRAS やマルチキャスト サーバなど）へのユニキャスト トラフィックだけが許可されます。

次に、Private Hosts によるトラフィック フローの制限方法の概要を示します。

- サービス プロバイダー ネットワークに入るブロードキャスト トラフィックは、BRAS およびマルチキャスト サーバ（ビデオ サーバなど）にリダイレクトされます。
- アクセス ルータ（相互に接続された Cisco 7600 ルータ）間のすべてのユニキャスト トラフィックは、BRAS およびマルチキャスト サーバへのトラフィックを除き、ブロックされます。
- 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）機能は、DSLAM 側のポート上の不明なユニキャストのブロックに使用されます。

図 38-2 に、Private Hosts 設定で使用されるさまざまなタイプのポート モード（独立、無差別、および混合）を示します。

図 38-2　プライベート ホストのポート タイプ（モード）



A	無差別ポート	BRAS からホストへのすべてのトラフィックを許可します。
B	混合モード ポート	BRAS からのブロードキャスト トラフィックを許可します。 ホストから無差別モード、および混合モードのポートへのブロードキャスト トラフィックをリダイレクト。 BRAS からホストおよびホストから BRAS へのトラフィックを許可します。 ホスト トラフィックへの他すべてのホストを拒否。
C	独立ポート	ホストから BRAS へのユニキャスト トラフィックだけを許可します。ポート間のユニキャスト トラフィックをブロックします。 ホストから BRAS へのすべてのブロードキャスト トラフィックをリダイレクトします。 BRAS からのトラフィックを拒否します（スプーフィングを防止するため）。 マルチキャスト トラフィックを許可（IPv4 および IPv6）。

（注） BRAS という用語は、BRAS、マルチキャスト サーバ（ビデオ サーバなど）、これらのデバイスへのアクセスを提供するコア ネットワーク デバイスなどのアップストリーム デバイスを表します。

ポート ACL

ルータ ポートにレイヤ 2 フォワーディング制約を課すために、Private Hosts ソフトウェアによって複数のタイプのポート ACL（PACL）が作成されます。それぞれのタイプの PACL により、特定のタイプのトラフィック（コンテンツ サーバから独立ホスト、独立ホストからサーバ、独立ホスト間のトラフィックなど）のトラフィック フローが制限されます。

このソフトウェアでは、ブロードバンド サービスを提供するコンテンツ サーバの MAC アドレスと、それらのサービスの提供先となる独立ホストの VLAN ID に基づいて、さまざまなタイプの Private Hosts ポート用の PACL が作成されます。各 Private Hosts ポートが動作するモードを指定すると、ポートのモード（独立、無差別、または混合）に基づいて、ソフトウェアによって適切な PACL がポートに適用されます。

次に、Private Hosts 機能で使用されるさまざまなタイプの PACL の例を示します。

独立ホスト PACL

次に、独立ポートの PACL の例を示します。

```
deny host BRAS_MAC any
permit any host BRAS_MAC
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit any 0100.5E00.0000/0000.007F.FFFF
permit any 3333.0000.0000/000.FFFF.FFFF
deny any any
```

無差別ポート PACL

次に、無差別ポートの PACL の例を示します。

```
permit host BRAS_MAC any
deny any any
```

混合モード ポート PACL

次に、混合モード ポートの PACL の例を示します。

```
permit host BRAS_MAC ffff.ffff.ffff
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit host BRAS_MAC any
permit any host BRAS_MAC
deny any any
```

設定時の注意事項および制限事項

Cisco 7600 ルータで Private Hosts 機能を設定する際は、次の注意事項と制約事項に従ってください。

- ソフトウェアおよびハードウェアの要件
  - Cisco IOS Release 12.2SRB 以降
  - RSP720（PFC3C または PFC3CXL 搭載）、Sup720（PFC3B または PFC3BXL 搭載）、または Sup32
  - スイッチ ポートとして設定可能なファスト イーサネットまたはギガビット イーサネット（GE）インターフェイスを備えたラインカード（SIP-600、ESM-20、67xx LAN カードなど）でのサポート
    （SIP-400 および拡張 FlexWAN では Private Hosts はサポートされないことに注意してください）

- Private Hosts およびプライベート VLAN は、同一ポート（インターフェイス）上には設定できません。両方の機能をルータ上に共存させることはできますが、各機能を異なるポート上に設定する必要があります。
- Private Hosts はエンドツーエンド機能です。DSLAM とアップストリーム デバイス（BRAS やマルチキャスト サーバなど）の間にあるすべてのルータでイネーブルにする必要があります。
- 現在は、信頼できるポートだけを独立ポートとして設定できます。
- スイッチ ポート（802.1q または ISL トランク ポート）として設定されるレイヤ 2 インターフェイスでのサポート。
- ポートチャネル インターフェイス（Etherchannel、FastEtherchannel、および GigabitEtherchannel）でのサポート。Private Hosts 機能はポートチャネル インターフェイスでイネーブルにする必要があります。メンバー ポートでイネーブルにすることはできません。
- LAN ベース機能（DAI や DHCP スヌーピングなど）は Private Hosts のポートで機能的に共存しません。これは、Private Hosts 機能によって MAC ベースのルックアップがスイッチポートで適用されますが、VLAN ベースではないためです。つまり、Private Hosts の vlan-list と、DAI または DHCP スヌーピングの VLAN リストは、相互に排他的でなければならず、Private Hosts のスイッチポートで重複していてはなりません。

次のプロトコル独立型 MAC ACL 制約事項も適用されます。

- プロトコル独立型 MAC ACL フィルタリング用に次のインターフェイス タイプを設定できます。
  - IP アドレスのない VLAN インターフェイス
  - EoMPLS をサポートする物理 LAN ポート
  - EoMPLS をサポートする論理 LAN サブインターフェイス
- プロトコル独立型 MAC ACL フィルタリングでは、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、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に MAC ACL が適用されます。
- プロトコル独立型 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 を適用できません。
- 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。
- 許可された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 PFC3 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 MSFC によってソフトウェアでルーティングされる場合、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。

設定された VLAN のサブセットのみを備えたポートにプライベート ホストを適用する場合は、次の制約事項が適用されます。

表 38-1　PACL シナリオと制約事項

シナリオ	制限事項
Private-Host VLAN-list に関連付けられた Private-Host 対応ポート内の VLAN の場合	• IP トラフィックと非 IP トラフィックは mac-list 内に設定された MAC アドレスに基づく PACL に従うため、IP トラフィックと非 IP トラフィックの両方が許可または拒否されます。 • 12.2(SRD4) 以降は、Private Host VLAN-list に、相互接続（xconnect）が設定された VLAN を 1 つしか関連付けることができません。独立ポートから届いたトラフィックは PACL に従います。VLAN-list 内の別の VLAN に相互接続を設定しようとすると、拒否されます。同様に、相互接続が設定された VLAN がすでに VLAN-list に掲載されている場合は、相互接続が設定された VLAN を Private Host VLAN-list に追加しようとすると、拒否されます。 • 上記ケースでは、PACL によって許可されたトラフィックが相互接続経由でスイッチングされます。
Private-Host VLAN-list に関連付けられていない Private-Host 対応ポート内の VLAN の場合	• すべての非 IP トラフィックが PACL に従います。トラフィックは、Private Host mac-list 内に設定された MAC アドレスに基づいて許可または拒否されます。 • このような VLAN 上での IP トラフィックは PACL に従いません。 • このような VLAN に相互接続が設定されている場合は、IP トラフィックが PACL に従わずに相互接続にスイッチングされます。 • VLAN がレイヤ 3 ルーテッド（SVI）で、IP トラフィックがレイヤ 3 ルーテッドの場合は、ポート上のデフォルト ACL を通してすべてのパケットが拒否されます。ただし、L3 パケットは、CPU（MSFC）に転送され、そこでレート制限されます。 • VLAN が相互接続に関連付けられている場合は、PACL によってトラフィックが許可される場合にのみ、非 IP トラフィックが相互接続上でスイッチングされます。 • VLAN が **mac packet-classify** を使用して設定されている場合は、VLAN 上の IP トラフィックと非 IP トラフィックの両方が PACL に従います。

- 12.2(33) SRD4 以降は、次のプロトコルに依存しない MAC ACL 制約事項も適用されます。
  - Private Host 機能は、Private Host が設定された VLAN 上のすべてのトラフィックが、VLAN を共有する 2 人の加入者間で直接やり取りされないようにします。

- 1 つの VLAN が Private Host および相互接続と連動するようにシステムを設定することができます。
- 1 つの VLAN が相互接続と Private Host 用に設定されている場合は、その VLAN の相互接続が無差別モードになります。ただし、トラフィックがコア側からリレーされる場合は、設定された相互接続に対して ACL を適用することができません。
- MAC ACL 制約事項を適用しても、スケールやパフォーマンスは変化しません。
- Private Host では、VPLS サポートが 1 つの VLAN に限定されます。Private Host VLAN-list に VPLS VLAN（相互接続が設定された VLAN）が掲載されている場合は、別の VPLS VLAN を追加しようとすると、ブロックされます。同様に、VLAN-list 内のいずれかの VLAN に相互接続が設定されている場合は、そのリスト内の別の VLAN に相互接続を設定しようとすると、ブロックされます。

（注）　Release 12.2SRB では、PACL は Private Hosts の一部としてだけサポートされます。独自の PACL は設定できません。代わりに、Private Hosts 設定に基づき、ルータにより PACL が作成されて適用されます。

ACL の注意事項

アクセス コントロール リスト（ACL）には、次の設定時の注意事項および制約事項が適用されます。

- Private Hosts 機能の 12.2 (33) SRD4 リリースでは、プロトコルに依存しない MAC ACL が使用されます。
  Private Hosts 用に設定されたポートに IP ベースの ACL を適用しないでください。適用した場合、Private Hosts 機能は中断されます（ルータが Private Hosts MAC ACL をポートに適用できないため）。
- VLAN ACL（VACL）およびポート ACL は、同じインターフェイスには適用できません。
- Routing ACL（RACL; ルーティング ACL）および PACL は、同じインターフェイスには適用できません。ただし、別々のインターフェイスには適用することができます。

トランク ポート上の VLAN

VLAN には、次の注意事項および制約事項が適用されます。

- Private Hosts 用に設定されたトランク ポートを使用する VLAN で IGMP スヌーピングをイネーブルにすることができます。
- Private Hosts 用に設定されたトランク ポートを使用する VLAN で IP マルチキャストをイネーブルにすることはできません。
- PACL はトランク ポート上で上書きモードで動作するため、VLAN ベースの機能をスイッチポートに適用することはできません。
- マルチキャスト ソースが無差別ポート上に存在している場合、マルチキャスト VLAN レジストレーション（MVR）機能は Private Hosts と共存できます。

他の機能との相互作用

Private Hosts 機能とルータで設定される他の機能との相互作用を次に示します。

- Private Hosts 機能は、MAC 制限、Unicast Flood Protection（UFP）、Unknown Unicast Flood Blocking（UUFB）などのレイヤ 2 ベースのサービスに影響しません。

- Private Hosts 機能は IGMP スヌーピングに影響しません。ただし、IGMP スヌーピングがグローバルにディセーブル化されている場合は、IGMP 制御パケットが ACL チェックの対象になります。IGMP 制御パケットを許可するために、Private Hosts ソフトウェアによって multicast permit ステートメントが独立ホストの PACL に追加されます。この動作は自動的に行われるため、ユーザの操作は必要ありません。
- 独立ポートでポート セキュリティをイネーブルにして、これらのポートにセキュリティを追加できます。
- 無差別ポートまたは混合モード ポートでポート セキュリティ機能をイネーブルにすると、アップストリーム デバイス（BRAS やマルチキャスト サーバなど）のソース ポートでの変更が制限される場合があります。
- アクセス ポート上でイネーブルにした場合は、802.1*x* が Private Hosts の影響を受けません。

スプーフィングからの保護

Private Hosts 機能では、MAC アドレス スプーフィングは防止されますが、カスタマー MAC または IP アドレスは確認されません。MAC アドレス スプーフィングを回避するために、Private Hosts 機能が行う処理は次のとおりです。

- BRAS およびマルチキャスト サーバのスタティック MAC アドレスを使用します。
- レイヤ 2（L2）転送テーブルでのラーニングをディセーブルにします。
- BRAS またはマルチキャスト サーバがソース ポートから別のポートに移動した場合に、ルータ ソフトウェアに通知します。ソフトウェアによって移動が確認され、L2 転送テーブルが更新されます。

マルチキャスト動作

アップストリーム デバイス（BRAS やマルチキャスト サーバなど）からのマルチキャスト トラフィックは常に許可されます。また、Private Hosts PACL はマルチキャスト制御パケット（IGMP クエリーや Join 要求など）には適用されません。この動作により、独立ホストはマルチキャスト グループに参加し、IGMP クエリーに応答し、目的のグループからトラフィックを受信できます。

ホストからのマルチキャスト トラフィックは、Private Hosts PACL によって廃棄されます。ただし、あるホストから発信されたマルチキャスト トラックを別のホストで受信する必要がある場合は、Private Hosts が PACL に *multicast permit* エントリを追加します。

Private Hosts の設定

ここでは、Cisco 7600 シリーズ ルータ上での Private Hosts 機能の設定およびこの機能の設定手順について説明します。

- 「設定の概要」（P.38-10）
- 「詳細設定手順」（P.38-11）
- 「設定例」（P.38-12）

設定の概要

ここでは、Cisco 7600 ルータ上で Private Hosts 機能を設定するために実行する手順の概要について説明します。次のセクションで、詳細な設定手順を説明します。

1. Private Hosts 機能で使用するルータ ポート（インターフェイス）を決定します。この機能は、スイッチポート（802.1q または ISL トランク ポート）またはポートチャネル インターフェイス（Etherchannel、FastEtherchannel、および GigabitEtherchannel）で設定できます。Private Hosts 機能はポートチャネル インターフェイスでイネーブルにする必要があります。メンバー ポートでイネーブルにすることはできません。
2. Private Hosts 以外の通常のサービス用の各ポート（インターフェイス）を設定します。これ以降は、VLAN を設定できることに注意してください。
3. ブロードバンド サービスをエンド ユーザに提供するために使用する VLAN または VLAN セットを決定します。Private Hosts 機能を使用すると、これらの VLAN のホスト間でのレイヤ 2 の分離を行うことができます。
4. エンド ユーザ（独立ホスト）にブロードバンド サービスを提供するために使用されているすべての BRAS とマルチキャスト サーバの MAC アドレスを指定します。

（注）　サーバがルータに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。

5. （任意）異なるタイプのブロードバンド サービスを異なる独立ホストのセットに提供する場合は、複数の MAC リストおよび VLAN リストを作成します。
   - 各 MAC アドレス リストでは、特定のタイプのサービスを提供するサーバまたはサーバ セットを指定します。
   - 各 VLAN リストでは、そのサービスが提供される独立ホストを指定します。
6. 無差別ポートを設定し、特定のサービス タイプ用のサーバと受信ホストを識別する MAC リストと VLAN リストを指定します。

（注）　異なるタイプのサービスを異なるホストのセットに提供できるように、複数の MAC と VLAN の組み合わせを指定できます。たとえば、xxxx.xxxx.xxxx の BRAS を使用して VLAN 20、25、および 30 で基本的なサービス セットを提供し、yyyy.yyyy.yyyy の BRAS を使用して VLAN 5、10、および 15 で高品質のサービス セットを提供できます。

7. Private Hosts をグローバルにイネーブルにします。
8. Private Hosts を個別のポート（インターフェイス）でイネーブルにし、ポートの動作モードを指定します。ポート モードを決定するには、ポートがアップストリーム側（コンテンツ サーバまたはコア ネットワーク方向）か、ダウンストリーム側（DSLAM ホストと独立ホスト方向）か、別の Cisco 7600 ルータに接続されている（通常は、リング トポロジを使用）かを把握する必要があります。「トラフィック フローの制限（Private Hosts ポート モードおよび PACL の使用）」（P.38-3）を参照してください。

個別のポートで Private Hosts 機能をイネーブルにすると、ルータでこの機能を実行する準備が整います。Private Hosts ソフトウェアによって、この設定の独立、無差別、および混合モード PACL を作成するために定義した MAC および VLAN リストが使用されます。次に、ポートのモードに応じて、適切な PACL が各 Private Hosts ポートに適用されます。

詳細設定手順

次の手順を実行して、Private Hosts 機能を設定します。これらの手順は、Private Hosts 用のレイヤ 2 インターフェイスをすでに設定していることを前提としています。次の表内のコマンドについては、「コマンド リファレンス」（P.38-13）を参照してください。

（注） Private Hosts は、スイッチポート（802.1q または ISL トランク ポート）または Etherchannel ポートだけで設定できます。また、DSLAM とアップストリーム デバイスの間にあるすべてのルータで Private Hosts をイネーブルにする必要があります。

	コマンドまたはアクション	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)# private-hosts mac-list` *mac-list-name mac-address* `[remark` *device-name* `|` *comment*`]`
	
	例：
	`Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose`
		ブロードバンド サービスを提供する BRAS およびマルチキャスト サーバを識別する MAC アドレスのリストを作成します。各項目の意味は次のとおりです。
		• *mac-list-name* は、このコンテンツ サーバのリストに割り当てる名前を指定します。
		• *mac-address* は、特定のブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定します。
		• **remark** を使用すると、この MAC リストに割り当てるデバイス名またはコメントをオプションで指定できます。
		サービスを提供するために使用されるすべてのコンテンツ サーバの MAC アドレスを指定します。異なるタイプのサービスを異なるホストのセットに提供する場合は、特定のサービスを提供するサーバまたはサーバ セットごとに別々の MAC リストを作成します。
		（注） サーバがルータに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。

ステップ 3	`Router(config)# private-hosts vlan-list` *vlan-ids* **例：** `Router(config)# private-hosts vlan-list 10,12,15,200-300`	ホストがブロードバンド サービスを受信できるようにホストを分離する必要がある VLAN（*vlan-ids*）のリストを作成します。 特定のサービスを異なるホストのセットに提供する場合は、別々の VLAN リストを作成します。それ以外の場合は、すべてのブロードバンド サービスがすべての独立ホストに提供されます。

	コマンドまたはアクション	目的

ステップ 4	`Router(config)# private-hosts promiscuous mac-list-name [vlan-list vlan-ids]`
	
	例：
	`Router(config)# private-hosts promiscuous BRAS_list vlan-list 1,2,3`
		ブロードバンド サービスのコンテンツ サーバおよびサービスの提供先のエンド ユーザ（独立ホスト）を指定します。各項目の意味は次のとおりです。
		• *mac-list-name* は、特定のタイプのブロードバンド サービスまたはサービス セットを提供する BRAS またはマルチキャスト サーバ（サーバ セット）を指定する MAC アドレス リストの名前を指定します。
		• *vlan-ids* は、ホストが上記のサーバからサービスを受信する VLAN または VLAN セットを指定します。VLAN リストを指定しない場合、ソフトウェアによりグローバル VLAN リスト（ステップ 3 で設定）が使用されます。
		（注） このコマンドを複数回発行して、MAC と VLAN の組み合わせを複数設定できます。それぞれの組み合わせによって、特定のタイプのサービスのサーバおよび受信ホストが定義されます。

ステップ 5	`Router(config)# private-hosts`	Private Hosts をルータでグローバルにイネーブルにします。
ステップ 6	`Router(config)# interface interface`	Private Hosts に対してイネーブルにするスイッチポート（802.1Q または ISL トランク ポート）または Etherchannel ポートを選択します。

ステップ 7	`Router(config-if)# private-hosts mode {promiscuous | isolated | mixed}`
	
	例：
	`Router(config-if)# private-hosts mode isolated`
		Private Hosts をポートでイネーブルにします。次のキーワードのいずれかを使用して、ポートが動作するモードを定義します。
		• **promiscuous**：ブロードバンド サーバ（BRAS、マルチキャスト、またはビデオ）またはこれらのサーバへのアクセスを提供するコア ネットワーク デバイスに接続する、アップストリームに面したポート。
		• **isolated**：DSLAM に接続するポート。
		• **mixed**：他の Cisco 7600 ルータに接続するポート（通常は、リング トポロジを使用）。
		（注） Private Hosts に使用される各ポートで、この手順を実行する必要があります。

ステップ 8	`Router(config-if)# end`	インターフェイスおよびグローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。Private Hosts 設定が完了します。

設定例

次に、Private Hosts 独立ポートのインターフェイス設定例を示します。

```
Router# show run int gi 5/2
Building configuration...

Current configuration : 200 bytes
!
interface GigabitEthernet5/2
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 private-hosts mode isolated
end
```

次に、Private Hosts 無差別ポートのインターフェイス設定例を示します。

```
Router# show run int gi 4/2
Building configuration...

Current configuration : 189 bytes
!
interface GigabitEthernet4/2
 switchport
 switchport access vlan 200
 switchport mode access
 private-hosts mode promiscuous
end

private-hosts
private-hosts vlan-list 200
private-hosts promiscuous bras-list
private-hosts mac-list bras-list 0000.1111.1111 remark BRAS-SERVER
```

コマンド リファレンス

ここでは、リリース 12.2(33) SRD4 で導入された Private Hosts 機能に関連するコマンドについて説明します。

- **private-hosts**
- **private-hosts mac-list**
- **private-hosts mode**
- **private-hosts promiscuous**
- **private-hosts vlan-list**
- **show fm private-hosts**
- **show private-hosts access-lists**
- **show private-hosts configuration**
- **show private-hosts interface configuration**
- **show private-hosts mac-list**
- **debug fm private-hosts**
- **debug private-hosts**

private-hosts

Private Hosts 機能をグローバルに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 **private-hosts** コマンドを使用します。機能をディセーブルにするには、コマンドの **no** 形式を入力します。

private-hosts

no private-hosts

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、ルータ上の Private Hosts をイネーブルにします。次に、**private-hosts mode** コマンドを使用して、個別のインターフェイス（ポート）で Private Hosts をイネーブルにします。

例

次のコマンド例は、Private Hosts 機能をルータでグローバルにイネーブルにします。

```
Router(config)# private-hosts
```

関連コマンド

コマンド	説明
private-hosts mac list	ブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレス リストを作成します。
private-hosts mode	Private Hosts ポートの動作モードを指定します。
private-hosts promiscuous	ブロードバンド サービスのコンテンツ サーバおよび受信ホストを指定します。
private-hosts vlan-list	ホストを分離する必要がある VLAN を指定します。
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show **private-hosts interface configuration**	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts mac-list

独立ホストにブロードバンド サービスを提供し、MAC アドレス リストを作成するコンテンツ サーバを指定して、グローバル コンフィギュレーション モードで **private-hosts mac-list** コマンドを使用します。MAC アドレス リストからアドレスを削除して、そのデバイスを Private Hosts 機能のサービスを提供するコンテンツ サーバのリストから削除するには、コマンドの **no** 形式を入力します。

private-hosts mac-list *mac-list-name mac-address* **[remark** *device-name* **|** *comment***]**

no private-hosts mac-list *mac-list-name mac-address*

構文の説明

mac-list-name	アドレス リストに割り当てる名前（最大 80 文字）。
mac-address	Private Hosts 機能のブロードバンド サービスを提供する Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）、マルチキャスト サーバ、またはビデオ サーバの MAC アドレス。 **（注）** サーバがルータに直接接続されていない場合は、サーバへのアクセスを提供するコア ネットワーク デバイスの MAC アドレスを指定します。
remark *device-name* | *comment*	（任意）この MAC アドレス リストに割り当てるデバイス名またはコメントをオプションで指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Private Hosts 設定でブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレスのリストを作成します。

このコマンドを使用して、Private Hosts 機能のブロードバンド サービスを提供するすべてのコンテンツ サーバの MAC アドレスを指定します。*コンテンツ サーバ*は、ネットワーク内の独立ホストに Broadband Remote Access Server（BRAS; ブロードバンド リモート アクセス サーバ）、マルチキャスト サーバ、またはビデオ サーバです。

すべてのコンテンツ サーバを 1 つの MAC アドレス リストに割り当てることができます。または、複数の MAC アドレス リストを作成して、それぞれで特定のタイプのブロードバンド サービスまたはサービス セットを提供するコンテンツ サーバを指定することもできます。Private Hosts 用の無差別ポートを設定する場合は、ブロードバンド サービスのサーバと受信ホストを指定する MAC アドレス リストおよび VLAN リストを指定します。

（注） MAC アドレス リストの最後のアドレスが削除されると、そのリストが自動的に削除されます。

例

この例では、アップストリーム BRAS の MAC アドレスを指定する BRAS_list という名前の MAC アドレス リストが作成されます。オプションの remark は、BRAS が San Jose にあることを示しています。

```
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_San-Jose
```

関連コマンド

コマンド	説明
show private-hosts mac-list	MAC アドレスのリストを表示します。このアドレスは、Private Hosts に対して定義されたブロードバンドを提供しているコンテンツ サーバを識別します。

private-hosts mode

Private Hosts をインターフェイス（ポート）でイネーブルにし、ポートの動作モードを指定するには、インターフェイス コンフィギュレーション モードで **private-hosts mode** コマンドを使用します。ポートで Private Hosts をディセーブルにするには、コマンドの **no** 形式を入力します。

private-hosts mode {**promiscuous** | **isolated** | **mixed**}

no private-hosts

構文の説明

promiscuous	ポートを無差別モードに設定します。このモードは、アップストリーム側のポートに使用します。これらは、ブロードバンド サービス（BRAS、マルチキャスト、またはビデオ）を提供するサーバ、または、これらのサーバへのアクセスを提供するコア ネットワーク デバイスにルータを接続するポートです。
isolated	ポートを独立モードに設定します。このモードは、独立ホストが接続される DSLAM 側のポートに使用します。
mixed	ポートを混合モードに設定します。このモードは、他の Cisco 7600 ルータに接続するポート（通常は、リング トポロジを使用）に使用します。このポートの動作は、スパニングツリー プロトコル（STP）トポロジに応じて変更されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。
mode のデフォルトは promiscuous です。

コマンド モード

インターフェイス コンフィギュレーション（スイッチポートまたはポートチャネル）

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**private-hosts** コマンドを発行して、ルータ上の Private Hosts 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して、Private Hosts 機能を個別のポートでイネーブルにし、ポートの動作モードを定義します。ポートのモードによって、ポートの通過が許可されるトラフィックのタイプを制限するためにポートに割り当てられる PACL のタイプが決定されます。各タイプの PACL は、それぞれ異なるタイプのトラフィックのトラフィック フローを制限します（たとえば、コンテンツ サーバから独立ホスト、独立ホストからサーバ、独立ホスト間のトラフィックなど）。Private Hosts ポートに割り当てられているモードを表示するには、**show private-hosts interface configuration** コマンドを使用します。

例

次のコマンド例は、Private Hosts 機能をインターフェイス（ポート）でグローバルにイネーブルにし、ポートを独立モードに設定します。

```
Router(config-if)# private-hosts mode isolated
```

関連コマンド

コマンド	説明
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts promiscuous

ブロードバンド サービスを提供するコンテンツ サーバと受信ホストを指定するには、グローバル コンフィギュレーション モードで **private-hosts promiscuous** コマンドを使用します。無差別ポート設定を削除するには、コマンドの **no** 形式を入力します。

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]

no private-hosts promiscuous *mac-list-name*

構文の説明

mac-list-name	Private Hosts のブロードバンド サービスを提供するコンテンツ サーバ（BRAS、マルチキャスト、またはビデオ）を指定する MAC アドレス リストの名前。
vlan *vlan-ids*	（任意）MAC アドレス リストで指定されたコンテンツ サーバからホストがサービスを受信できる VLAN または VLAN セット。個別の VLAN をカンマで区切るか、VLAN の範囲を指定します（1,3,5,20-25 など）。 **（注）** VLAN リストを指定しない場合、グローバル VLAN リストが使用されます。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

MAC アドレス リストと VLAN リストでは、ブロードバンド サービスを提供するコンテンツ サーバと受信ホストが定義されます。VLAN リストを指定しない場合、**private-hosts vlan-list** コマンドで作成されたグローバル VLAN リストが使用されます。

このコマンドを複数回発行して、MAC リストと VLAN リストの組み合わせを複数指定できます。それぞれの組み合わせによって、特定のタイプのサービスのサーバおよび受信ホストが定義されます。たとえば、xxxx.xxxx.xxxx の BRAS を使用して VLAN 20、25、および 30 で基本的なサービス セットを提供し、yyyy.yyyy.yyyy の BRAS を使用して VLAN 5、10、および 15 で高品質のサービス セットを提供できます。

例

次のコマンド例は、BRAS_list アドレス リストで定義されたコンテンツ サーバによって提供されるブロードバンド サービスが、VLAN 10、12、15、および 200 ～ 300 内の独立ホストに配信されるように設定します。

```
Router(config)# private-hosts promiscuous BRAS_list vlan 10,12,15,200-300
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

private-hosts vlan-list

相互にホストを分離する必要のある VLAN を特定して（VLAN を使用してブロードバンド サービスを提供するため）、グローバル コンフィギュレーション モードで **private-hosts vlan-list** コマンドを使用します。ホストの分離が必要な VLAN のリストから VLAN を削除するには、コマンドの **no** 形式を入力します。

private-hosts vlan-list *vlan-ids*

no private-hosts vlan-list *vlan-ids*

構文の説明

vlan-ids	ホストを相互に分離する必要がある VLAN のリスト。個別の VLAN をカンマで区切るか、VLAN の範囲を指定します（1,3,5,20-25 など）。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Private Hosts 機能によってホストを分離する必要がある VLAN のリストを作成します。VLAN リストには、複数のエンド ユーザ（独立ホスト）にブロードバンド サービスを提供するためのすべての VLAN が含まれている必要があります。

異なるタイプのブロードバンド サービスを異なるホストのセットに提供する場合は、複数の VLAN リストと複数の MAC アドレス リストを作成できます。無差別ポートを設定する場合は、MAC リストと VLAN リストのさまざまな組み合わせを指定して、サービスのタイプごとにコンテンツ サーバと受信ホストを指定できます。

無差別ポートを設定するときに VLAN リストを指定しない場合、このコマンドで作成されたグローバル VLAN リストが使用されます。

（注） Private Hosts 機能によって、VLAN リストに含まれているすべての VLAN 内のホストが分離されます。したがって、ブロードバンド サービスを提供するために使用されている VLAN だけを VLAN リストに含める必要があります。

例

このコマンドは、Private Hosts 機能を設定して VLAN 10、12、15、および 200 ～ 300 のホストを分離します。

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。

show fm private-hosts

Private Hosts 機能マネージャに関する情報を表示するには、特権 EXEC モードで **show fm private-hosts** コマンドを実行します。

show fm private-hosts {**all** | **interface** *intf*}

構文の説明

all	Private Hosts 用に設定されているすべてのインターフェイスの機能マネージャ情報を表示します。
interface *intf*	機能マネージャ情報を表示するインターフェイスを指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show fm private-hosts interface GigabitEthernet 1/2
------------------------------------------------------------------------------
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
==============================================================================

---------------------------------------------------------------
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
---------------------------------------------------------------
Indx - VMR index      T     - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo  - Ethernet Code
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

---------------------------------------------------------------
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
---------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.1111.4001 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
```

```
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V ffff.ffff.ffff 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0100.5e00.0000 0000.0000.0000    0 0
      M ffff.ff80.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 3333.0000.0000 0000.0000.0000    0 0
      M ffff.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 3    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

------------------------------------------------------------
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+

 1    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT

 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT


Interfaces using this pvt host feature in ingress dir.:
-----------------------------------------------
  Interfaces (I/E = Ingress/Egress)

Router#
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show **private-hosts interface configuration**	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts access-lists

Private Hosts 設定に関するアクセス リストを表示するには、特権 EXEC モードで **show private-hosts access-lists** コマンドを実行します。

show private-hosts access-lists

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、カスタマイズされた設定に関する Private Hosts アクセス リストを表示する例を示します。

```
Router# show private-hosts access-lists

Promiscuous ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny     Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Isolated ACLs
Action Deny     Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Mixed ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Router#
```

関連コマンド

コマンド	説明
show fm private-hosts	Private Hosts 機能マネージャに関する情報を表示します。
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts configuration

ルータの Private Hosts 設定に関する情報を表示するには、特権 EXEC モードで **show private-hosts configuration** コマンドを実行します。

show private-hosts configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show private-hosts configuration

    Private hosts enabled. BR INDEX 6 State 0000000F
    Privated hosts vlans lists:
    200
    Privated promiscuous MAC configuration:
    A '*' mark behind the mac list indicates non-existant mac-list
    -------------------------------------------------------------------------------
    MAC-list                       VLAN list
    -------------------------------------------------------------------------------
    bras-list                     *** Uses the isolated vlans (if any) ***
```

関連コマンド

コマンド	説明
show private-hosts interface configuration	個別のインターフェイスの Private Hosts 設定情報を表示します。

show private-hosts interface configuration

個別のインターフェイス（ポート）の Private Hosts 設定に関する情報を表示するには、特権 EXEC モードで **show private-hosts interface configuration** コマンドを実行します。

show private-hosts interface configuration

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルト設定がありません。

コマンド モード　特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例　次に、コマンドの出力例を示します。

```
Router# show private-hosts interface configuration

    Private hosts enabled
    Debug Events: 0 Acl: 0 API: 0
    Promiscuous interface list
    --------------------------
    GigabitEthernet4/2
    Isolated interface list
    -------------------------
    GigabitEthernet5/2
    Mixed mode interface list
    -------------------------
```

関連コマンド

コマンド	説明
show private-hosts configuration	ルータの Private Hosts 設定情報を表示します。

show private-hosts mac-list

Private Hosts に対して定義された MAC アドレス リストの内容を表示するには、特権 EXEC モードで **show private-hosts mac-list** コマンドを実行します。

show private-hosts mac-list [*list-name*]

構文の説明

list-name	（任意）内容を表示する MAC アドレス リストの名前。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# show private-hosts mac-list

    MAC-List: bras-list
    ----------------------------------------------------------------------
    MAC address    Description
    ----------------------------------------------------------------------
    0000.1111.1111 BRAS-SERVER
```

関連コマンド

コマンド	説明
private-hosts mac-list	ブロードバンド サービスを独立ホストに提供するために使用されているコンテンツ サーバを指定する MAC アドレス リストを作成します。

debug fm private-hosts

Private Hosts 機能マネージャに関するデバッグ メッセージをイネーブルにするには、特権 EXEC モードで **debug fm private-hosts** コマンドを実行します。

debug fm private-hosts {**all** | **vmr** | **unusual** | **events**}

構文の説明

all	すべての Private Hosts エラーおよびイベントに関するデバッグ メッセージをイネーブルにします。
vmr	マルチキャスト VLAN レジストレーション（MVR）機能に関するデバッグ メッセージをイネーブルにします。
unusual	予期せぬ Private Hosts 動作に関するデバッグ メッセージをイネーブルにします。
events	Private Hosts イベントに関するデバッグ メッセージをイネーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# debug fm private-hosts all
fm private-hosts vmr debugging is on
fm private-hosts unusual debugging is on
fm private-hosts events debugging is on
Router#
```

関連コマンド

コマンド	説明
debug private-hosts	Private Hosts に関するデバッグ メッセージをイネーブルにします。

debug private-hosts

Private Hosts 機能に関するデバッグ メッセージをイネーブルにするには、特権 EXEC モードで **debug private-hosts** コマンドを実行します。

debug private-hosts {**all** | **events** | **acl** | **api**}

構文の説明

all	すべての Private Hosts エラーおよびイベントに関するデバッグ メッセージをイネーブルにします。
events	Private Hosts イベントに伴う問題に関するデバッグ メッセージをイネーブルにします。
acl	ACL に伴う問題およびイベントに関するデバッグ メッセージをイネーブルにします。
api	アプリケーション プログラミング インターフェイスに伴う問題に関するデバッグ メッセージをイネーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(33)SRB	このコマンドが追加されました。

例

次に、コマンドの出力例を示します。

```
Router# debug private-hosts all
private-hosts events debugging is on
private-hosts api debugging is on
private-hosts acl debugging is on
Router#
```

関連コマンド

コマンド	説明
debug fm private-hosts	Private Hosts 機能マネージャに関するデバッグ メッセージをイネーブルにします。

CHAPTER 39

オンライン診断の設定

この章では、Cisco 7600 シリーズ ルータにオンライン診断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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.39-1）
- 「オンライン診断の設定」（P.39-2）
- 「オンライン診断テストの実行」（P.39-6）
- 「メモリ テストの実行」（P.39-10）

オンライン診断テストの詳細については、付録 A「オンライン診断テスト」を参照してください。

オンライン診断の機能概要

オンライン診断では、ルータがアクティブなネットワークに接続されている間、スーパーバイザ エンジン、モジュール、ルータのハードウェア機能をテストおよび確認できます。

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。Built-In Self-Test（BIST）や中断ループバック テストなどの中断オンライン診断テスト、およびパケット スイッチングなどの非中断オンライン診断テストは、起動時、ラインカードの Online Insertion and Removal（OIR; ホットスワップ）時、およびシステム リセット時に動作します。非中断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、またはこのテストをユーザが要求した場合（オンデマンド）に実行されます。

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（GBIC、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、ハイ アベイラビリティ機能の要件の 1 つです。ハイ アベイラビリティは、装置の故障によるネットワークへの影響を制限しようとする、一連の品質規格です。ハイ アベイラビリティの重要な機能は、アクティブなネットワークでルータが稼働している状態のままハードウェア障害を検出して、対処することです。ハイ アベイラビリティ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ハイ アベイラビリティ ソフトウェアにフィードバックします。

オンライン診断は起動診断、オンデマンド診断、スケジュール診断、またはヘルス モニタリング診断に分類されます。起動診断は起動時、モジュールの OIR 時、またはバックアップ スーパーバイザ エンジンへのスイッチング時に動作します。オンデマンド診断は、CLI から実行します。スケジュール診断は、ルータがアクティブなネットワークに接続されている場合に、ユーザが指定したインターバルまたは指定時刻に動作します。ヘルスモニタリング診断はバックグラウンドで動作します。

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」（P.39-2）
- 「オンデマンド オンライン診断の設定」（P.39-3）
- 「オンライン診断のスケジューリング」（P.39-5）

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 オンライン診断をまったく実行しないこともできます。すべての診断テストを実行するには、**complete** キーワードを入力します。スーパーバイザ エンジンに EARL テストだけを実行し、ルータのすべてのポートにループバック テストを実行するには、**minimal** キーワードを入力します。すべての診断テストを省略するには、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。

（注） 診断レベルはルータ全体に適用されます。モジュール単位での設定はできません。

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。障害が検出された場合にテストを停止または継続するように、あるいは障害カウントを使用して特定の障害数に達した場合にテストを停止するように、実行アクションを設定できます。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。メモリ テストは、スーパーバイザ エンジンで実行する前に、他のモジュール上で実行してください。

（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. ノンディスラプティブ 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　ノンディスラプティブ 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、ノンディスラプティブ カテゴリに属するコマンドを判別するには、**show diagnostic content** コマンドを入力します。

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。個々のモジュールに、すべての機能分野が存在するわけではありません。テストに必要な機能エリア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** キーワードを入力します。

ステップ 3　TestTrafficStress テストを実行します。

これは、スーパーバイザ エンジンだけで使用可能なディスラプティブ 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。テストが完了するまで、リンク フラップは回復しません。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** *module* **test all** コマンドを使用して、テスト対象のモジュールに対するすべてのヘルス モニタリング テストをディセーブルにしてください。

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** *module* **test all** コマンドを使用して、テスト対象のモジュールに対するすべてのヘルス モニタリング テストをディセーブルにしてください。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。

すべてのモジュールでは、完全メモリ テストを使用できます。完全メモリ テストの実行後は、スーパーバイザ エンジンは使用不可状態となり、再起動が必要になるため、最初に他のすべてのモジュールでこのテストを実行するようにしてください。モジュールに大容量メモリが搭載されている場合は、完全メモリ テストが完了するまでに数時間かかることもあります。

完全メモリ テストを実行する前に、このテストを実行するモジュール上ですべてのヘルス モニタリング テストをディセーブルにしてください。ヘルス モニタリングがイネーブルにされていると、テストが失敗し、スイッチは回復アクションを実行するためです。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** *module* **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（特定のモジュールで使用できないテストはすべて省略できます）。

1. TestFibTcamSSRAM
2. TestAclQosTcam
3. TestNetFlowTcam
4. TestAsicMemory
5. TestAsicMemory

完全メモリ テストの実行後は、スーパーバイザ エンジンを再起動して、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、スーパーバイザ エンジンまたは他のモジュール上でその他のテストを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。モジュールを動作可能な状態に戻すには、電源をオフ / オンする必要があります。モジュールがオンライン状態に戻ったあとで、**diagnostic monitor module** *module* **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

特定のモジュールについて特定日の指定時間、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 回だけ、または繰り返しテストを実行するようスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

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** *num*} **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、特定のモジュールおよびポートについて、特定の日時にオンデマンド診断テストを実行するよう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、特定のモジュールおよびポートについて、毎日一定の時間にオンデマンド診断テストを実行するよう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、特定のモジュールおよびポートについて、毎週一定の曜日にオンデマンド診断テストを実行するよう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

ルータがアクティブなネットワークに接続されている状態で、特定のモジュールにヘルス モニタリング診断テストを実行するように設定できます。各ヘルス モニタリング テストの実行インターバル、テストに失敗した場合のシステム メッセージ生成の有無、テストの個別のイネーブル化またはディセーブル化を設定します。テストをディセーブルにするには、コマンドの **no** 形式を入力します。

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** *num*} **test** {*test_id* | *test_id_range* | **all**} [**hour** *hh*] [**min** *mm*] [**second** *ss*] [**millisec** *ms*] [**day** *day*]	指定されたモジュール用に指定されたテストのヘルス モニタリング間隔を設定します。インターバルをデフォルトのインターバル、またはゼロにするには、コマンドの **no** 形式を入力します。
ステップ 2	Router(config)#[**no**] **diagnostic monitor** {**module** *num*} **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、指定されたモジュールで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 テストに失敗した場合に、Syslog メッセージの生成をイネーブルにする例を示します。

```
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停止したり、テスト結果を表示したりできます。モジュールごとに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または停止」（P.39-6）
- 「オンライン診断テストおよびテスト結果の表示」（P.39-7）

オンライン診断テストの開始または停止

ルータまたは各モジュールで実行する診断テストを設定したあとに、診断テストを開始または終了するには、**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** *num*} **test** {*test_id* | *test_id_range* | **minimal** | **complete** | **basic** | **per-port** | **non-disruptive** | **all**} [**port** {*num* | *port#_range* | **all**}]	特定のモジュール、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** *num*}	特定のモジュール上の診断テストを停止します。

次に、特定のモジュールで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、特定のモジュールの診断テストを停止する例を示します。

```
Router# diagnostic stop module 3
Router#
```

オンライン診断テストおよびテスト結果の表示

特定のモジュールに設定されたオンライン診断テストを表示して、テスト結果を確認するには、**show** コマンドを使用します。

モジュールに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** *num*]	モジュールに設定されたオンライン診断を表示します。

次に、モジュール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 7

Module 7:

  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、モジュールの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 5
Current bootup diagnostic level:minimal

Module 5:

  Overall Diagnostic Result for Module 5 :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、モジュールの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 5 detail
Current bootup diagnostic level:minimal

Module 5:

  Overall Diagnostic Result for Module 5 :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#
```

スケジュール スイッチオーバー

スケジュール スイッチオーバーを使用すると、アクティブ スーパーバイザ エンジンに障害が発生するか、または処理が中断した場合に、処理を引き継ぐスタンバイ スーパーバイザ エンジンの準備状態を確認できます。このテストは 1 回実行することも、定期的（毎日、毎週、毎月）に実行されるようにすることもできます。

（注） 両方のスーパーバイザ エンジンにスケジュール スイッチオーバーの時間を設定する場合は、スイッチオーバーに失敗した場合のシステム ダウンタイムを短縮するために、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 エンジンのスイッチオーバー間隔が 10 分以上となるようにスケジューリングする必要があります。

スケジュール スイッチオーバーを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	**show diagnostic content** [**module** *num*]	モジュールに設定されたオンライン診断を表示します。このコマンドは、スケジュール スイッチオーバーのテスト ID を取得する場合に使用します。
ステップ 2	Router(config)# **diagnostic schedule module** {*num* | *active-sup-slot*} **test** {*test-id*} {**on** *mm dd yyyy hh:mm*} | {**daily** *hh:mm* } | {**weekly** *day-of-week hh:mm*}	特定の日時にスーパーバイザエンジンにスケジュール スイッチオーバー テストを設定します。

次に、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を毎週金曜日の午後 10:00 にスケジューリングし、アクティブ スーパーバイザ エンジンからのスケジュール済みスイッチオーバーが発生してから 10 分後に、スタンバイ スーパーバイザ エンジンをアクティブ スーパーバイザ エンジンに切り替える例を示します。

```
Router(config)# diagnostic schedule module 5 test 32 weekly Friday 22:00
Router(config)# diagnostic schedule module 6 test 32 weekly Friday 22:10
Router(config)#
```

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る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。
  - スーパーバイザ エンジンの Policy Feature Card（PFC; ポリシー フィーチャ カード）において FIB TCAM および SSRAM のテスト対象のすべてのスイッチング モジュールを取り外します。

  - システムを通常の動作モードに戻す前に、テストしているシステムまたはモジュールをリセットします。
- 推奨される作業
  - Distributed Forwarding Card（DFC）が搭載されている場合、スーパーバイザ エンジンまたはルート スイッチ プロセッサの中心の PFC にメモリ テストを実行する前に、すべてのスイッチング モジュールを取り外し、システムを再起動します。
  - **no diagnostic monitor module** *num* **test all** コマンドを使用して、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 テストをオフにします。

診断の健全性チェック

ネットワーク内の潜在的な問題領域を検出するため、診断の健全性チェックを実行できます。健全性チェックでは、想定される特定のシステム状態の組み合わせを使用した設定に対し、既定の一連のチェックを実行して、警告状況の一覧をコンパイルします。このチェックの目的は、不適切な状態の要素がないかどうかを調べ、システムの健全性を維持するための支援を行うことです。

診断の健全性チェックを実行するには、次の作業を行います。

コマンド	目的
show diagnostic sanity	Cisco 7600 シリーズ ルータのすべてのギガビット イーサネット WAN インターフェイスで、一連のテストを実行します。

次に、**show diagnostic sanity** コマンドの結果として表示される可能性があるメッセージの例を示します。

```
Router# show diagnostic sanity
Pinging default gateway 10.6.141.1 ....
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.141.1, timeout is 2 seconds:
..!!.
Success rate is 0 percent (0/5)

IGMP snooping disabled please enable it for optimum config.

IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan1, Vlan2, GigabitEthernet1/1

Multicast routing is enabled globally but not enabled on the following
interfaces:
GigabitEthernet1/1, GigabitEthernet1/2

A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended.

The bootflash: does not have enough free space to accomodate the crashinfo file.

Please check your confreg value : 0x0.

Please check your confreg value on standby: 0x0.

The boot string is empty. Please enter a valid boot string .
```

```
Could not verify boot image "disk0:" specified in the boot string on the
slave.

Invalid boot image "bootflash:asdasd" specified in the boot string on the
slave.

Please check your boot string on the slave.

UDLD has been disabled globally - port-level UDLD sanity checks are
being bypassed.
OR
[
The following ports have UDLD disabled. Please enable UDLD for optimum
config:
Fa9/45

The following ports have an unknown UDLD link state. Please enable UDLD
on both sides of the link:
Fa9/45
]

The following ports have portfast enabled:
Fa9/35, Fa9/45

The following ports have trunk mode set to on:
Fa4/1, Fa4/13

The following trunks have mode set to auto:
Fa4/2, Fa4/3

The following ports with mode set to desirable are not trunking:
Fa4/3, Fa4/4

The following trunk ports have negotiated to half-duplex:
Fa4/3, Fa4/4

The following ports are configured for channel mode on:
Fa4/1, Fa4/2, Fa4/3, Fa4/4

The following ports, not channeling are configured for channel mode
desirable:
Fa4/14

The following vlan(s) have a spanning tree root of 32768:
1

The following vlan(s) have max age on the spanning tree root different from
the default:
1-2

The following vlan(s) have forward delay on the spanning tree root different
from the default:
1-2

The following vlan(s) have hello time on the spanning tree root different
from the default:
1-2

The following vlan(s) have max age on the bridge different from the
default:
1-2

The following vlan(s) have fwd delay on the bridge different from the
default:
```

```
1-2

The following vlan(s) have hello time on the bridge different from the
default:
1-2

The following vlan(s) have a different port priority than the default
on the port FastEthernet4/1
1-2

The following ports have recieve flow control disabled:
Fa9/35, Fa9/45

The following inline power ports have power-deny/faulty status:
Gi7/1, Gi7/2

The following ports have negotiated to half-duplex:
Fa9/45

The following vlans have a duplex mismatch:
Fas 9/45

The following interafaces have a native vlan mismatch:
interface (native vlan - neighbor vlan)
 Fas 9/45 (1 - 64)

The value for Community-Access on read-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.

The value for Community-Access on write-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.

The value for Community-Access on read-write operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.

Please check the status of the following modules:
8,9

Module 2 had a MINOR_ERROR.

The Module 2 failed the following tests:
TestIngressSpan

The following ports from Module2 failed test1:
1,2,4,48
```

CHAPTER 40

サービス拒絶保護の設定

この章では、サービス拒否（DoS）攻撃から Cisco 7600 シリーズ ルータを保護する方法について説明します。この章の情報は Cisco 7600 シリーズ ルータに固有であり、この資料の「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手順、および次のマニュアルのネットワーク セキュリティ情報と手順を補います。

- 次の URL にある『*Cisco IOS Security Configuration Guide*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html
- 次の URL の『*Cisco 7600 Series Routers Command References*』
  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章で説明する内容は、次のとおりです。

- 「コントロール プレーン保護の概要」（P.40-1）
- 「DoS 保護の機能概要」（P.40-11）
- 「MLS レート リミッタのデフォルト設定」（P.40-24）
- 「DoS 保護の設定時の注意事項および制約事項」（P.40-24）
- 「制御プレーン ポリシングの機能概要」（P.40-31）
- 「CoPP のデフォルト設定」（P.40-31）
- 「CoPP の設定時の注意事項および制約事項」（P.40-31）
- 「CoPP の設定」（P.40-33）
- 「CoPP のモニタ」（P.40-35）
- 「CoPP ポリシーのカスタマイズ」（P.40-36）
- 「CoPP ポリシーの作成」（P.40-36）
- 「トラフィック分類の定義」（P.40-40）
- 「スティッキ ARP の設定」（P.40-43）

コントロール プレーン保護の概要

ルーティングの安定性を確保するには、重要なコントロール プレーンおよび管理トラフィックが確実に Cisco 7600 ルータのルート プロセッサ（RP）またはスイッチ プロセッサ（SP）CPU に到達することが不可欠です。また、IP オプション、Time to Live（TTL）パケット、エラーのあるパケット、レイヤ 2 ブロードキャストおよびマルチキャスト パケットなどのトラフィックも RP に転送され、輻輳を引

き起こすので、そのようなトラフィックは制御する必要があります。コントロール プレーンの保護には、不要なトラフィックから RP や SP を保護し、さらに、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 RP または SP に確実に配信することが必要です。

7600 で DOS からの保護を行うには、次のコントロールプレーン保護メカニズムをイネーブルにします。

- Modular QoS Command Line（MQC; モジュラ QoS コマンド ライン）を使用する Control Plane Policing（CoPP; コントロール プレーン ポリシング）
- Multi Layer Switching（MLS; マルチ レイヤ スイッチング）レート リミッタ
- MLS プロトコル ポリシング
- ブロードキャストおよびマルチキャスト ストーム制御
- Selective Packet Discard（SPD; 選択的パケット廃棄）

デフォルトでは、コントロール プレーン保護メカニズムの基本セットだけがイネーブルになります。コントロール プレーン メカニズムは、必要に応じてカスタマイズする必要があります。

Cisco 7600 におけるコントロール プレーン保護の実装

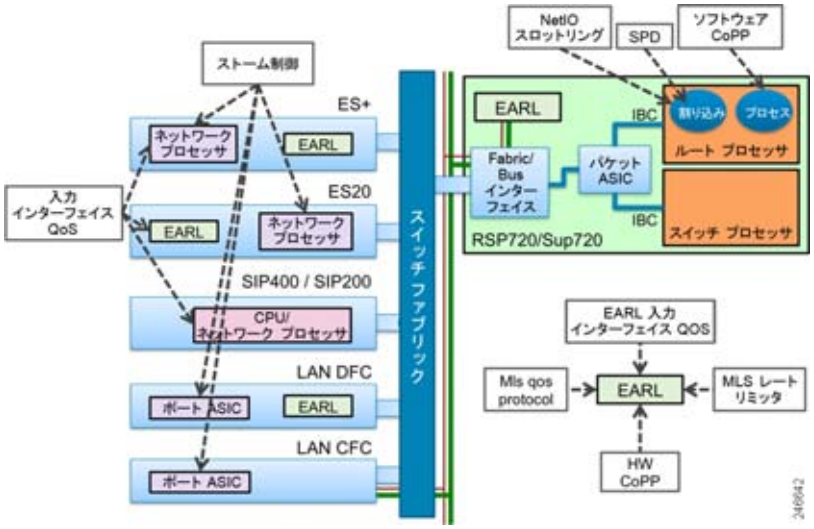
ここでは、コントロール プレーン保護を実装するために Cisco 7600 ルータで使用できるメカニズムについて、また、c7600 ルータ内のパケット フローについて説明します。コントロール プレーン保護はさまざまなステージで実装でき、通常は、パケットを分析して、ルート プロセッサに転送（パケットをパント）するときに適用されます。パケットをパントする決定は、Policy Feature Card（PFC; ポリシー フィーチャ カード）または DFC レベル、あるいは RP または SP の IOS プロセス レベルで行われます。パケットのパントが決定されたら、ポリシングとレート制限を使用してコントロール プレーン保護を実装できます。インターフェイスにトラフィック ストーム制御、アクセス コントロール リスト（ACL）、または入力 Quality of Service（QoS）を設定し、不要なデータ パケットをドロップすることによって、パントが決定される前にコントロール プレーン保護を適用することもできます。

次の項では、Cisco 7600 ルータにおける SP または RP の IOS プロセス レベルへのパケットのパスについて説明します。データ パケットのパスを理解しておくと、コントロール プレーン保護をより適切に設定できます。

制御パケットのパス

図 40-1 に、c7600 ルータの基本的なアーキテクチャと、パケットのパント パスにおけるアクションを示します。

図 40-1　パントされたパケットのパス



PFC または DFC での転送決定に至る、パントされたパケットのパスは、送信パケットのパスと似ています。パケットが RP または SP CPU にパントされる必要があると PFC または DFC で判断された場合、入力ラインカードはスイッチ ファブリック経由でアクティブ スーパーバイザのファブリック インターフェイスまたはバス インターフェイスにパケットを転送します。その後、パケットはパケット ASIC を通過して RP または SP CPU に到達します。

ラインカードによるコントロール パネル保護のサポート

ここでは、コントロール プレーン保護に影響する、C7600 にサポートされているラインカード上の QoS 機能およびその他の機能について説明します。

LAN カード

ユニキャスト、ブロードキャスト、またはマルチキャスト ストーム制御は、LAN カードのポートの特定用途向け集積回路（ASIC）に実装されます。ストーム制御の結果としてドロップされたパケットは、DFC または PFC の EARL に到達しません。パケットはまず、ポート ASIC を通過し、次に LAN カードの Encoded Address Recognition Logic（EARL）を通過します。EARL は、MAC アドレスに基づいたパケットの学習と転送を行うための、c7600 スーパーバイザ エンジン内の中央集中処理エンジンです。

DSCP 状態のポートでキューイングを実行できる WS-X6708 ラインカードを除き、入力キューイングは信頼できるサービス クラス（CoS）状態のポートと、有効な CoS タグを伝送するフレームに対してのみ実行されます。グローバル マッピングを変更することで、この設定を変更できます。変更しない場合、内部データバス ヘッダーの DSCP はゼロに設定されます。重要なパケットが、インターフェイスから SP または RP CPU へのパス全体において高いプライオリティで処理されるようにするには、それらのパケットの元の dot1q CoS、IP COS または DSCP フィールド値を維持することが重要です。ポートの信頼状態を確認するには、**show queueing interface** コマンドを使用します。

パケットに対するそれ以上のアクションは、ラインカードに DFC が存在する場合は DFC で、または PFC で実行されます。SUP 720 または RSP720 上のポートは、LAN カード上のポートと見なすことができます。

次に、**show queueing interface** コマンドを使用してポートの信頼状態を確認する例を示します。

```
Router# show queueing int Gig5/1 | inc Port
  Port QoS is enabled
  Port is untrusted
```

入力 CoS とキューのデフォルト マッピング、および WS-X6708 モジュールに対する入力 DSCP キューイングの詳細については、第 45 章「PFC QoS の設定」を参照してください。

7600-SIP-200 カード

ユニキャスト、ブロードキャスト、またはマルチキャスト ストーム制御は、SIP-200 ラインカードでは実装されません。

SIP-200 の QoS は、MQC を使用して設定されます。分類、マーキング、ポリシング、WRED、CBWFQ、シャーピング、プライオリティ キューイング、および LLQ などの QoS 機能は、7600-SIP-200 の RX（受信）CPU で実行されます。RX CPU では、非 IP パケットに対して QoS は適用されません。

内部データ バス ヘッダー内の CoS は、IP precedence から作成されます。非 IP トラフィックの場合、コントロール プレーン トラフィックに対する CoS は 6 に設定されます。制御トラフィック以外の非 IP パケットの場合、内部 CoS は 0 に設定されます。7600-SIP-200 カードでは、ポートの信頼の概念は使用されません。

7600-SIP-400 カード

ユニキャスト、ブロードキャスト、またはマルチキャスト ストーム制御は、SIP-400 ラインカードでは実装されません。

SPA からパケットを受信すると、Ingress Network Processor（INP; 入力ネットワーク プロセッサ）はまず、パケットを分類します。内部の **pak_priority** フラグが、IP ルーティング プロトコル パケットと非 IP コントロール プレーン トラフィック（ARP を含む）に設定されます。SIP-400 の **pak_priority** フラグは、ローカルな意味しか持ちません。このフラグはデータ バス ヘッダーが作成されるときに考慮されますが、SP または RP CPU の IOS に **pak_priority** フラグを伝送するためのプロビジョニングはありません。**pak_priority** が設定され、パケットが非 IP である場合、内部データバス ヘッダーにインデックス誘導型ビットが設定されます。

内部データバス ヘッダーの CoS フィールドは、dot1q タグからコピーされます。パケットが非 IP であり、**pak_priority** が設定されている場合、データバスの CoS 値は 6 に設定されます。Ingress Network Processor（INP; 入力ネットワーク プロセッサ）は、入力 QoS が入力インターフェイスに設定されている場合、これを適用します。内部データ バス CoS 値が 6 に設定されたパケットは、別個のチャネルのファブリックに送信されます。パケットはその後、ファブリック インターフェイスを介して PFC に送信されます。

7600-SIP-400 カードでは、ポートの信頼の概念は使用されません。

7600-ES20 および 7600-SIP-600 カード

ユニキャスト、ブロードキャスト、またはマルチキャスト ストーム制御は、SIP-600 および ES20 ラインカード上の Network Processor（NP; ネットワーク プロセッサ）に実装されます。パケットは、SIP-600 または ES20 ラインカード上の EARL を通過してから、NP を通過します。SIP-600 では、ストーム制御はギガビット インターフェイスおよび 10 ギガビット インターフェイスでのみサポートされます。ES20 および SIP-600 カードには DFC が搭載されています。パケットが EARL に送信される前に、Cisco Discovery Protocol（CDP）、スパニングツリー プロトコル（STP）、ダイナミック トランキング プロトコル（DTP）、VLAN トランキング プロトコル（VTP）、単方向リンク検出（UDLD）、ポート集約プロトコル（PAgP）、リンク集約制御プロトコル（LACP）または IEEE フロー制御パケットに対してデータバス BPDU が設定されます。IP パケットについては、ポートの信頼状態によって IP

precedence からデータバス CoS フィールドがコピーされる場合があります。ES20 および SIP-600 には DFC への 2 つのキューがあり、CoS 値 0 ～ 5 のパケットは低プライオリティ キューに移動し、CoS 値 6 および 7 のパケットは高プライオリティ キューに移動します。

7600-SIP-600 カードと 7600-ES20 カードでは、ポートの信頼の概念が使用されます。意味するところは、LAN カードの場合と同じです。

ES+ ラインカード

ユニキャスト、ブロードキャスト、またはマルチキャスト ストーム制御は、ES+ ラインカード上の Network Processor（NP; ネットワーク プロセッサ）に実装されます。パケットは NP を通過してから、ES+ ラインカード上の EARL を通過します。ストーム制御によってドロップされたパケットは、ES+ ラインカード上の EARL に到達しません。

ES+ カード上の Network Processor Unit（NPU）の入力パケットメモリには、ポートごとに 2 つの RX キュー（高プライオリティ キューと低プライオリティ キュー）が存在します。また、Intermediate System-to-Intermediate System（IS-IS）には、独自の特別なキューがあります。高プライオリティの制御パケットは、高プライオリティ キューに配置されます。

NP で入力 QoS が適用されます。その後、パケットは EARL に渡されます。7600-ES+ カードでは、ポートは常に信頼されます。

共有ポート アダプタ（SPA）

Shared Port Adapter（SPA; 共有ポート アダプタ）は、7600-SIP-200 カード、7600-SIP-400 カード、および 7600-SIP-600 カードで使用されます。

一部の SPA には、制限付きの QoS 機能が備わっています。各 SPA の QoS 機能の詳細については、次の URL にある『Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw.html

PFC または DFC 上の EARL 経由でパントされるパケットのパス

ここでは、パントを招くチェックやアクションのみに焦点を当てながら、PFC または DFC 経由でパントされるパケットのパスについて説明します。

PFC または DFC でパケットを受信すると、まず、宛先 MAC のルックアップが行われ、次のようにパケットのタイプに応じて適切なアクションが実行されます。

- ブロードキャスト フレーム：パケットが受信された VLAN にレイヤ 3 インターフェイスが存在する場合、ブロードキャスト フレームは RP CPU にパントされます。ブロードキャスト パケットは、MLS レート制限の影響を受けません。
- マルチキャスト フレーム：パケットを受信した VLAN にレイヤ 3 インターフェイスが存在し、さらに宛先 MAC アドレスが IPv4 ローカル ネットワーク制御ブロック マルチキャストまたは IPv4 インターネットワーク制御ブロック マルチキャストに対応する場合（0100.5e00.0000 ～ 0100.5e00.01ff）、フレームは RP CPU にパントされます。その他のマルチキャスト フレームは、さまざまな理由で RP または SP CPU にパントされる可能性があります。すべてのパケットは MLS QoS プロトコル ポリサーに照らして評価され、ポリサーは MLS QoS プロトコル ポリサーの設定に応じて適用されます。RP または SP CPU にパントされたマルチキャスト パケットは、MLS レート リミッタに従います。

- ユニキャスト フレーム：同じルータの宛先 MAC アドレスを持つフレームは、レイヤ 3 のルックアップ用に転送される場合があります。レイヤ 3 のルックアップでは、レイヤ 3 アドレスが、PFC または DFC でサポートされていないルータまたは機能に対してローカルであるなど、さまざまな理由からパントを招く可能性があります。RP または SP CPU にパントされたユニキャスト パケットも、MLS レート制限の影響を受けます。また、ユニキャスト パケットにはコントロール プレーン ポリシングも適用されます。コントロール プレーン ポリシングは設定する必要があり、デフォルトではアクティブになりません。

PFC または DFC におけるコントロール プレーン トラフィックのポリシング

PFC または DFC には、コントロール プレーン トラフィックをポリシングするための 3 つのメカニズムがあります。

- MLS プロトコル ポリサー：MLS プロトコル ポリサーは、RP または SP CPU にパントされるトラフィックだけでなく、指定のプロトコルのすべてのトラフィックをポリシングします。このポリサーを使用して、これらのパケットの IP precedence を変更することもできます。このポリサーの設定には、**mls qos protocol police** コマンドを使用します。MLS プロトコル ポリシングの詳細については、「MLS プロトコル ポリシング」（P.40-15）を参照してください。
- MLS レート リミッタ：MLS レート リミッタは、RP または SP CPU にパントされるトラフィックにのみ適用されます。
  PFC3 または DFC3 上の EARL には 10 個のレート リミッタ レジスタが搭載されており、グローバル コンフィギュレーション モードで設定されます。これらのレート リミッタ レジスタには、特定のレート リミッタに一致する結果パケットのレート制限情報が含まれます。10 個のレート リミッタ レジスタのうち、2 つのレジスタはレイヤ 2 フォワーディング エンジンにあり、レイヤ 2 レート リミッタ用に予約されています。残りの 8 つのレジスタはレイヤ 3 フォワーディング エンジンにあり、レイヤ 3 レート リミッタ用に予約されています。一部のレート リミッタはデフォルトでイネーブルになりますが、その他は設定する必要があります。MLS レート リミッタの設定には、**mls rate-limit** コマンドを使用します。

  アクティブおよび非アクティブのレート リミッタと、パント パケットに使用される宛先インデックスを表示するには、RP CPU では **show mls rate-limit** コマンド、SP CPU では **show mls rate-limit hw-detail** コマンドを使用します。一部のレート制限シナリオは、同じレジスタを共有するように事前設定されています。どのレート リミッタが同じレジスタを共有するかを調べるには、RP CPU に対して **show mls rate-limit usage** コマンドを実行します。MLS レート リミッタの設定の詳細については、「MLS レート リミッタのデフォルト設定」（P.40-24）を参照してください。
- コントロール プレーン ポリサー：MQC を使用して設定されたコントロール プレーン ポリサーは、RP CPU にパントされるユニキャスト トラフィックにのみ適用されます。コントロール プレーン ポリサーおよび MLS レート リミッタを経由するパケット パスを同時に使用することはできません。パケットが MLS レート リミッタを通過する場合は、コントロール プレーン ポリサーによって制限することはできません。CoPP は、提供されるレート、ドロップ レート、およびパケット カウンタの可視性を高めます。
  show policy-map control-plane コマンドを実行すると、コントロール プレーン ポリサーの統計情報が表示されます。

図 40-2 および図 40-3 に、EARL におけるユニキャスト パケットとマルチキャスト パケットのパケット パスを示します。

図 40-2　EARL におけるユニキャスト パケットのパケット パス

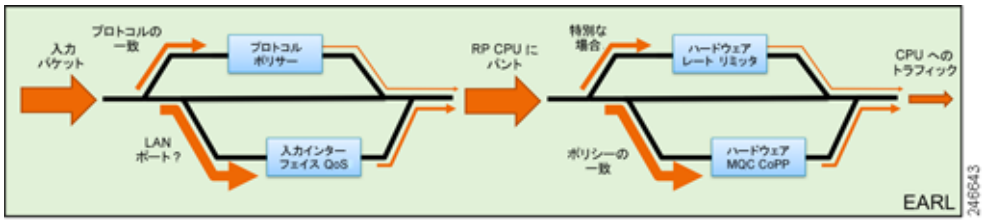
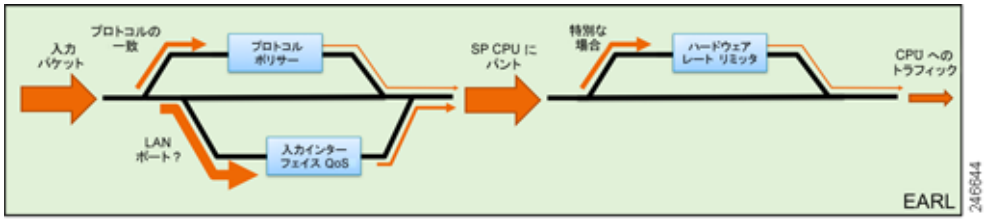


図 40-3　EARL におけるマルチキャスト パケットのパケット パス

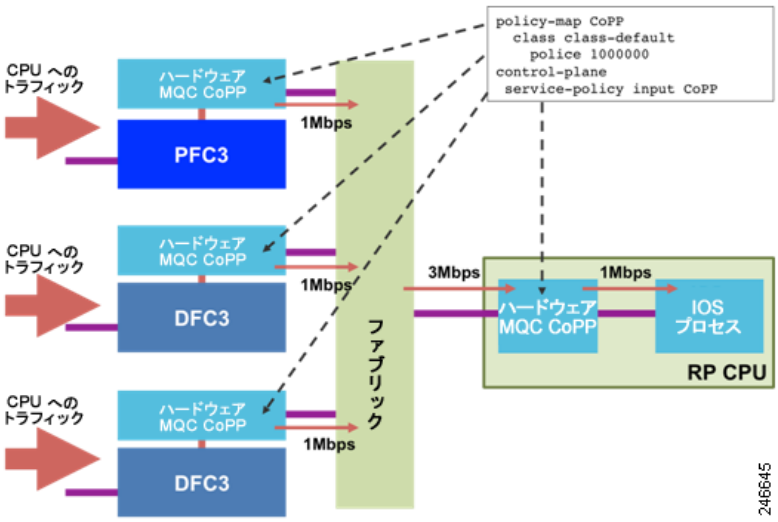


着信パケットはまず、MLS プロトコル ポリサーに照らして評価されます。MLS プロトコル ポリサーと入力 PFC または DFC QoS は、同時に使用できません。MLS プロトコル ポリサーと入力 PFC または DFC QoS は、転送が決定される前に実行されます。

転送の決定により、パケットが RP CPU にパントされる場合、パント パケットは設定されているレート リミッタに照らして評価されます。パケットがレート リミッタに一致した場合、パケットは適切なレート リミッタを通過します。設定されているレート リミッタのいずれにも一致せず、RP CPU に宛先指定される場合は、ハードウェア CoPP を通過します。MLS レート リミッタおよびハードウェア CoPP は同時に使用できません。ハードウェア CoPP は、SP CPU へのパント パスでは適用されません。MLS レート リミッタおよびハードウェア CoPP は出力機能であり、転送の決定後に適用されます。

図 40-4 で、PFC または DFC 上の CoPP について説明します。

図 40-4　PFC または DFC 上のコントロール パネル ポリサー（ハードウェア CoPP）



MLS レート リミッタと CoPP は両方ともグローバル コンフィギュレーション モードで設定されます。いったん設定されると、同じ設定がシャーシ内のすべての PFC または DFC に伝播されます。CoPP の最初の部分は PFC または DFC に適用され、2 番目の部分は RP CPU に適用されます。MLS レート リミッタは、PFC または DFC 上のハードウェアにのみ適用されます。

コントロール プレーン保護のためのハードウェア ポリシングおよびレート制限は、PFC または DFC ごとに集約されます。各 PFC または DFC を介して集約されたトラフィックは、CoPP によってソフトウェア レベルで再びポリシングされます。

たとえば、シャーシに 2 つの DFC と 1 つの PFC があり、CoPP の集約ポリサー レートが 1 Mbps に設定されている場合、RP CPU は最大 3 Mbps のトラフィックを受信し、ソフトウェアで 1 Mbps にポリシングされます。

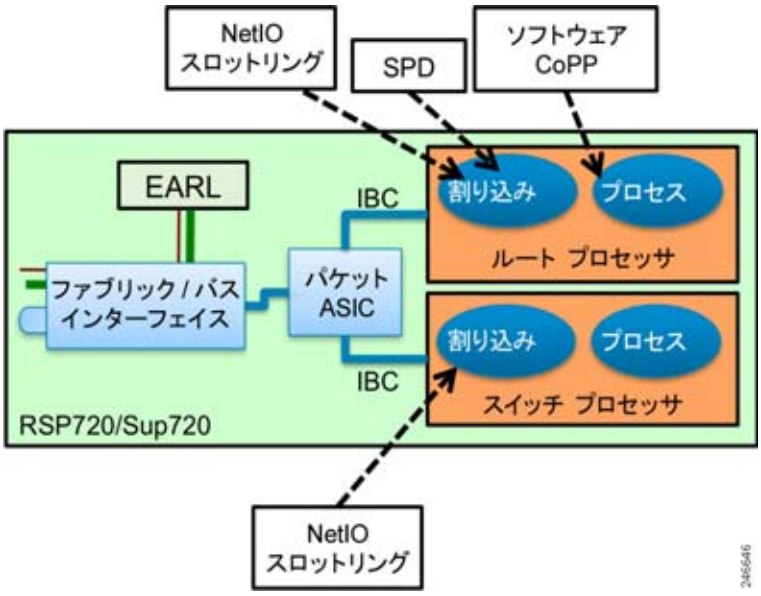
show policy-map control-plane コマンドを実行すると、すべての PFC または DFC、および IOS に関するコントロール プレーン ポリサーの統計情報が表示されます。RP CPU に対して **show mls rate-limit** コマンドを実行すると、アクティブ PFC の設定のみが表示されます。DFC とスタンバイ PFC の設定を表示するには、DFC およびスタンバイ RP それぞれに対して **show mls rate-limit** コマンドを実行します。

PFC または DFC の後にパントされるパケットのパス

RSP720/SUP 720 ハードウェア

図 40-5 に、PFC または DFC の後にパントされるパケットのパスを示します。

図 40-5　RSP720 または SUP 720 上のパケット パス



PFC または DFC は、パケットのパントを決定すると、スイッチ ファブリック経由でスーパーバイザ上のファブリック インターフェイスまたはバス インターフェイスにパケットを送信するよう、入力ラインカードに指示します。ファブリックまたはバス インターフェイスはパケットをパケット ASIC に転送します。パケット ASIC は、パケットを SP または RP CPU に転送します。

各プロセッサには、2 つの入力キューを持つ別個の In-band Interface Channel（IBC）が搭載されています。高プライオリティ キュー（キュー 0）は、データ バス CoS 値 4 ～ 7 のパケットを受信し、低プライオリティ キュー（キュー 1）は、データバス CoS 値 0 ～ 3 のパケットを受信します。IBC コントローラは、パケットを受信すると、そのパケットを IOS 入出力メモリにコピーし、Network Input/Output（NetIO; ネットワーク入出力）割り込みを CPU に要求します。

SPD の統計情報を含む、IBC で受信したパケットの詳細情報を得るには、**show ibc exec** コマンドを使用します。このコマンドを実行すると、カウンタに関する情報が表示され、設定されているコントロール プレーン保護がパントされたトラフィックのレートを制限していることを確認するのに役立ちます。また、SP および RP でパントされたトラフィックをトラブルシューティングするのにも役立ちます。

次に、**show ibc exec** コマンドの出力例を示します。

```
Router# show ibc | inc Rx\(
  Rx(0)    23116485         2693239358
  Rx(1)    2294534          386747297
```

IOS 上のパントされたパケットのパス

NetIO 割り込みが要求されると、NetIO 割り込みハンドラ ルーチンによってインターフェイス ドライバが呼び出されます。IBC から受信した複数のパケットを 1 つの NetIO 割り込みで処理できます。現在の NetIO 割り込みが netint usec（ネットワーク レベルの割り込みの実行が許可されている最大時間、マイクロ秒単位）期間よりも長い場合、NetIO 割り込みハンドラは終了し、netint mask usec（ネットワーク レベルの割り込みがマスキングされる最大時間）期間中は NetIO 割り込みがディセーブルになります。このメカニズムを NetIO スロットリングと呼びます。NetIO スロットル中は、受信バッファが満杯にならない限り、DMA を介した IO メモリへのパケットのコピーが行われます。NetIO スロットリングによって遅延するのは、NetIO 割り込みの処理のみです。NetIO スロットリング中にドロップされるパケットに対する制御はないので、RP または SP CPU にパントされるパケットに対して適切な制御を課すことが重要です。

NetIO 割り込み中は、インターフェイス ドライバがパケットのタイプの決定し、適切なネットワーク プロトコル パケットに対応する NetIO 割り込みハンドラを呼び出します。パケットが IP パケットである場合、c7600 では RP CPU によるソフトウェア転送が許可されているので、IOS はまず Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）ルーチンを呼び出します。パケットを割り込みレベルで転送できない場合、またはルータに宛先指定される場合、パケットはプロセス レベルにパントされます。

パケットを入力プロセス キューに配置するように CEF が試みる前に、SPD メカニズムが適用されます。SPD では、通常のパケットに許可された制限を超える高プライオリティ パケットをバッファリングして、重要なパケットのドロップを回避できます。

インターフェイスの入力キュー内のパケット数が入力キューの制限に達すると、インターフェイスはスロットリングされます。つまり、スロットルが解除されるまで、このインターフェイスではそれ以上のパケットは受信されません。このメカニズムをインターフェイス スロットリングと呼びます。スロットリングされたインターフェイスでドロップされるパケット数を確認するには **show ibc** コマンドを使用し、インターフェイスがスロットリングされる回数を確認するには **show interfaces** コマンドを使用します。インターフェイスのスロットル時に SPD ヘッドルームおよび SPD 拡張ヘッドルームに入るパケットのドロップを防止するには、throttle selective インターフェイス コンフィギュレーション コマンドを設定します。SPD でパケットがドロップされない場合は、ソフトウェア CoPP がプロセス レベルで適用されます。したがって、CoPP の設定が最適であることを確認することが重要です。

NetIO 割り込みタイマーおよびスロットリングの統計情報を調べるには、**show platform netint** コマンドを使用します。

次に、**show platform netint** コマンドの出力例を示します。

```
Router# show platform netint
 Network IO Interrupt Throttling:
 throttle count=90, timer count=90
 active=0, configured=1
 netint usec=4000, netint mask usec=800
inband_throttle_mask_hi = 0x0
inband_throttle_mask_lo = 0x800000
```

show platform netint コマンドの **timer count** は **netint mask usec** タイマーが起動した回数を示し、**throttle count** は NetIO 割り込みがスロットリングされる回数を示します。

コントロール プレーン保護のベスト プラクティス

次に、コントロール プレーン保護に伴うベスト プラクティスを示します。

- ストーム制御を展開します。
- 重要なコントロール プレーン トラフィックがインターフェイスで受信される場合、ポート状態を trust として設定します。ポートが信頼できない場合、CoS および IP precedence はゼロにリセットされ、パント パスにおけるパケットの優先順位付けに影響します。
- 適用する必要のある CoPP ポリシーを決定します。
- c7600 上の異なる保護メカニズムの制限を考慮しながら、コントロール プレーン保護を実装します。
- MLS レート リミッタまたは MLS プロトコル ポリシングを使用して、その他のトラフィックをレート制限する必要があるかどうかを判断します。
- トラフィック レートをモニタし、調整します。トラフィック レートのモニタについては、次のコマンドが役立ちます。
  - **show mls statistics [***module***]** コマンド。MLS 統計情報に関する情報を表示します。
  - **show policy-map control-plane** コマンド。特に class-default における、コントロール プレーン ポリサーの分類カウンタの情報を表示します。
  - **show platform netint** コマンド。NetIO スロットル カウントおよびタイマー カウントに関する情報を表示します。
  - **show ibc** コマンド。分類およびドロップ カウンタに関する情報を表示します。
  - **debug netdr capture** コマンド。パントされたパケットのキャプチャに関する情報を表示します。キャプチャされたパケットを表示するには、**show netdr captured-packets** コマンドを使用します。

DoS 保護の機能概要

ここでは、Cisco 7600 シリーズ ルータにおける DoS 保護の概要、および数種類の DoS 攻撃シナリオについて説明します。

- 「PFC3 による DoS 保護」（P.40-11）

PFC3 による DoS 保護

ここでは、PFC3 によって DoS 攻撃に対処する方法、および設定例について説明します。PFC3 では、次の方法を使用して DoS 攻撃に対する多重保護を実現します。

- CPU レート リミッタ：トラフィック タイプを制御します。
- Control Plane Policing（CoPP）：コントロール プレーン トラフィックのフィルタ処理およびレート制限を行います。CoPP の詳細については、「制御プレーン ポリシングの機能概要」（P.40-31）を参照してください。

ここでは PFC3 による DoS 保護について説明します。

- 「セキュリティ ACL および VACL」（P.40-12）
- 「QoS レート制限」（P.40-13）
- 「uRPF チェック」（P.40-13）

- 「トラフィック ストーム制御」（P.40-14）
- 「SYN 攻撃を受けているネットワーク」（P.40-14）
- 「MLS プロトコル ポリシング」（P.40-15）
- 「PFC3 におけるハードウェアベースのレート リミッタ」（P.40-16）
- 「共有レート リミッタ」（P.40-16）
- 「推奨レート リミッタ設定」（P.40-16）
  - 「入出力 ACL ブリッジド パケット（ユニキャストのみ）」（P.40-17）
  - 「uRPF チェック エラー」（P.40-18）
  - 「TTL エラー」（P.40-18）
  - 「ICMP 到達不能（ユニキャストのみ）」（P.40-18）
  - 「FIB（CEF）受信ケース（ユニキャストのみ）」（P.40-19）
  - 「FIB 収集（ユニキャストのみ）」（P.40-19）
  - 「レイヤ 3 セキュリティ機能（ユニキャストのみ）」（P.40-19）
  - 「ICMP リダイレクト（ユニキャストのみ）」（P.40-20）
  - 「VACL ログ（ユニキャストのみ）」（P.40-20）
  - 「MTU エラー」（P.40-20）
  - 「レイヤ 2 マルチキャスト IGMP スヌーピング」（P.40-20）
  - 「レイヤ 2 PDU」（P.40-21）
  - 「レイヤ 2 プロトコル トンネリング」（P.40-21）
  - 「IP エラー」（P.40-21）
  - 「IPv4 マルチキャスト」（P.40-21）
  - 「IPv6 マルチキャスト」（P.40-22）

セキュリティ ACL および VACL

ネットワークが DoS 攻撃を受けている場合、DoS パケットがターゲットに達する前に DoS パケットをドロップする有効な方法は ACL です。特定ホストからの攻撃が検出された場合は、セキュリティ ACL を使用します。次の例では、ホスト 10.1.1.10 およびそのホストからのすべてのトラフィックが拒否されます。

```
Router(config)# access-list 101 deny ip host 10.1.1.10 any
Router(config)# access-list 101 permit ip any any
```

セキュリティ ACL は、アドレスのスプーフィングからも保護します。たとえば送信元アドレス A がネットワーク内にあり、ルータ インターフェイスがインターネットに向いているとします。ルータ インターネット インターフェイスで着信 ACL を適用すれば、送信元が A（内部アドレス）になっているすべてのアドレスを拒否できます。この処理では、攻撃者が内部送信元アドレスをスプーフィングする攻撃が防止されます。パケットは、ルータ インターフェイスに到着したとき、その ACL と一致してドロップされるので、被害は発生しません。

Cisco 7600 シリーズ ルータを Cisco Intrusion Detection Module（CIDM）で使用している場合は、センシング エンジンによる攻撃の検出に対応して、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、レイヤ 4 の情報に基づくセキュリティ処理ツールです。パケットに対する VACL ルックアップの結果は、許可、拒否、許可および取り込み、リダイレクトのうちいずれかになります。VACL を特定 VLAN に関連付けると、すべてのトラフィックは、VACL によって許可されないと VLAN に入ることができません。VACL はハードウェアで処理されるので、Cisco 7600 シリーズ ルータで VACL を VLAN に適用してもパフォーマンスは低下しません。

QoS レート制限

QoS ACL は、MSFC3 によって処理される特定タイプのトラフィックの量を制限します。MSFC に DoS 攻撃が仕掛けられた場合、QoS ACL では、DoS トラフィックが MSFC データ パスに達して MSFC データ パスを輻輳させることを防止できます。PFC3 は QoS をハードウェアで実行するので、DoS トラフィックが効果的に制限され（そのトラフィックが識別されている場合）、ルータが MSFC に影響を与えることを防止できます。

たとえば Ping-of-Death 攻撃または smurf 攻撃をネットワークが受けている場合、管理者は ICMP トラフィックをレート制限して DoS 攻撃に対処する必要がありますが、正当なトラフィックがプロセッサを通り、MSFC またはホストに転送されるようにする必要があります。このレート制限設定は、レート制限が必要なフローごとに実行する必要があり、レート制限ポリシー アクションはインターフェイスに適用する必要があります。

次の例では、アクセス リスト 101 が、任意の送信元から任意の宛先への ping（エコー）ICMP メッセージを許可してトラフィックとして識別します。ポリシー マップ内では、ポリシング ルールが特定認定情報レート（CIR）とバースト値（96000 bps および 16000 bps）を定義し、シャーシを経由する ping（ICMP）トラフィックをレート制限します。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。ポリシー マップが適用されている VLAN またはインターフェイスにおいて ping トラフィックが指定したレートを超えた場合、ping トラフィックはマークダウン マップに指定されたようにドロップされます（通常バースト設定のマークダウン マップは、この例に示していません）。

```
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、検証可能送信元 IP アドレスがないパケットはドロップされます。送信元アドレス、および受信したインターフェイスが、スーパーバイザ エンジンの FIB テーブルと一致することを確認するために、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）テーブルが使用されます。

uRPF チェックをインターフェイスで VLAN ごとにイネーブルにすると、着信パケットは逆ルックアップで CEF テーブルと比較されます。いずれかの逆パス ルートからパケットを受信した場合、そのパケットは転送されます。パケットを受信したインターフェイスに逆パス ルートがない場合、パケットは uRPF チェックでエラーになり、uRPF チェック エラー トラフィックに ACL が適用されるかどうかによってドロップされるか転送されます。CEF テーブルで ACL が指定されていない場合、偽造パケットはすぐにドロップされます。

uRPF チェックでエラーになったパケットには、uRPF チェックの ACL だけを指定できます。ACL では、パケットをすぐにドロップする必要があるか転送する必要があるかがチェックされます。ACL を使用した uRPF チェックは、ハードウェアの PFC3 で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。

ハードウェアでは、PFC3 での uRPF チェックがサポートされます。ただし uRPF チェックでエラーになって、適用された ACL のために転送されたすべてのパケットは、MSFC に送信されてレート制限され、ICMP 到達不能メッセージが生成されます。この処理はすべてソフトウェアで行われます。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 ストーム制御機能では、ネットワーク設定の誤りから、または DoS 攻撃をしているユーザから、物理インターフェイスでのブロードキャスト トラフィック ストーム、マルチキャスト トラフィック ストーム、ユニキャスト トラフィック ストームによって LAN ポートが中断するのを防止します。トラフィック ストーム制御（トラフィック抑制）は、1 秒間のトラフィック ストーム制御インターバルで着信トラフィック レベルをモニタします。インターバル中は、トラフィック ストーム制御により、設定されているトラフィック ストーム制御レベルとトラフィック 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割合です。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で設定し、デフォルトではディセーブルです。次の設定例では、FastEthernet 2/3 でブロードキャスト アドレス ストーム制御のレベルを 20% にしています。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 ストーム制御インターバル内で、ポートの総使用可能帯域幅の 20% を超えた場合、トラフィック ストーム制御インターバルが終わるまで、トラフィック ストーム制御によってすべてのブロードキャスト トラフィックがドロップされます。

```
Router(config-if)# storm-control broadcast level 20
```

Cisco 7600 シリーズ ルータでは、すべての LAN ポートでブロードキャスト ストーム制御がサポートされ、ギガビット イーサネット ポートでマルチキャスト ストーム制御およびユニキャスト ストーム制御がサポートされます。

2 つまたは 3 つの抑制モードが同時に設定されている場合は、同一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、マルチキャスト抑制もイネーブルにして 70% のしきい値で設定した場合、ブロードキャスト抑制も 70% の設定になります。

SYN 攻撃を受けているネットワーク

SYN 攻撃を受けているネットワークは容易にわかります。ターゲット ホストは、異常に遅くなったり、クラッシュしたり、処理を中断したりします。MSFC では、ターゲット ホストから返されたトラフィックもトラブルの原因となります。リターン トラフィックは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、「本来の」IP トラフィックの場所が不足して、ルート キャッシュまたは CEF テーブルがオーバーフローすることがあるからです。

ネットワークが SYN 攻撃を受けている場合は、TCP 代行受信機能が攻撃的な保護となります。ルータにおける攻撃的な動作の開始時期と終了時期は、次の 2 つの要因によって決まります。

- 不完全接続の合計
- 最後の 1 分間のサンプル期間における接続要求数

低い値と高い値で両方の要因を設定します。

不完全接続数が 1,100 を超えるか、最後の 1 分間に到着した接続数が 1,100 を超えた場合は、新たに接続が到着するたびに、最も古い部分接続（またはランダム接続）が削除されます。これがデフォルト値ですが、変更できます。どちらかのしきい値を超えた場合、TCP 代行受信は、サーバが攻撃されていると見なし、アグレッシブ モードになって次のように反応します。

- 新たに接続が到着するたびに、最も古い部分（またはランダムな部分）が削除されます。
- 初期再送信タイムアウトが半減して 0.5 秒になり、接続の確立を試す合計時間が半分に短縮されます。
- ウォッチ モードでは、ウォッチ タイムアウトが半減します。

（注） 両方のしきい値が、設定されている低い値を下回ると、攻撃的な動作は終了します（デフォルト値は両方の要因で 900）。

すべての PFC3 タイプで、TCP フローはハードウェアによって処理されます。

MLS プロトコル ポリシング

悪意があるユーザは、攻撃中に、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で MSFC CPU を過負荷にしようとすることがあります。この特殊な制御パケットは、**mls qos protocol** コマンドで設定可能な特定ルーティング プロトコルおよび ARP ポリシング メカニズムを使用して、ハードウェアでレート制限できます。サポートされているルーティング プロトコルは、RIP、BGP、LDP、OSPF、IS-IS、IGRP、および EIGRP です。たとえば **mls qos protocol arp police 32000** コマンドでは、ハードウェアで ARP パケットが 32,000 bps にレート制限されます。このポリシング メカニズムでは、ラインレート ARP 攻撃などの攻撃から MSFC CPU が効果的に保護されますが、ルータへのルーティング プロトコルおよび ARP パケットがポリシングされるだけでなく、CoPP より粒度が低い機器を通過するトラフィックもポリシングされます。

ポリシング メカニズムとポリシング回避メカニズムは、ルート設定を共有します。ポリシング回避メカニズムでは、ルーティング プロトコルと ARP パケットが、QoS ポリサーに達したとき、ネットワークを流れます。このメカニズムは、**mls qos protocol** *protocol* **pass-through** コマンドで設定できます。

次に、ARP ポリシングで使用できるプロトコルを表示する例を示します。

```
Router(config)# mls qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp
```

次に、**mls qos protocol arp** コマンドで使用できるキーワードを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)
```

PFC3 におけるハードウェアベースのレート リミッタ

PFC3 では、ハードウェアベースのレート リミッタを追加でサポートします。PFC3 には新しいレート リミッタ用に 8 個のレート リミッタ レジスタがあり、ルータでグローバルに設定されます。このレート リミッタ レジスタはレイヤ 3 フォワーディング エンジン（PFC）に存在し、これにはさまざまな使用可能な設定済みレート リミッタと一致する結果パケットのレート制限情報が含まれます。

8 個のレート リミッタ レジスタが PFC3 に存在するので、このレジスタにより、さまざまなレート制限シナリオで同一レジスタを共有できます。このレジスタは先着順で割り当てられます。すべてのレジスタが使用されている場合は、あるレジスタを解放しないと、別のレート リミッタを設定できません。

PFC3 で使用できる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。

- 入力と出力の ACL ブリッジド パケット
- uRPF チェック エラー
- FIB 受信ケース
- FIB 収集ケース
- 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 ドロップ）
- ルートなし（FIB ミス）
- VACL ログ
- TTL エラー
- MTU エラー
- マルチキャスト IPv4
- マルチキャスト IPv6

共有レート リミッタ

次の共有レート リミッタを Cisco 7600 ルータ上で設定することができます。

- IP RPF エラー
- ICMP 到達不能ルートなし
- ICMP 到達不能 ACL 廃棄
- IP エラー

いずれかの共有レート リミッタをイネーブルまたはディセーブルにすると、その他すべての共有リミッタもイネーブルまたはディセーブルになります。

推奨レート リミッタ設定

推奨レート リミッタ設定は次のとおりです。

- DoS 攻撃によく使用されるトラフィック タイプに対して、レート リミッタをイネーブルにします。
- VACL ロギングを設定しない場合は、VACL ロギングでレート リミッタを使用しないでください。
- リダイレクトをディセーブルにします。Cisco 7600 シリーズ ルータのようにハードウェア転送をサポートするプラットフォームでは、リダイレクトの必要性が少なくなるからです。

- 到達不能をディセーブルにします。Cisco 7600 シリーズ ルータのようにハードウェア到達不能をサポートするプラットフォームでは、到達不能の必要性が少なくなるからです。
- すべてのインターフェイスで MTU が同一である場合は、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 PDU レート リミッタを設定する場合は、以下に注意してください。
  - 有効な PDU の予想数またはその可能な数を計算し、その数を 2 倍か 3 倍にします。
  - PDU には BPDU、DTP、VTP、PAgP、LACP、UDLD などが含まれます。
  - レート リミッタでは、優良フレームと不良フレームが区別されません。
- 15.1(1)S1 および 15.0(1)S3a リリース以降、MTU レート リミッタと TTL レート リミッタはデフォルトでイネーブルになります。
  - MTU と TTL のデフォルト値は、それぞれ 970 と 97 です。ルータの起動後にデフォルト値を変更することができます。
  - ルータ上で MTU と TTL のデフォルト以外の値が設定されている場合は、ユーザ定義の設定が優先されます。
  - MTU レート リミッタと TTL レート リミッタのデフォルト値を変更して、設定に保存することができます。
  - サポートされている最大レート リミッタが設定されている場合は、起動時に MTU レート リミッタと TTL レート リミッタがデフォルトでイネーブルになりません。ユーザ定義のレート リミッタが優先されます。

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 リミッタでは、入出力 ACL ブリッジ結果として、MSFC に送信されたパケットをレート制限します。ルータは、TCAM ブリッジ結果を含む既存および新規 ACL TCAM エントリを MSFC を示すレイヤ 3 リダイレクト結果に変更して、これを達成します。変更されたレイヤ 3 リダイレクト レート制限結果を含む TCAM エントリにヒットしたパケットは、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、両方とも同じレート リミッタ レジスタを共有するので、同じ値になります。ACL ブリッジ入出力レート制限がディセーブルである場合、レイヤ 3 リダイレクト レート制限結果は、ブリッジ結果に変換されます。

入力または出力の ACL ブリッジド パケット ケースでは、単一のレート リミッタ レジスタが共有されます。この機能がオンに切り替わっている場合、入力および出力の ACL では同一レート リミッタ値が使用されます。

バースト値では、バーストで許容されるパケット数が規制されます。各許容パケットではトークンが消費され、パケットが許容されるには、トークンが使用可能である必要があります。1 つのトークンは 1 ミリ秒ごとに生成されます。パケットが到着しない場合、トークンはバースト値まで累積されます。たとえばバースト値が 50 に設定されている場合、ルータは 50 個までのトークンを累積し、50 個のパケットのバーストを吸収できます。

次に、入力 ACL ブリッジ結果からのユニキャストパケットを 50000 パケット/秒にレート制限し、バーストの場合は 50 パケットにレート制限する例を示します。

```
Router(config)# mls rate-limit unicast acl input 50000 50
```

次に、出力 ACL ブリッジ結果において、入力 ACL ブリッジ結果からのユニキャスト パケットを同じレート（50000 pps、バーストの場合は 50 パケット）にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast acl output 50000 50
```

入力と出力の両方をイネーブルにしているとき、入力または出力のどちらかでレート リミッタの値を変更すると、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 インおよび ACL ブリッジド アウトの両方で新しい値 40000 pps が表示されます。

```
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 エラー

uRPF チェック エラー レート リミッタでは、uRPF チェックでエラーになったために MSFC に送信する必要があるパケットのレートを設定できます。uRPF チェックでは、インターフェイスの着信パケットが有効な送信元からのものであることが検証され、スプーフィングされた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限に抑えることができます。スプーフィングされたパケットが uRPF チェックでエラーになると、そのエラーが MSFC に送信されます。uRPF チェック レート リミッタでは、uRPF チェック エラーが発生したとき MSFC CPU にブリッジされる、pps をレート制限できます。

次に、バーストを 100 パケットにして、MSFC に送信される uRPF チェック エラー パケットを 100,000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast ip rpf-failure 100000 100
```

TTL エラー

このレート リミッタでは、TTL チェック エラーのために MSFC に送信されるパケットがレート制限されます。次の例で **all** キーワードによって示されるように、このレート リミッタは、マルチキャスト トラフィックとユニキャスト トラフィックの両方に適用されます。

（注） TTL エラー レート リミッタは、IPv6 マルチキャストでサポートされません。

次に、バーストを 150 にして TTL エラーを 70000 pps にレート制限する例を示します。

```
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、フラッディングさせるデバイス（この場合は MSFC）から到達不能な宛先アドレスを含む多数のパケットでデバイスがフラッディングされます。ICMP 到達不能レート リミッタでは、到達不能アドレスを含む、MSFC に送信されるパケットをレート制限できます。

次に、ACL 廃棄のために MSFC に送信されるパケットを 10,000 pps、バーストを 100 にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable acl-drop 10000 100
```

次に、FIB ミスのために ICMP 到達不能メッセージの生成が必要となったパケットを 80000 pps、バーストを 70 にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable no-route 80000 70
```

4 つのレート リミッタ、ICMP 到達不能ルートなし、ICMP 到達不能 ACL ドロップ、IP エラー、IP RPF エラーでは、単一のレート リミッタ レジスタが共有されます。このリミッタのいずれかをイネーブルにしている場合、このグループのすべてのリミッタでは同じ値が共有され、同じ状態（ON/ON/ON など）が共有されることもあります。レート リミッタの確認時に、別の機能を通してこのレジスタのメンバーがイネーブルになっていた場合は、ON ステータスの代わりに ON-Sharing ステータスが表示されます。TTL エラー レート リミッタは例外であり、その機能を手動でイネーブルにした場合は、この値はレジスタのその他のメンバーと同じ値を共有します。

FIB（CEF）受信ケース（ユニキャストのみ）

FIB 受信レート リミッタでは、MSFC IP アドレスを宛先アドレスとして含むすべてのパケットをレート制限できます。このレート リミッタでは、優良フレームと不良フレームが区別されません。

（注）　CoPP を使用している場合は、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。

次に、バーストを 60 にして、トラフィックを 25000 pps にレート制限する例を示します。

```
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 リミッタでは ARP トラフィックが制限されませんが、アドレス解決（ARP）が必要で MSFC に送信する必要があるトラフィックをレート制限する機能が用意されています。この状況は、トラフィックがポートに入り、MSFC にローカルに接続されているサブネットのホストが宛先になっていますが、その宛先ホスト用の ARP エントリが存在しない場合に発生します。この場合は、直接接続されている不明サブネットのホストによって宛先ホストの MAC アドレスが回答されないため、「収集」隣接がヒットし、トラフィックは MSFC に直接送信されて ARP 解決が行われます。このレート リミッタでは、攻撃者がこのような ARP 要求で CPU に過剰な負荷をかけることが制限されます。

次に、このトラフィックが MSFC に送信されるレートを 20,000 pps、バーストを 60 にレート制限する例を示します。

```
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）

一部のセキュリティ機能は、最初に MSFC に送信されて処理されます。このようなセキュリティ機能の場合は、MSFC に送信されるパケット数をレート制限し、潜在的な過負荷を削減する必要があります。このセキュリティ機能には、認証プロキシ（auth-proxy）、IPSEC、検査が含まれます。

認証プロキシは、入力ユーザか出力ユーザ、またはその両方を認証するために使用されます。このようなユーザは一般的にアクセス リストによってブロックされますが、auth-proxy を使用した場合、ユーザはブラウザを起動してファイアウォールを通過し、Terminal Access Controller Access Control System Plus（TACACS+）または RADIUS サーバ（IP アドレスに基づく）で認証できます。サーバは、アクセス リスト エントリをルータにさらに渡し、ユーザが認証後に通過できるようにします。この ACL はソフトウェアで保存されて処理されます。多くのユーザが auth-proxy を利用している場合は、MSFC に過剰な負荷がかかる場合があります。レート制限を行うとこのような状況で効果的になります。

IPSec および検査も MSFC によって実行され、レート制限が必要になることがあります。レイヤ 3 セキュリティ機能レート リミッタがイネーブルの場合は、auth-proxy、IPSec、検査のすべてのレイヤ 3 レート リミッタが同一レートでイネーブルになります。

次に、MSFC のセキュリティ機能を 100,000 pps に、バーストを 10 パケットにレート制限する例を示します。

```
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。たとえば最適でないルータでホストがパケットを送信すると、MSFC は ICMP リダイレクト メッセージをホストに送信し、その送信パスを訂正します。このトラフィックが継続的に発生してレート制限されない場合、MSFC は ICMP リダイレクト メッセージを継続的に生成します。

次に、バーストを 20 パケットにして、ICMP リダイレクトを 20000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 20000 20
```

VACL ログ（ユニキャストのみ）

VLAN-ACL ロギングのために MSFC に送信されるパケットをレート制限し、ロギング タスクによって CPU が過負荷にならないようにできます。VACL はハードウェアで処理されますが、MSFC がロギングを行います。VACL ロギングをルータで設定すると、VACL で拒否された IP パケットによってログ メッセージが生成されます。

次に、ロギング要求を 5000 pps にレート制限する例を示します（このレート リミッタの範囲は 10 ～ 5000 pps です）。

```
Router(config)# mls rate-limit unicast acl vacl-log 5000
```

MTU エラー

TTL エラー レート リミッタと同じように、MTU エラーのレート リミッタは、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でサポートされます。MTU チェックでエラーになったパケットは、MSFC CPU に送信されます。これにより、MSFC に過剰な負荷がかかることがあります。

次に、MSFC に送信される MTU エラー パケットを 10,000 pps に、バーストを 10 にレート制限する例を示します。

```
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

IIGMP スヌーピング レート リミッタでは、スーパーバイザ エンジンを宛先とするレイヤ 2 IGMP パケットの数が制限されます。IGMP スヌーピングは、ホストとスーパーバイザ エンジンの間で IGMP メッセージを待ち受けます。Cisco 7600 シリーズ ルータが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。ルータに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が両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、ルータはスイッチ 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（フレームの最初の 64 バイト）を送信します。

次に、IGMP スヌーピング トラフィックをレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

レイヤ 2 PDU

レイヤ 2 プロトコル データ ユニット（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 エンジンを宛先とするレイヤ 2 PDU プロトコル パケット（BPDU、DTP、PAgP、CDP、STP、および VTP パケット）の数を制限できます。Cisco 7600 シリーズ ルータが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。ルータに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が両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、ルータはスイッチ 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（フレームの最初の 64 バイト）を送信します。

次に、バーストを 20 パケットにして、レイヤ 2 PDU を 20,000 pps にレート制限する例を示します。

```
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 リミッタでは、スーパーバイザ エンジンを宛先とする制御 PDU、CDP、STP、VTP パケットなど、レイヤ 2 プロトコル トンネリング パケットが制限されます。これらのパケットはソフトウェアでカプセル化され（PDU で宛先 MAC アドレスが書き換えられ）、独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）に転送されます。Cisco 7600 シリーズ ルータが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。ルータに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が両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、ルータはスイッチ 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（フレームの最初の 64 バイト）を送信します。

次に、バーストを 10 パケットにして、レイヤ 2 プロトコル トンネリング パケットを 10000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit layer2 l2pt 10000 10
```

IP エラー

このレート リミッタでは、IP チェックサムと長さにエラーがあるパケットが制限されます。IP チェックサム エラーまたは長さ矛盾エラーを含むパケットは、PFC3 に到達すると、MSFC に送信してさらに処理する必要があります。攻撃者は、誤った形式のパケットを使用して DoS 攻撃を実行することがありますが、ネットワーク管理者は、このタイプのパケットにレートを設定し、制御パスを保護できます。

次に、バーストを 20 パケットにして、MSFC に送信される IP エラーを 1,000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit unicast ip errors 1000 20
```

IPv4 マルチキャスト

このレート リミッタでは、IPv4 マルチキャスト パケットが制限されます。このレート リミッタでは、ハードウェアのデータ パスからソフトウェアのデータ パスに送信されるパケットをレート制限できます。このレート リミッタでは、ソフトウェアの制御パスを輻輳から保護し、設定レートを超えるトラフィックをドロップします。IPv4 マルチキャスト レート リミッタには、FIB ミス レート リミッタ、マルチキャスト部分スイッチ フロー レート リミッタ、マルチキャスト直接接続レート リミッタという 3 つのレート リミッタがあり、設定することもできます。

FIB ミス レート リミッタでは、mroute テーブル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。

部分的にスイッチングされるフロー レート リミッタを使用すると、転送および複製用に MSFC3 を宛先とするフローをレート制限できます。特定マルチキャスト トラフィック フローでは、最低 1 つの発信レイヤ 3 インターフェイスがマルチレイヤ スイッチングされ、最低 1 つの発信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（ハードウェア スイッチング用に H ビットが設定されない）、特定フローは部分的にスイッチングされるか、部分 SC（部分ショートカット）と見なされます。H ビット フラグが設定されている発信インターフェイスはハードウェアでスイッチングされ、残りのトラフィックは MSFC3 によってソフトウェアでスイッチングされます。このため、転送および複製用に MSFC3 を宛先としたフローをレート制限することが望ましいことがあり、レート制限しない場合は CPU 使用率が上がることがあります。

マルチキャスト直接接続レート リミッタでは、直接接続された送信元からのマルチキャスト パケットが制限されます。

次に、バーストを 30 にして、マルチキャスト パケットを 30000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 30
```

ip-option キーワードおよび ip-option レート リミッタは、PFC3B モード、PFC3BXL モード、PFC3C モードまたは PFC3CXL モードだけでサポートされます。

次に、uRPF チェックでエラーとなった IPv4 マルチキャスト パケットのレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
```

次に、バーストを 10 にして、マルチキャスト FIB ミス パケットを 10000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 10000 10
```

次に、バーストを 20 パケットにして、部分ショートカット フローを 20000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 partial 20000 20
```

次に、バーストを 20 にして、マルチキャスト パケットを 30000 pps にレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 20
```

次に、IGMP スヌーピング トラフィックをレート制限する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

IPv6 マルチキャスト

このレート リミッタでは、IPv6 マルチキャスト パケットが制限されます。表 40-1 に、IPv6 レート リミッタ、およびそれぞれのレート リミッタによって処理されるトラフィック クラスを示します。

表 40-1　　IPv6 レート リミッタ

レート リミッタ	レート制限されるトラフィック クラス
接続	直接接続されている送信元トラフィック
デフォルト ドロップ	* (*, G/m) SSM * (*, G/m) SSM 非 rpf
ルート制御	* (*, FF02::X/128)

表 40-1　IPv6 レート リミッタ （続き）

レート リミッタ	レート制限されるトラフィック クラス
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

次のいずれかの方法を使用し、IPv6 マルチキャスト トラフィックのレート リミッタを設定できます。

- あるトラフィック クラスのレート リミッタの直接関連付け：レートを選択し、そのレートをレート リミッタに関連付けます。次に、1000 pps のレートおよびバーストごとに 20 パケットを選択し、そのレートを **default-drop** レート リミッタに関連付ける例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- 別の設定済みレート リミッタとのレート リミッタのスタティック共有：使用可能な隣接ベースのレート リミッタが十分でない場合は、設定済みレート 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。次に、**default-drop** ターゲット レート リミッタと **route-cntl** レート リミッタを共有する例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  ターゲット レート リミッタが設定されていない場合は、ターゲット レート リミッタを設定しないと、その他のレート リミッタと共有できないことを示すメッセージが表示されます。

- レート リミッタのダイナミック共有：どのレート リミッタを共有するかわからない場合は、**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、設定済みレート リミッタが選択され、その設定済みレート リミッタと指定レート リミッタが共有されます。次に、route-cntrl レート リミッタ用にダイナミックな共有を選択する例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

次に、直接接続された送信元からの IPv6 マルチキャスト パケットにレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
```

次に、あるトラフィック クラスにレート リミッタの直接関連を設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

次に、別の設定済みレート リミッタとレート リミッタをスタティックに共有することを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

次に、ルート制御レート リミッタでダイナミック共有をイネーブルにする例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

MLS レート リミッタのデフォルト設定

表 40-2 に、PFC3 ハードウェアベース レート リミッタの MLS レート リミッタのデフォルト設定を示します。

表 40-2　PFC3 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
入出力 ACL ブリッジド パケット	OFF	
RPF 障害	ON	100 pps、バーストは 10 パケット
FIB 受信ケース	OFF	
FIB 収集ケース	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、バーストは 10 パケット
VACL ログ	ON	2000 pps、バーストは 10 パケット
TTL エラー	OFF	
MTU エラー	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、バーストは 10 パケット
マルチキャスト IGMP	OFF	
マルチキャスト FIB ミス	ON	100000 pps、バーストは 100 パケット
マルチキャスト部分 SC	ON	100000 pps、バーストは 100 パケット
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、マルチキャストのケースではデフォルトの **100** がプログラムされます。

DoS 保護の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。

- 「PFC3」（P.40-24）

PFC3

PFC3 で設定したシステムに DoS 保護を設定する場合は、次の CPU レート リミッタの注意事項および制約事項に従ってください。

（注）　CoPP の注意事項および制約事項については、「CoPP の設定時の注意事項および制約事項」（P.40-31）を参照してください。

- PFC3A で設定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、次のレート リミッタを使用しないでください。
  - TTL エラー
  - MTU エラー
- 次のレート リミッタは、PFC3B モード、PFC3BXL モード、PFC3C モードまたは PFC3CXL モードだけ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 リミッタは次のとおりです。
  - 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 個のレイヤ 3 レジスタおよび 2 個のレイヤ 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 受信リミッタを使用しないでください。CEF 受信リミッタにより、CoPP トラフィックが無効になります。
- 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、それぞれのフォワーディング エンジンに適用されます（グローバルに適用されるレイヤ 2 ハードウェア レート リミッタを除く）。
- レイヤ 2 レート リミッタは、truncated モードでサポートされません。
- 入力および出力の ACL ブリッジド パケット レート リミッタの使用時には、次の制約事項が適用されます。
  - 入力と出力の ACL ブリッジド パケット レート リミッタは、ユニキャスト トラフィックだけで使用できます。
  - 入力および出力の ACL ブリッジド パケット レート リミッタでは、単一のレート リミッタ レジスタが共有されます。ACL ブリッジ入力レート リミッタおよび ACL ブリッジ出力レート リミッタをイネーブルにする場合は、入力 ACL および出力 ACL の両方で同一レート リミッタ値を共有する必要があります。
- 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 2/3 クラウドの IGMP または PIM パケットのパントを制限するには、mls rate-limit multicast ipv4 igmp/pim *rate in pps* burst *size* コマンドを使用します。

パケット廃棄統計情報のモニタ

あるインターフェイスの着信トラフィックまたは発信トラフィックを取り込み、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、トラフィック アナライザによってモニタできます。トラフィックを取り込んで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。

トラフィックの取り込み時には、次の制約事項が適用されます。

- 着信取り込みトラフィックはフィルタ処理されません。
- 着信取り込みトラフィックは、取り込み宛先にレート制限されません。

monitor session コマンドを使用したドロップ パケットのモニタ

次に、**monitor session** コマンドを使用して、トラフィックを取り込んで外部インターフェイスに転送する例を示します。

```
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
```

次に、**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例を示します。

```
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 コマンドを使用したドロップ パケットのモニタ

PFC3B モード、PFC3BXL モード、PFC3C モードおよび PFC3CXL モードでは、ハードウェアにおける ACL ヒット カウンタがサポートされます。ACL TCAM におけるそれぞれのエントリを表示するには、**show tcam interface** コマンドを使用できます。

次に、**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する例を示します。

```
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 および IP のオプション カウンタを使用し、レイヤ 3 フォワーディング 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。

次に、**show mls statistics** コマンドを使用して、レイヤ 3 フォワーディング エンジンに関連するパケット統計およびエラーを表示する例を示します。

```
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 取り込みを使用したドロップ パケットのモニタ

VACL 取り込み機能では、取り込み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。

各 VLAN から別のインターフェイスにトラフィックを割り当てるには、VACL 取り込みを使用できます。

VACL 取り込みでは、HTTP などの、あるタイプのトラフィックを 1 つのインターフェイスに、DNS などの別のタイプのトラフィックを別のインターフェイスに送信できません。VACL 取り込み粒度は、ローカルにスイッチングされるトラフィックだけに適用可能です。トラフィックをリモート ルータに転送する場合は、粒度を維持できません。

次に、VACL 取り込みを使用して、トラフィックを取り込んでローカル インターフェイスに転送する例を示します。

```
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 コマンドでは、設定したレート リミッタに関する情報が表示されます。**show mls rate-limit usage** コマンドでは、レート リミッタ タイプによって使用されるハードウェア レジスタが表示されます。レジスタが、どのレート リミッタ タイプによっても使用されない場合は、出力に Free と表示されます。レジスタがレート リミッタ タイプによって使用されている場合は、Used と表示されて、レート リミッタ タイプも表示されます。

コマンド出力において、レート制限ステータスは次のうちいずれかになります。

- On は、特定ケースのレートが設定されていることを示します。
- Off は、レート リミッタ タイプが設定されておらず、そのケースのパケットがレート制限を受けないことを示します。
- CPU の使用率が高くなるのは次のような場合です。
  - CoPP レートが過剰なトラフィックを制限してドロップしている
  - mls qos protocol protocol pass-through が設定されている

  これを回避するには、**mls qos protocol** ではなく、過剰なトラフィックをドロップする CoPP に依存します。
- On/Sharing は、同一共有グループに属する別のレート リミッタの設定により、特定ケース（手動で設定していない）が影響されることを示します。
- ハイフンは、マルチキャスト部分 SC レート リミッタがディセーブルであることを示します。

コマンド出力において、レート制限共有は次の情報を示します。

- 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 ダイナミック共有コード

設定されているレート リミッタを表示するには、**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#
```

ハードウェア制限により、PFC または DFC は、MLS レート リミッタに渡したパケット数またはドロップしたパケット数を報告できません。ただし、**show mls statistics** コマンドと **terminal exec prompt timestamp** コマンドを使用して、一部のエラー パケットのレートを計算できます。

MLS レート リミッタの設定例

ここでは、MLS レート リミッタの設定例を示します。要件を満たすには、この例を適宜変更する必要があります。

この設定例は、Cisco IOS 12.2(33)SRE3、15.0(1)S3、15.1(1)S2、およびそれ以降のリリースに有効です。

```
Router(config)# mls rate-limit unicast acl input 1000 10
Router(config)# mls rate-limit unicast acl output 1000 10
```

```
Router(config)# mls rate-limit multicast ipv4 igmp 1000 10
Router(config)# mls rate-limit multicast ipv4 fib-miss 100 10
Router(config)# mls rate-limit multicast ipv4 partial 100 10
Router(config)# mls rate-limit multicast ipv4 connected 100 250
Router(config)# no mls rate-limit unicast acl vacl-log
Router(config)# mls rate-limit unicast ip options 1000 10
Router(config)# mls rate-limit multicast ipv4 ip-options 1000 10
```

Cisco IOS 12.2(33)SRE3 よりも前のリリースについては、MLS レート リミッタの設定に次の 2 行を追加してください。

```
Router(config)# mls rate-limit all ttl-failure 100 10
Router(config)# mls rate-limit all mtu-failure 100 10
```

この設定では、**show mls rate-limit** コマンドの出力例にあるとおり、8 つのレート制限レジスタをすべて使用しています。

```
Router# show mls rate-limit | exclude -     -
 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 DFLT ADJ   On                100      10  Not sharing
      MCAST DIRECT CON   On                100     250  Not sharing
        ACL BRIDGED IN   On               1000      10  Group:1 S
       ACL BRIDGED OUT   On               1000      10  Group:1 S
      MCAST PARTIAL SC   On                100      10  Not sharing
        IP RPF FAILURE   On                100      10  Group:0 S
           TTL FAILURE   On                 97      10  Not sharing
 ICMP UNREAC. NO-ROUTE   On                100      10  Group:0 S
 ICMP UNREAC. ACL-DROP   On                100      10  Group:0 S
           MTU FAILURE   On                997      10  Not sharing
       MCAST IP OPTION   On               1000      10  Group:3 S
       UCAST IP OPTION   On               1000      10  Group:2 S
             IP ERRORS   On                100      10  Group:0 S


Router# show mls rate-limit usage
                             Rate Limiter Type     Packets/s   Burst
                           ---------------------   ---------   -----
Layer3 Rate Limiters:
             RL# 0: Used
                                  MCAST IP OPTION        1000      10
             RL# 1: Used
                                MCAST DIRECT CON         100     250
             RL# 2: Used
                                  ACL BRIDGED IN        1000      10
                                 ACL BRIDGED OUT        1000      10
             RL# 3: Used
                                 UCAST IP OPTION        1000      10
             RL# 4: Used
                                  MCAST DFLT ADJ         100      10
             RL# 5: Used
                                  IP RPF FAILURE         100      10
                               ICMP UNREAC. NO-ROUTE     100      10
                               ICMP UNREAC. ACL-DROP     100      10
                                        IP ERRORS        100      10
             RL# 6: Used
                                    MTU FAILURE         997      10
             RL# 7: Used
                                    TTL FAILURE          97      10
             RL# 8: Rsvd for capture           -           -       -
```

```
Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
             RL#11: Free                    -          -       -
             RL#12: Free                    -          -       -
```

制御プレーン ポリシングの機能概要

Control Plane Policing（CoPP; 制御プレーン）機能では、不必要なトラフィックや DoS トラフィックから MSFC を保護して、重要な制御プレーンおよび管理トラフィックに優先順位を付けることによって、Cisco 7600 シリーズ ルータのセキュリティが向上します。PFC3 および DFC3 では、CoPP がハードウェアでサポートされます。CoPP は PFC3 レート リミッタと連携して動作します。

PFC3 では、組み込みの「特殊ケース」レート リミッタがサポートされます。IP オプション ケース、TTL および MTU のエラー ケース、エラーを含むパケット、マルチキャスト パケットなどの特定シナリオを ACL が分類できない場合は、これを使用できます。特殊ケース レート リミッタをイネーブルにすると、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされます。

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、つまり *プレーン*に分割されます。

- データ プレーン
- 管理プレーン
- 制御プレーン

MSFC によって管理されるトラフィックの大部分は、制御プレーンおよび管理プレーンの方法によって処理されます。CoPP を使用すると、制御プレーンおよび管理プレーンを保護でき、ルーティングの安定性、到達可能性、パケット配信を確保できます。CoPP では、Modular QoS CLI（MQC）で専用制御プレーン設定が使用され、フィルタ機能およびレート制限機能が制御プレーン パケットに提供されます。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルになります。CoPP をイネーブルにすることを推奨します。CoPP の詳細については、次の URL にある『Control Plane Policing Implementation Best Practices』を参照してください。http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

CoPP の設定時の注意事項および制約事項

CoPP を設定するときは、次の注意事項および制約事項に従ってください。

- マルチキャストに一致するクラスはハードウェアで適用されず、ソフトウェアで適用されます。
- CPP は、ハードウェアでブロードキャスト パケット用にサポートされません。ACL、トラフィック ストーム制御、CPP ソフトウェア保護の組み合わせにより、ブロードキャスト DoS 攻撃から保護されます。
- CoPP では ARP ポリシーがサポートされません。ARP ポリシング メカニズムにより、ARP ストームから保護されます。

- CoPP では、デフォルトの非 IP クラスを除いて、非 IP クラスがサポートされません。非 IP クラスの代わりに ACL を使用して非 IP トラフィックを廃棄でき、デフォルトの非 IP CoPP クラスを使用して、RP CPU に到達する非 IP トラフィックに制限できます。
- CoPP ポリシー ACL では **log** キーワードを使用しないでください。
- PFC3A では、出力 QoS および CoPP を同時に設定できません。この状況では、CoPP がソフトウェアで実行されます。出力 QoS および CoPP を同時に設定できないことを通知する警告メッセージが表示されます。
- QoS 設定が大きい場合は、TCAM スペースが不足することがあります。この場合は、CoPP がソフトウェアで実行される場合があります。
- その他のインターフェイスで QoS 設定が大きい場合は、TCAM スペースが不足することがあります。この状況が発生した場合は、CoPP が全体的にソフトウェアで実行され、パフォーマンスの低下および CPU サイクルの消費という結果になることがあります。
- CoPP ポリシーによって、ルーティング プロトコルまたはルータへの対話型アクセスなどの重要なトラフィックがフィルタリングされないことを確認してください。このトラフィックをフィルタリングすると、ルータへのリモート アクセスが妨害され、コンソール接続が必要になることがあります。
- PFC3 では組み込みの特殊ケース レート リミッタがサポートされます。これは、TTL、MTU、IP のオプションなど、ACL を使用できない状況で役立ちます。特殊ケース レート リミッタをイネーブルにする場合は、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされることに注意してください。
- **mls qos** コマンドを使用して MMLS QoS をグローバルにイネーブルにしないと、CoPP はハードウェアでイネーブルになりません。**mls qos** コマンドを入力しない場合、CoPP はソフトウェアだけで動作し、ハードウェアにとって有用にはなりません。
- 出力 CoPP もサイレント モードも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、制御プレーン インターフェイスに適用できません）。
- ハードウェアの ACE ヒット カウンタは ACL ロジック専用です。ソフトウェア ACE ヒット カウンタ、および **show access-list** コマンド、**show policy-map control-plane** コマンド、**show mls ip qos** コマンドを使用して、CPU トラフィックのトラブルシューティングと評価ができます。
- CoPP は転送エンジンごとに実行され、ソフトウェア CoPP は一括で実行されます。
- CoPP は、ハードウェアでマルチキャスト パケット用にサポートされません。ACL、マルチキャスト CPU レート リミッタ、CoPP ソフトウェア保護の組み合わせにより、マルチキャスト DoS 攻撃から保護できます。
- CoPP では、**log** キーワードを使用した ACE がサポートされません。
- CoPP では、ハードウェア QoS TCAM リソースが使用されます。**show tcam utilization** コマンドを入力し、TCAM の使用状況を確認してください。
- CoPP が設定されているときに、ユニキャスト トラフィックが CoPP 分類を通過すると、入力ポート上で設定された信頼に関係なく、RP にパントされたパケットが trust DSCP アクションを使用して処理されます。CoPP が設定されており、パントされたパケットを入力ポートに基づいてマーキングまたは信頼する場合は、入力ポート上で **platform ip features sequential** コマンドを実行します。マルチキャスト トラフィックとブロードキャスト トラフィックはハードウェア Copp 分類を通過しないため、この動作はマルチキャスト トラフィックとブロードキャスト トラフィックに適用されません。
- ポリサー値を設定する場合は、mls qos protocol がサポートされており、ルータ内のトラフィック スイッチが影響を受けることに注意してください。

- 着信制御パケットにコントロール プレーン SPD で優先順位を付けるには、これらのパケットが信頼される必要があります。そうしないと、これらのパケットは、RP にパントされるその他のデータ パケットと競合する場合があり、それによってドロップされる可能性が高まります。
- LAN インターフェイスに入るパケットの場合：
  - CoPP がルータで適用されない場合は、**mls qos trust** を使用して、入力トラフィック DSCP または precedence が信頼されるようにすることをお勧めします。着信制御プロトコル パケットの precedence 6 未満の precedence 値への再マーキングを回避してください。制御プロトコル パケットは、その precedence 値または DSCP 値に基づいて分類することができます。
  - CoPP が適用され、ユニキャスト トラフィックが CoPP 分類に到達した場合、CoPP は着信信頼状態を trust dscp にオーバーライドし、コントロール プレーンにパントされるパケットの DSCP または precedence を維持します。マルチキャスト トラフィックおよびブロードキャスト トラフィックはハードウェア CoPP 分類を通過しないので、これはマルチキャスト トラフィックとブロードキャスト トラフィックには適用されません。
- SIP 400 および ES+ ラインカードなどの WAN インターフェイスに入るパケットについては、着信制御プロトコル パケットの precedence 値が precedence 6 または 7 未満に再マーキングされないようにしてください。制御プロトコル パケットは、その precedence 値または DSCP 値に基づいて識別することができます。
- CoPP がレート制限して過剰なトラフィックをドロップし、さらに、**mls qos protocol** コマンドで protocol pass-through モードが設定されていると、CPU の使用率が高くなります。これを回避するには、過剰なトラフィックをドロップするための CoPP は使用して、トラフィックをルート プロセッサに直接ルーティングするための **mls qos protocol** コマンドは使用しないでください。CoPP トラフィックの分類については、「トラフィック分類の概要」（P.40-40）を参照してください。

CoPP の設定

CoPP は MQC を使用してトラフィック分類基準を定義し、分類されたトラフィックの設定可能ポリシー アクションを指定します。最初にクラス マップを定義し、分類するトラフィックを識別する必要があります。クラス マップでは、特定トラフィック クラスのパケットが定義されます。トラフィックを分類したら、識別されたトラフィックにポリシー アクションを実行するための、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 コマンドでは、CoPP サービス ポリシーを制御プレーンに直接付加できます。

トラフィック分類基準の定義方法については、「トラフィック分類の定義」（P.40-40）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にします。
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]`	次のように、トラフィックと照合する ACL を定義します。 • **permit** では、パケットが名前付き IP アクセス リストで合格する条件を設定します。 • **deny** では、パケットが名前付き IP アクセス リストで不合格にな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または重要でないトラフィックを識別する 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。クラスに関連するトラフィックを識別するには、**match** ステートメントを使用します。

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。クラスをサービス ポリシー マップに関連付けるには、**class** *traffic-class-name* コマンドを使用します。サービス ポリシー マップにアクションを関連付けるには、**police** ステートメントを使用します。

ステップ 5	`Router(config)# control-plane` `Router(config-cp)#`	制御プレーン コンフィギュレーション モードに入ります。
ステップ 6	`Router(config-cp)# service-policy input service-policy-name`	QoS サービス ポリシーを制御プレーンに適用します。

パケット分類基準を定義するときは、次の注意事項および制約事項に従ってください。

- 後続クラスで設定されるフィルタリングとポリシングに一致しないようにするには、クラスごとにポリシングを設定します。CoPP は、police コマンドを含まないクラスでフィルタリングを適用しません。police コマンドを含まないクラスはどのトラフィックとも一致しません。
- 分類に使用される ACL は QoS ACL です。サポートされる QoS ACL は、IP 標準、拡張、名前付きです。
- サポートされる一致タイプは以下だけです。
  - **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 ベースの照合はソフトウェアだけで実行されます。
- 単一クラス マップで入力できる **match** コマンドは 1 つだけです。

サービス ポリシーを定義する場合、サポートされているアクションは **police** ポリシー マップ アクションだけです。

制御プレーンにサービス ポリシーを適用する場合は、**input** 方向だけがサポートされます。

CoPP のモニタ

サイト固有ポリシーを開発して制御プレーン ポリシーの統計をモニタし、CoPP をトラブルシューティングするには、**show policy-map control-plane** コマンドを入力できます。このコマンドでは、レート情報、およびハードウェアとソフトウェアの両方で設定されたポリシーに適合するバイト数（およびパケット数）と適合しないバイト数（およびパケット数）など、実際に適用されたポリシーに関するダイナミックな情報が表示されます。

show policy-map control-plane コマンドの出力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#
```

ポリシーによって廃棄されたり転送されたりしたバイトのハードウェア カウンタを表示するには、**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 リスト情報を表示するには、show 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
```

CoPP ポリシーのカスタマイズ

ルータ上で適用される CoPP ポリシーは、RP にパントされるルータ トラフィック プロファイルに適合するようにカスタマイズする必要があります。

カスタマイズによって、次のことが確実になります。

- 正しい種類のトラフィックが、優先順位の低い他のトラフィックや、非優先トラフィックよりも優先されます。
- ネットワークが安定します。
- コントロール プレーン保護が実現されます。
- 分類に失敗したトラフィックの存在が確認されます。

ポリシーをカスタマイズするには、Mini Protocol Analyzer ツールを使用して、RP にパントされるトラフィックを分析します。このツールは、RP にパントされるトラフィックをキャプチャし、パケットがパントされるレートをチェックするのに役立ちます。取得したデータを使用して、クラスを識別し、CoPP の設定に必要なレートをポリシングできます。Mini Protocol Analyzer ツールの詳細については、「Mini Protocol Analyzer の使用」を参照してください。

CoPP ポリシーの作成

CoPP ポリシーを作成する前に、必要なトラフィック量を特定して、複数のクラスに分類する必要があります。相対的な重要度に基づいてトラフィックを分類する方法が推奨されています。

CoPP ポリサーの作成時に使用されるサンプル分類基準を次に示します。

- ポリサーは class-default で使用しないでください。可能性のあるすべてのトラフィックを class-default 以外の特定のクラスに分類する必要があります。
- catch-all トラフィックには、**match ipv4 any class** コマンドまたは **match ipv6 any class** コマンドを使用します。class-default を同じ目的で使用することができますが、次の例で示すように、class-default アクションを使用してトラフィックを最小限に抑えることが推奨されます。

```
Policy-map CoPP
   Class CLASS1
      Police <>
   Class CLASS2
     Police <>
Class MATCH-IPv4-ANY Match all IPv4 traffic which doesn't fall in any of the above
mentioned classes
     Police <>
   Class MATCH-IPV6-ANY Match all IPV6 traffic which doesn't fall in any of the above
mentioned classes
     Police <>
```

「CoPP ポリシーの例」（P.40-40）では、トラフィックが 5 つのクラスに分類されます。実際のクラス数は、5 とは限らないため、ローカルな要件とセキュリティ ポリシーに基づいて選択する必要があります。これらのトラフィック クラスは、CPU またはコントロール プレーンに関して定義されます。

5 つのクラスは次のとおりです。

- Critical
  - ルータとネットワークの運用に不可欠なトラフィック。
  - 例：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）などのルーティング プロトコル
  - サイトによっては、必要に応じて、運用に不可欠なトラフィック以外のトラフィックを Critical として分類する場合があります。
- Important
  - 日常業務に必要な頻繁に使用されるトラフィック
  - 例：リモート ネットワーク アクセスおよび管理（telnet、Secure Shell（SSH; セキュア シェル）、ネットワーク タイム プロトコル（NTP）、および簡易ネットワーク管理プロトコル（SNMP））に使用されるトラフィック
- Normal
  - 機能的だが、ネットワーク運用に不可欠ではないトラフィック
  - ルータに悪影響を及ぼさない範囲で許可しなければならないため、コントロール プレーン保護スキームの設計時に特に解決が難しい通常のトラフィック。CoPP を使用している場合は、このトラフィックが許可されますが、低レートに制限されます。
  - 例：ICMP エコー要求
- Undesirable
  - ドロップして、ルータ プロセッサへのアクセスを拒否すべき、明らかに不良な、または悪意のあるトラフィック
  - 特に、ルータ宛ての既知のトラフィックを必ず拒否して、デフォルト カテゴリに分類しない場合に便利です。トラフィックを明示的に拒否することによって、エンドユーザは show コマンドを使用してそのトラフィックに関する大まかな統計情報を収集できるため、拒否対象のトラフィックのレートに対して何らかの見識を示すことができます。
- Layer 2 class
  - アドレス解決プロトコル（ARP）に使用されるトラフィック。過剰な ARP パケットが RP CPU リソースを独占することによって、その他の重要なプロセス用のリソースが不足する可能性があります。CoPP を使用すれば、ARP パケットをレート制限してこの状況を回避することができます。現在、一致プロトコル分類基準を使用して明確に分類されるレイヤ 2 プロトコルは ARP だけです。
- Match-Any class
  - その他のすべての IPv4/IPv6 トラフィック（上述したどのクラスにも属さない）と一致し、必要に応じて、それらをポリシングします。特に、class-default でポリサーが必要とされないように設計されています。
- Default
  - ルータ プロセッサ宛てのその他の未確認トラフィック
  - デフォルト分類を使用すれば、コントロール プレーン宛ての未確認トラフィックのレートを特定するための統計情報のモニタリングが容易になります。確認されたトラフィックは、分析を通してさらに細かく分類したり、必要に応じて、他の CoPP ポリシー エントリで更新したりすることができます。
  - リリース 12.2(18)SXD1 内の Sup720 は、ハードウェアで MQC **class-default** をサポートしていません。このサポートは、リリース 12.2(18)SXE1 ソフトウェア リリースで追加されました。下の例で "class-default" が通常の class-map に置き換えられていることからもわかるように、これは大きな制限事項ではありません。

- レイヤ 2 キープアライブ、CLNS、その他の非 IP パケットなどのトラフィック タイプは CoPP（class-default 内のみ）で認識されます。これらのトラフィック タイプは MQC for CoPP では分類できないため、必ず、CoPP class-default クラスに分類されます。CoPP が設定されている場合は、レイヤ 2 キープアライブやその他の不可欠なコントロール プレーン トラフィックがドロップされないように、class-default をレート制限しないことが重要です。必ず、class-default の直前にある CoPP policy-map 内で "catch all" IP クラスを設定するのはこのためです。

上記分類スキームでは、よく使用されるトラフィックが一連の ACL を使用して識別されます。

- Class CoPP-CRITICAL：CL 120：critical トラフィック
- Class CoPP-IMPORTANT：ACL 121：important トラフィック
- Class CoPP-NORMAL：ACL 122：normal トラフィック
- Class CoPP-UNWANTED ACL 123：不要なトラフィック（スラマー ワーム トラフィックなど）を明示的に拒否する
- Class CoPP-ARP：ARP プロトコルと一致する
- Class CoPP-Match-all ACL 124：その他のトラフィック

ACL はポリシーの定義に使用されるトラフィックのクラスを編成します。

サンプル CoPP ポリシー

これは、上記 ACL を使用して作成された CoPP ポリシーの例です。

```
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 120 remark *** LDP ***
access-list 120 permit udp 172.0.0.0 0.0.255.255 eq 646 any
access-list 120 permit udp 172.0.0.0 0.0.255.255 any eq 646
access-list 120 permit tcp 172.0.0.0 0.0.255.255 eq 646 any
access-list 120 permit tcp 172.0.0.0 0.0.255.255 any eq 646
access-list 120 remark *** BGP ***
access-list 120 permit tcp 172.0.0.0 0.0.255.255 eq bgp any
access-list 120 permit tcp 172.0.0.0 0.0.255.255 any eq bgp
access-list 120 remark *** PIM ***
access-list 120 permit pim 172.0.0.0 0.0.255.255 any
access-list 120 permit pim any 172.0.0.0 0.0.255.255
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 121 remark *** Telnet ***
access-list 121 permit tcp 172.0.0.0 0.0.255.255 172.0.0.0 0.0.255.255 eq telnet
access-list 121 remark *** SSH ***
access-list 121 permit tcp 172.0.0.0 0.0.255.255 152.0.0.0 0.255.255.255 eq 22
access-list 121 remark *** SNMP ***
access-list 121 permit udp 172.0.0.0 0.0.255.255  152.0.0.0 0.255.255.255 eq snmp
access-list 121 remark *** NTP ***
access-list 121 permit udp 172.0.0.0 0.0.255.255  host 192.168.70.10 eq ntp
access-list 121 permit udp 172.0.0.0 0.0.255.255  host 192.168.70.30 eq ntp
access-list 121 remark *** Syslog ***
access-list 121 permit udp 172.0.0.0 0.0.255.255  152.0.0.0 0.255.255.255 eq syslog
access-list 121 remark *** TACAS+ ***
access-list 121 permit tcp 172.0.0.0 0.0.255.255  152.0.0.0 0.255.255.255 eq tacacs
access-list 122 remark CoPP normal traffic
access-list 122 permit icmp any any ttl-exceeded
access-list 122 permit icmp any any port-unreachable

access-list 122 permit icmp any any echo-reply
access-list 122 permit icmp any any echo

access-list 123 remark *** ACL for CoPP-UNDESIRABLE
access-list 123 permit icmp any any fragments
```

```
access-list 123 permit udp any any fragments
access-list 123 permit tcp any any fragments
access-list 123 permit ip any any fragments
access-list 124 remark *** ACL for CoPP-Match-all
access-list 124 permit ip any any
access-list 124 permit ipv6 any any

class-map match-all CoPP-CRITICAL
match access-group 120
class-map match-all CoPP-IMPORTANT
match access-group 121
class-map match-all CoPP-NORMAL
match access-group 122
class-map match-all CoPP-ARP
match protocol ARP
class-map match-all CoPP-UNWANTED
match access-group 123
class-map match-all CoPP-Match-all
match access-group 124
```

パント対象トラフィックのレート制限が推奨されていますが、特に、critical トラフィックの場合は、必要なトラフィック レートが十分把握されていることを確認してください。レートが低すぎると、必要なトラフィックが廃棄またはドロップされる可能性があり、レートが高すぎると、ルータ プロセッサを非 critical パケットの処理に集中させることになりかねません。これらのレートは、サイト固有であり、ローカルなトポロジとルーティング テーブルのサイズに大きく影響します。

ポリシングするレートは、決定された重要度とサイト固有のレート値の両方に依存します。たとえば、「通常の」SNMP レートは環境によって異なります。上記分類スキームを使用すれば、critical トラフィックは無条件で許可されますが、important、normal、および default トラフィックは適切なレート制限を通して許可されます。ただし、この実装ではネットワーク上で undesirable トラフィックが即座にドロップされます。

表 39-3 では、この例を拡張し、サンプル ポリシーを要約しています。表内のレートは説明用として使用されていることに注意してください。環境によって基準値が異なります。たとえば、大規模なサービス プロバイダー トポロジでは、標準的な企業ネットワークに比べて、critical トラフィックのレートを高くする必要があります（BGP ルーティング テーブルが大きいため）。

critical トラフィック クラスを定義する目的は、レートを制限することはでなく、このトラフィックに critical というタグを付け、ルータ プロセッサへの無条件アクセスを許可することです。ポリシーが精緻化されるのに従って、critical トラフィックにより適切なレートを使用する必要があります。また、show コマンドでトラフィック レートの異常な上昇を検出することができます。

表 40-3　サンプル CoPP ポリシー

トラフィック クラス	速度（bps）	Conform アクション	Exceed アクション
Critical	N/A	送信	送信
Important	125,000	送信	ドロップ
Normal	64,000	送信	ドロップ
Undesirable	32,000	ドロップ	ドロップ
ARP	64,000	送信	ドロップ
MATCH-ALL	96,000	送信	ドロップ
Class-default	-	-	-

CoPP ポリシーの例

```
policy-map CoPP
class CoPP-CRITICAL
police 1000000 31250 31250 conform-action transmit exceed-action transmit violate-action
transmit
class CoPP-IMPORTANT
police 128000 4000 4000 conform-action transmit exceed-action drop violate-action drop
class CoPP-NORMAL
police 64000 2000 2000 conform-action transmit exceed-action drop violate-action drop
class CoPP-UNDESIRABLE
police 32000 1500 1500 conform-action transmit exceed-action drop violate-action drop
class CoPP-ARP
police 64000 1500 1500 conform-action transmit exceed-action drop violate-action drop
class CoPP-Match-all
police 96000 3000 3000 conform-action transmit exceed-action drop violate-action drop
class class-default
```

トラフィック分類の定義

ここでは、CoPP トラフィックの分類方法について説明します。

- 「トラフィック分類の概要」（P.40-40）
- 「トラフィック分類のガイドライン」（P.40-41）
- 「CoPP トラフィック分類の基本 ACL 例」（P.40-42）

トラフィック分類の概要

任意の数のクラスを定義できますが、一般的にトラフィックは、相対的な重要性に基づいたクラスにグループ化されます。グループ化の例を以下に示します。

- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）: BGP キープアライブおよびルーティング アップデートなどの BGP ルーティング プロトコルのネイバー関係の維持で重要となるトラフィック。BGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために、またはサービス プロバイダーにとって重要です。BGP を実行しないサイトで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）: Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などの IGP ルーティング プロトコルの維持で重要になるトラフィック。IGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために重要となります。
- 管理：日常業務で必要な、頻繁に使用される必須トラフィック。たとえば、Telnet、Secure Shell（SSH; セキュア シェル）、ネットワーク タイム プロトコル（NTP）、簡易ネットワーク管理プロトコル（SNMP）、Terminal Access Controller Access Control System（TACACS）、ハイパーテキスト転送プロトコル（HTTP）、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、ファイル転送プロトコル（FTP）など、リモート ネットワーク アクセス、および Cisco IOS イメージのアップグレートと管理に使用されるトラフィック。
- レポート：レポートする目的でネットワーク パフォーマンス統計を生成するために使用されるトラフィック。たとえば、さまざまな QoS データ クラス内の応答時間でレポートするために、Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）を使用して、さまざまな DSCP 設定で ICMP を生成することなど。

- モニタ：ルータのモニタに使用されるトラフィック。トラフィックを許可する必要がありますが、ルータにリスクがかからないようにする必要があります。CoPP を使用すると、このトラフィックを許可できますが、低レートに制限されます。たとえば、ICMP エコー要求（ping）および traceroute など。
- クリティカル アプリケーション：特定カスタマーの環境に固有で重要なクリティカル 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お客様もいれば、IPSec または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用するお客様もいます。たとえば、GRE、ホットスタンバイ ルータ プロトコル（HSRP）、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、Session Initiation Protocol（SIP）、Data Link Switching（DLSw; データ リンク スイッチング）、Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）、Multicast Source Discovery Protocol（MSDP）、インターネット グループ管理プロトコル（IGMP）、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPSec など。
- レイヤ 2 プロトコル：アドレス解決プロトコル（ARP）に使用されるトラフィック。過剰な ARP パケットが MSFC リソースを独占し、その他の重要なプロセスで MSFC リソースが足りなくなることがあります。CoPP を使用すると、ARP パケットをレート制限してこの状況を防止できます。現在、一致プロトコル分類基準を使用して明確に分類できるレイヤ 2 プロトコルは、ARP だけです。
- 不要：無条件でドロップして MSFC へのアクセスを拒否する必要がある不良トラフィックまたは悪質トラフィックを明示的に識別します。ルータを宛先とした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 カテゴリに配置しない場合は、この不要分類が特に役立ちます。トラフィックを明示的に拒否する場合は、**show** コマンドを入力して拒否トラフィックに関する概算統計を収集してレートを見積もることができます。
- デフォルト：識別されなかった、MSFC を宛先とするすべてのトラフィック。MQC はデフォルト クラスを提供するので、ユーザは、その他のユーザ定義クラスで明示的に識別されないトラフィックに適用する処置を指定できます。このトラフィックは、MSFC にアクセスするレートが大幅に制限されます。デフォルト分類を適切に使用すると、統計をモニタし、これを使用しない場合は識別されないコントロール プレーンを宛先とするトラフィックのレートを判断できます。このトラフィックが識別されたあとは、さらに分析を実行して分類し、必要な場合は、その他の CoPP ポリシー エントリを更新してこのトラフィックに対応できます。

トラフィックの分類が完了したら、ポリシーの定義に使用される、トラフィックのクラスを ACL が構築します。CoPP 分類の基本的な ACL の例については、「CoPP トラフィック分類の基本 ACL 例」（P.40-42）を参照してください。

トラフィック分類のガイドライン

トラフィック分類を定義するときは、次のガイドラインおよび制約事項に従ってください。

- 実際の CoPP ポリシーを開発する前に、必要なトラフィックを識別してさまざまなクラスに分類する必要があります。トラフィックは、相対的な重要性に基づく 9 個のクラスにグループ化されます。実際に必要となるクラスの数は異なることがあり、ローカルの要件とセキュリティ ポリシーに基づいて選択する必要があります。
- 双方向に一致するポリシーを定義する必要はありません。ポリシーは入力だけで適用されるので、単方向（ネットワークから MSFC へ）でトラフィックを識別する必要しかありません。

CoPP トラフィック分類の基本 ACL 例

ここでは、CoPP 分類の基本的な ACL 例を示します。この例では、一般的に必要なトラフィックが、次の ACL で識別されます。

- ACL 120：クリティカル トラフィック
- ACL 121：重要トラフィック
- ACL 122：通常トラフィック
- 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

次に、クリティカル トラフィック用に ACL 120 を定義する例を示します。

```
Router(config)# access-list 120 remark CoPP ACL for critical traffic
```

次に、既知のピアからこのルータの BGP TCP ポートへの BGP を許可する例を示します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
```

次に、ピアの BGP ポートからこのルータへの BGP を許可する例を示します。

```
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
```

次に、重要クラス用に ACL 121 を定義する例を示します。

```
Router(config)# access-list 121 remark CoPP Important traffic
```

次に、TACACS ホストからのリターン トラフィックを許可する例を示します。

```
Router(config)# access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
```

次に、サブネットからルータへの SSH アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
```

次に、特定サブネットのホストからルータへの Telnet の完全アクセスを許可し、残りのサブネットをポリシングする例を示します。

```
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
```

次に、NMS ホストからルータへの SNMP アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
```

次に、ルータが既知のクロック ソースから NTP パケットを受信できるようにする例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

次に、通常トラフィック クラス用に ACL 122 を定義する例を示します。

```
Router(config)# access-list 122 remark CoPP normal traffic
```

次に、ルータからの traceroute トラフィックを許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any ttl-exceeded
Router(config)# access-list 122 permit icmp any any port-unreachable
```

次に、ping を発信したルータに応答の受信を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo-reply
```

次に、ルータへの ping を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo
```

次に、不要クラス用に ACL 123 を定義する例を示します。

```
Router(config)# access-list 123 remark explicitly defined "undesirable" traffic
```

（注）　次の例において、ACL 123 は分類とモニタを目的とした許可エントリであり、トラフィックは CoPP ポリシーの結果としてドロップされます。

次に、UDP 1434 を宛先とするすべてのトラフィックをポリシング用に許可する例を示します。

```
Router(config)# access-list 123 permit udp any any eq 1434
```

次に、その他すべてのトラフィック用に ACL 124 を定義する例を示します。

```
Router(config)# access-list 124 remark rest of the IP traffic for CoPP
Router(config)# access-list 124 permit ip any any
```

スティッキ ARP の設定

スティッキ ARP では、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して、MAC アドレスのスプーフィングを防止します。ルータは ARP エントリを、エンド デバイスまたはその他のルータにトラフィックを転送するために維持します。ARP エントリは、一般的に定期的に更新されるか、ARP ブロードキャストを受信したときに修正されます。攻撃中に ARP ブロードキャストは、スプーフィングされた MAC アドレス（正当な IP アドレスを含む）を使用して送信されるので、ルータは、スプーフィングされた MAC アドレスを含む正当な IP アドレスを学習し、その MAC アドレスにトラフィックを転送し始めます。スティッキ ARP をイネーブルにすると、ルータは ARP エントリを学習し、ARP ブロードキャストで受信した修正を受け入れません。スティッキ ARP 設定を上書きしようとすると、エラー メッセージが表示されます。システム エラー メッセージの詳細については、次の URL の『*Cisco 7600 Series Router Cisco IOS System Message Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sr/msggd/index.htm

（注）　スティッキ ARP は設定可能です。

レイヤ 3 インターフェイスでスティッキ 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*	スティッキ 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`	スティッキ ARP をイネーブルにします。
	`Router(config-if)# no ip sticky-arp ignore`	以前設定したスティッキ ARP コマンドを削除します。
ステップ 3	`Router(config-if)# ip sticky-arp ignore`	スティッキ 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 でスティッキ 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 41

DHCP スヌーピングの設定

この章では、Cisco 7600 シリーズ ルータに 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、PFC3 と Release 12.2(18)SXE およびそれ以降のリリースが必要です。PFC2 では、DHCP スヌーピングはサポートされません。

この章で説明する主な内容は、次のとおりです。

- 「DHCP スヌーピングの概要」（P.41-1）
- 「DHCP スヌーピングのデフォルト設定」（P.41-7）
- 「DHCP スヌーピング設定時の制約事項および注意事項」（P.41-8）
- 「DHCP スヌーピングの設定」（P.41-9）

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.41-2）
- 「信頼できるソースおよび信頼できないソース」（P.41-2）
- 「DHCP スヌーピング バインディング データベース」（P.41-3）
- 「パケット検証」（P.41-3）
- 「DHCP スヌーピングの Option 82 データ挿入」（P.41-4）
- 「DHCP スヌーピング データベース エージェントの概要」（P.41-6）

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済み DHCP サーバとの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、次のアクティビティが実行されます。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外する。
- 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、管理する。このデータベースには、リースされた IP アドレスを持つ信頼できないホストに関する情報が保存されています。
- 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後続リクエストを検証する。

ダイナミック ARP インスペクション（DAI）など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 データベースに保存されている情報が使用されます。

DHCP スヌーピングは、VLAN ベースごとにイネーブルになっています。デフォルトでは、すべての VLAN でこの機能は非アクティブです。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、MSFC 上のソフトウェアで実行されます。したがって、イネーブルな VLAN へのすべての DHCP メッセージは、PFC で止められ、処理のために MSFC に送信されます。

信頼できるソースおよび信頼できないソース

DHCP スヌーピング機能では、トラフィックの送信元が信頼できるかどうかを判別します。信頼できない送信元の場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。このような攻撃を防ぐために、DHCP スヌーピング機能では、メッセージをフィルタ処理し、信頼できないソース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、管理担当者の管理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、ネットワークのスイッチ、ルータ、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。ホスト ポートは、一般的に、信頼できないソースとして扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できないソースです（カスタマー 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 シリーズのスイッチでは、その接続インターフェイスの信頼状態を設定することによって、ソースが信頼できることを示します。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態です。DHCP サーバ インターフェイスは、信頼できるインターフェイスとして設定する必要があります。ユーザのネットワーク内でデバイス（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（注） DHCP スヌーピングが正しく機能するには、すべての DHCP サーバが、信頼できるインターフェイスを介してルータに接続されている必要があります。

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 スヌーピング機能では、DHCP メッセージを傍受して抽出した情報を使用して、データベースを動的に構築して保持します。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、リースされた IP アドレスを持つ信頼できない各ホストのエントリが保存されています。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するホストに関するエントリは保存されません。

DHCP スヌーピング機能では、スイッチで特定の DHCP メッセージを受信すると、データベースが更新されます。たとえば、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、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切れると、またはホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベース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 データベース内の各エントリには、ホストの MAC アドレス、リースされた IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

パケット検証

ルータでは、DHCP スヌーピングがイネーブルな VLAN の信頼できないインターフェイス上で受信した DHCP パケットが検証されます。次の条件が発生（この場合パケットは破棄される）しない限り、スイッチでは、DHCP パケットが転送されます。

- ルータで、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、（DHCPOFFER、DHCPACK、DHCPNAK、DHCPLEASEQUERY などの）パケットを受信した場合。
- ルータ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の場合だけ、実行されます。
- ルータが、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 メッセージまたは 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。
- ルータが、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。

リリース 12.2(18)SXF1 よりも前のリリースでは、ルータで、信頼できないポートで Option 82 情報を保持する DHCP パケットは破棄されます。リリース 12.2(18)SXF1 およびそれ以降のリリースで、信頼できない収集ルータ ポートに接続されている信頼エッジ ルータをサポートする場合、信頼できないポート機能で DHCP Option 82 をイネーブルにできます。これによって、信頼できない集約ルータ ポートでは、Option 82 情報が保存されている DHCP パケットを受信します。信頼ポートとして集約スイッチに接続されているエッジ ルータで、ポートを設定します。

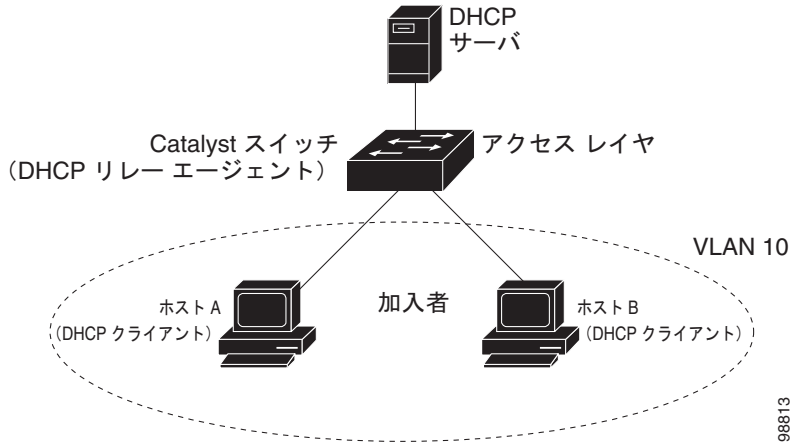
（注） 信頼できないポート機能で DHCP Option 82 がイネーブルである場合は、集約ルータでダイナミック ARP インスペクションを使用して、信頼できない入力インターフェイスを保護します。

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。ルータで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者デバイスは MAC アドレスだけでなく、このデバイスをネットワークに接続するルータ ポートによっても識別されます。加入者 LAN 上の複数のホストをアクセス ルータ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 41-1 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 レイヤのルータ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。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 41-1　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



ルータに対して DHCP スヌーピング情報の Option 82 をイネーブルにすると、以下のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- ルータはこの 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、ルータの 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、ルータは DHCP パケット内にこの IP アドレスを追加します。
- ルータは、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うことができます。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。
- 要求がルータによってサーバにリレーされている場合は、DHCP サーバは応答をルータ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。ルータはリモート 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。ルータは 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ルータ ポートにパケットを転送します。

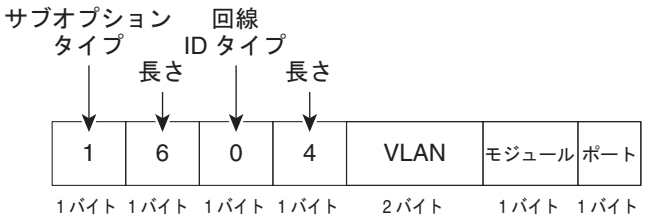
上記の一連のイベントが発生する間、図 41-2 に示す次のフィールドの値は変更されません。

- 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

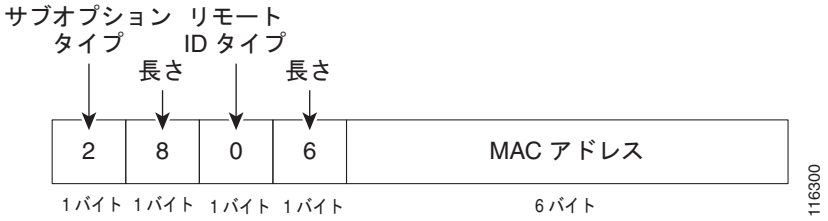
図 41-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。ルータがこれらのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化されている場合、および **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力された場合です。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

図 41-2　　サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット



DHCP スヌーピング 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。ルータ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。ルータ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 行めの <initial-checksum> エントリは、最新の書き込みに関連するエントリを以前の書き込みに関連するエントリと区別するのに役立ちます。

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保持します。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ています。

起動時に、算出されたチェックサムが格納されたチェックサムに合致すると、ルータはファイルからエントリを読み取り、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。算出されたチェックサムが格納されたチェックサムに合致しない場合、ファイルから読み取られたエントリが無視され、失敗したエントリに続くすべてのエントリも無視されます。また、ルータは、リース期間が期限切れになったファイルのすべてのエントリも無視します。（リース時間が期限切れの時刻を示している場合があるため、この可能性があります）。エントリ内で参照されるインターフェイスが、システム上に存在しなくなった場合、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、ファイル内のエントリが無視されます。

ルータ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、ルータは変更されたエントリのセットをスヌーピング データベースから抽出し、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 41-1 に、各 DHCP スヌーピング オプションのデフォルトの設定値をすべて示します。

表 41-1　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の DHCP Option 82 機能	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	untrusted
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.41-8）
- 「DHCP スヌーピング設定時の注意事項」（P.41-8）
- 「DHCP スヌーピングの最小設定」（P.41-9）

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、次の制約事項に注意してください。

- PFC2 では、DHCP スヌーピングはサポートされません。
- リリース 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースで、最大 512 のバインディングが保存されます。512 を超える DHCP バインディングを追加する場合、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。
- リリース 12.2(18)SXF5 とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 8,000 のバインディングが保存されます。
- リリース 12.2(18)SRA とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 64,000 のバインディングが保存されます。

DHCP スヌーピング設定時の注意事項

DHCP の設定時には、次の注意事項に従ってください。

- DHCP スヌーピングは、この機能を少なくとも 1 つの VLAN 上でオンにし、ルータ上でグローバルにオンにするまで、アクティブになりません。サービス DHCP がイネーブルであることを確認してください（サービス DHCP はデフォルトでイネーブルに設定されています）。
- ルータ上で DHCP スヌーピングをグローバルにイネーブル化する前に、DHCP サーバおよび DHCP リレー エージェントとして機能するデバイスを事前に設定およびイネーブル化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 の『*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、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 だけで有効になります。
- 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なっているすべての VLAN（プライマリおよびセカンダリの両方）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限の設定手順は、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 の『*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、すべての VLAN で DHCP スヌーピングは非アクティブです。「VLAN 上での DHCP スヌーピングのイネーブル化」（P.41-12）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介し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デフォルトの信頼状態は、信頼できない状態です。「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.41-14）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。

   この手順では、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.41-15）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化します。

   この機能は、この手順を完了するまでアクティブになりません。「DHCP スヌーピングのグローバルなイネーブル化」（P.41-10）を参照してください。

DHCP リレーのスイッチを設定する場合、次の追加手順が必要です。

1. DHCP リレー エージェント IP アドレスを定義し、設定します。

   DHCP サーバが、DHCP クライアントと異なるサブネットにある場合、クライアント側の VLAN のヘルパー アドレス フィールドで、サーバ IP アドレスを設定します。

2. 信頼できないポートで DHCP Option 82 を設定します。

   「信頼できないポートの DHCP Option 82 機能のイネーブル化」（P.41-11）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」（P.41-10）
- 「DHCP Option 82 データ挿入のイネーブル化」（P.41-10）
- 「信頼できないポートの DHCP Option 82 機能のイネーブル化」（P.41-11）

- 「DHCP スヌーピングの MAC アドレス検証のイネーブル化」（P.41-12）
- 「VLAN 上での DHCP スヌーピングのイネーブル化」（P.41-12）
- 「レイヤ 2 LAN インターフェイスでの DHCP 信頼状態の設定」（P.41-14）
- 「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」（P.41-14）
- 「DHCP スヌーピング データベース エージェントの設定」（P.41-15）
- 「データベース エージェントの設定例」（P.41-16）
- 「バインディング テーブルの表示」（P.41-19）

DHCP スヌーピングのグローバルなイネーブル化

（注）　このコマンドは、最後の設定手順として設定してください（または、予定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てください）。これは、DHCP スヌーピングをグローバルにイネーブル化すると、ポートを設定しない限り、ルータが DHCP 要求をドロップするためです。

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`	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)#
```

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`	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の DHCP Option 82 機能のイネーブル化

（注）　信頼できないポートの DHCP Option 82 機能をイネーブルにした場合、ルータは信頼できないポートで受信された Option 82 情報を含む DHCP パケットをドロップしません。信頼できないデバイスが接続されている集約ルータでは、**ip dhcp snooping information option allowed-untrusted** コマンドは入力しないでください。

リリース 12.2(18)SXF1 およびそれ以降のリリースで、Option 82 情報が含まれている DHCP パケットを受け付けるよう、信頼できないポートをイネーブル化するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping information option allow-untrusted`	（任意）Option 82 情報が含まれている DHCP の着信パケットを受け付けるよう、信頼できないポートをイネーブル化します。 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の DHCP Option 82 機能のディセーブル化
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の DHCP Option 82 機能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 パケット内のクライアント ハードウェア アドレスが、送信元 MAC アドレスと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ているレイヤ 2 フィールドであり、クライアント ハードウェア アドレスは、DHCP パケットのレイヤ 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 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、すべての VLAN で DHCP スヌーピング機能は非アクティブです。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。

VLAN でイネーブル化されている場合、DHCP スヌーピング機能では、MFC3 の VACL テーブルで 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 では、この VLAN 上のすべての DHCP メッセージが止められ、MSFC に送信されます。DHCP スヌーピング機能は、MSFC ソフトウェアで実行されます。

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 で設定するには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲を設定するには、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（-）でつなげて入力します。
- 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、VLAN 10 ～ 12 で DHCP スヌーピング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 dhcp snooping vlan 10-12
```

次に、VLAN 10 ～ 12 で DHCP スヌーピング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 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 インターフェイスだけを選択してください。
ステップ 2	`Router(config-if)# ip dhcp snooping trust` `Router(config-if)# no ip dhcp snooping trust`	インターフェイスを trusted として設定します。 デフォルトの（untrusted）状態に戻します。
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 インターフェイスだけ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。

	コマンド	目的
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、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 スヌーピングがイネーブルになっている 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しなければならない場合があります。
- 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 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、次の作業の 1 つまたは複数を実行します。

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、次の点に注意してください。

- リリース 12.2(18)SXF5 よりも前のリリースでは、DHCP スヌーピング データベースで、最大 512 のバインディングが保存されます。512 を超える DHCP バインディングを追加する場合、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。
- リリース 12.2(18)SXF5 とそれ以降のリリースでは、DHCP スヌーピング データベースで、少なくとも 8,000 のバインディングが保存されます。
- ルータのストレージ デバイスの記憶域が消費されることを避けるため、ファイルは TFTP 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、FTP など）では、ルータ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」（P.41-16）
- 「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」（P.41-17）
- 「例 3：DHCP スヌーピング データベースへの情報の追加」（P.41-19）

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。

この他の統計情報として出力結果で示されるスタートアップ時の失敗は、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を表します。

（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、ルータ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。Invalid interfaces カウンタは読み取りの際に、エントリで指定されたインターフェイスがシステムに存在しない場合、またはインターフェイスが存在する場合は、それがルータ、または DHCP スヌーピングで信頼されたインターフェイスのいずれかであるために無視されたバインディング数を示します。Unsupported vlans は、エントリの示す VLAN がシステム上でサポートされないために無視されたエントリの数を示します。Parse failures カウンタは、ルータがファイルのエントリの意味を解釈できなかった場合に無視されたエントリ数を示します。

ルータは、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。これらのカウンタは、「Last ignored bindings counters」として表示されます。もう 1 つは「total ignored bindings counters」であり、ルータの起動時からの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** コマンドによってクリアされます。総数カウンタは、最後にクリアが行われてから無視されたバインディング数を示す場合があります。

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*	ルータに、指定の URL からファイルを読み取るように指示します。

	コマンド	目的
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正常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

個々のルータが持つ 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。相互接続する各ルータは、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、ルータの 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 41-2 に、**show ip dhcp snooping binding** コマンド出力のフィールドの説明を示します。

表 41-2　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

表 41-2　show ip dhcp snooping binding コマンドの出力結果 （続き）

フィールド	説明
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、またはスタティックに設定されたバインディング
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 42

ダイナミック ARP インスペクションの設定

この章では、Cisco 7600 シリーズ ルータにダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「DAI の概要」（P.42-1）
- 「DAI のデフォルト設定」（P.42-5）
- 「DAI 設定時の注意事項および制約事項」（P.42-6）
- 「DAI の設定」（P.42-7）
- 「DAI の設定例」（P.42-17）

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」（P.42-1）
- 「ARP スプーフィング攻撃の概要」（P.42-2）
- 「DAI および ARP スプーフィング攻撃の概要」（P.42-2）

ARP の概要

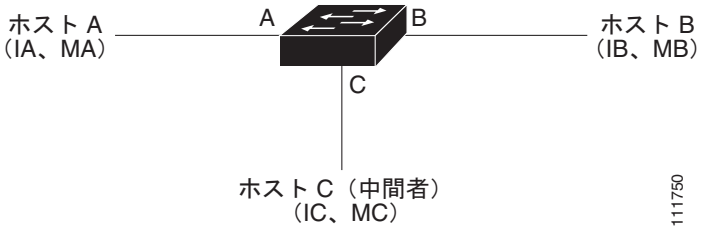
ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとする場合、ホスト B の ARP キャッシュにホスト A の MAC アドレスが存在しないとします。ホスト B はホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスで応答します。

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ホストでも応答できる ARP の機能性を利用して行う攻撃です。攻撃が開始されると、攻撃を受けたデバイス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することができます。図 42-1 は、ARP キャッシュ ポイズニングの例を示します。

図 42-1　　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 を介してルータ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。ルータとホスト 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 キャッシュ内に読み込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答すると、ルータとホスト 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 キャッシュ内に読み込みます。

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、ルータ、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ーです。

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、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リレーされるようになります。ルータ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 ARP キャッシュを更新するか、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 IP アドレスと MAC アドレスとの有効な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、Dynamic Host Configuration Protocol（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 およびルータ上で 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、ルータ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、ルータは有効性を確認できたパケットだけを転送します。

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、ユーザ設定の ARP アクセス コントロール リスト（ACL）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.42-9）を参照）。ルータは、ドロップされたパケットを記録します（「ドロップされたパケットのロギング」（P.42-5）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、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（「追加検証のイネーブル化」（P.42-12）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

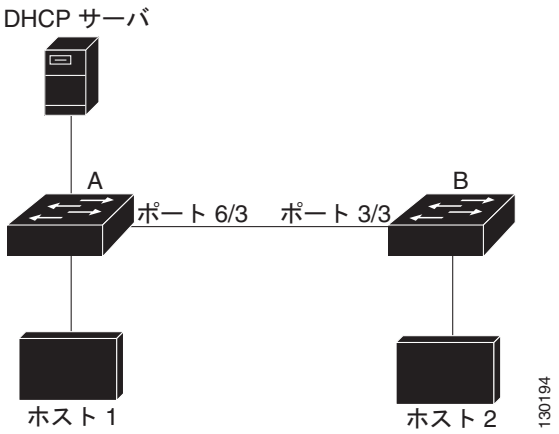
DAI は、ルータの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、ホスト ポートに接続されているすべてのルータ ポートを信頼できないポートとして、ルータに接続されているすべてのルータ ポートは信頼できるポートとして設定します。この構成では、特定ルータ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、慎重に使用してください。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 42-2 では、ルータ A と ルータ B の両方が、ホスト 1 とホスト 2 を収容する 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 がルータ 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、ルータ A だけがホスト 1 の IP アドレスと MAC アドレスをバインドします。したがって、ルータ A とルータ 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 パケットはルータ 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 42-2　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。ルータ A が DAI を実行していなければ、ホスト 1 はルータ B（ルータ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、ルータ B が DAI を実行している場合でも発生する場合があります。

DAI は、DAI を実行するルータに接続された、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します。ただし、ネットワークのその他の場所にあるホストが、DAI を実行するルータ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 内の一部のルータが DAI を実行し、他のルータは DAI を実行していない状況では、これらのルータ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ルータからのパケットのバインディングを検証するには、DAI を実行するルータ上で 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 を実行するルータを DAI を実行しないルータから切り離します。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.42-21）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 内のすべてのルータで、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

ルータは、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、DoS 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 packets per second（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、ルータはこのポートを errdisable ステートにします。ユーザが介入するまで、ポートは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時間が経過すると、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.42-10）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、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

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 の方が優先されます。**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設定している場合に限り、ACL はルータに適用されます。ルータはまず、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読み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、ルータはこのパケットを拒否します。

ドロップされたパケットのロギング

ルータ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、ルータ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含まれます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、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なエントリ数を設定します。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.42-13）を参照してください。

DAI のデフォルト設定

表 42-1 に、DAI のデフォルト設定を示します。

表 42-1　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。

表 42-1　DAI のデフォルト設定 （続き）

機能	デフォルト設定
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、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 をサポートしないルータ、またはこの機能がイネーブルにされていないルータ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、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、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 アドレスが動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングを必ずイネーブルにしてください。設定の詳細については、第 41 章「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または拒否を行います。
- 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、ルータ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 メンバー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 メンバーが受信する 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。

- 着信トランク 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、各ポートのアグリゲーションを考慮し、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 DoS 攻撃を招く可能性があります。
- Cisco IOS Release 12.2(33)SRD2 は 512k までの ARP スケール（スタティックまたはダイナミック）をサポートします。この機能は、2G SP メモリを搭載した RSP720-3CXL-GE または 2G SP メモリを搭載した RSP720-3CXL-10GE を備えた Cisco 7600 シリーズ ES+ ラインカードの 3CXL バージョンでサポートされます。次の注意事項に従ってください。
  - レイヤ 3 インターフェイスとして Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用している場合は、MAC ラーニングをディセーブルにする必要があります。
  - IPv4 の Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の容量を増やすには、**mls cef maximum-routes** コマンドを使用します。

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」（P.42-7）
- 「DAI インターフェイスの信頼状態の設定」（P.42-8）
- 「DAI フィルタリングのための ARP ACL の適用」（P.42-9）
- 「ARP パケットのレート制限の設定」（P.42-10）
- 「DAI errdisable ステート回復のイネーブル化」（P.42-11）
- 「追加検証のイネーブル化」（P.42-12）
- 「DAI ログ機能の設定」（P.42-13）
- 「DAI 情報の表示」（P.42-16）

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（-）でつなげて入力します。
- 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

ルータは、信頼できるインターフェイス上の他のルータから受信した ARP パケットは検査しません。この場合、パケットはそのまま転送されます。

信頼できないインターフェイスでは、ルータはすべての ARP 要求および ARP 応答を代行受信します。ルータは、代行受信されたパケットが有効な IP-to-MAC アドレス 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、適切な宛先にパケットを転送します。ルータ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.42-13）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}`	別のルータ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`	ルータ間の接続を、trusted として設定します（デフォルトでは untrusted）。
	`Router(config)# no ip arp inspection trust`	ルータ間の接続を、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 7600 Series Router Cisco IOS Command Reference*』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}`	入力を確認します。

ARP ACL を適用する場合、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 範囲で指定にするには、一組の VLAN 番号をダッシュ（-）でつなげて入力します。

  - 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 句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 句に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-to-MAC アドレス バインディングしか持たない ARP パケットは、ACL と比較されます。パケットは、アクセス リストで許可された場合だけに許可されます。

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、ルータは ARP パケットの有効性検査を実行します。これにより、ルータは ARP パケットの DoS 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 DoS 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、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、ルータはこのポートを errdisable ステートにします。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.42-6）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
```

追加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、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、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 検証だけ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 応答内だけで検査されます。
  - **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」（P.42-13）
- 「DAI のログ バッファ サイズの設定」（P.42-14）
- 「DAI のログ システム メッセージの設定」（P.42-14）
- 「DAI のログ フィルタリングの設定」（P.42-15）

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含まれます。

ログ バッファ エントリは、複数のパケットを表すことができます。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 バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。この場合は、パケット数と時間だけが表示され、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、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）。値 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 ～ 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* あたり *number_of_messages* のレートで送信されます。

次に、2 秒おきに 12 メッセージが送信されるように DAI のログ機能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 秒おきに 20 メッセージが送信されるように DAI のログ機能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、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 範囲で指定にするには、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 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 コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットが記録されます。
- **acl-match none**：ACL と一致したパケットを記録しません。
- **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 42-2 に示す各特権 EXEC コマンドを使用します。

表 42-2　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 だけ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 42-3 に示す各特権 EXEC コマンドを使用します。

表 42-3　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 によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN 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 だけの情報が表示されます。

show ip arp inspection statistics コマンドでは、ルータは信頼できる 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。ルータは送信元 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パケット、または DHCP によって許可されたパケットの数を増分します。また、ルータは、該当する失敗回数の値も増分します。

DAI ログ情報を消去または表示するには、表 42-4 に示す各特権 EXEC コマンドを使用します。

表 42-4　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」（P.42-17）
- 「例 2：1 つのスイッチが DAI をサポートする場合」（P.42-21）

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 つのルータが 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 42-2（P.42-4）に示すように、ホスト 1 はルータ A に、ホスト 2 はルータ B にそれぞれ接続されています。両方のルータは、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 ルータ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。ルータ A はホスト 1 およびホスト 2 のバインディングを持ち、ルータ B はホスト 2 のバインディングを持ちます。ルータ A のファスト イーサネット ポート 6/3 は、ルータ 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、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、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 アドレスが動的に割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。設定の詳細については、第 41 章「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 サーバがルータ 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、ルータ A のファスト イーサネット ポート 6/3、およびルータ 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。

ルータ A の設定

ルータ 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　ルータ A およびルータ B 間の接続を確認します。

```
RouterA# 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
```

```
RouterB          Fas 6/3           177         R S I     WS-C6506  Fas 3/3
RouterA#
```

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。

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# ip arp inspection vlan 1
RouterA(config)# end
RouterA# 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
RouterA#
```

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。

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# interface fastethernet 6/3
RouterA(config-if)# ip arp inspection trust
RouterA(config-if)# end
RouterA# show ip arp inspection interfaces fastethernet 6/3

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted              None
RouterA#
```

ステップ 4　バインディングを確認します。

```
RouterA# 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
RouterA#
```

ステップ 5　DAI がパケットを処理する前後の統計情報を調べます。

```
RouterA# 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
RouterA#
```

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。

```
RouterA# 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
RouterA#
```

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])
RouterA# show ip arp inspection statistics vlan 1
RouterA#
```

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
RouterA#
```

ルータ B の設定

ルータ 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。

```
RouterA# 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
RouterB          Fas 3/3            120         R S I     WS-C6506  Fas 6/3
RouterB#
```

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。

```
RouterB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
RouterB(config)# ip arp inspection vlan 1
RouterB(config)# end
RouterB# 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
RouterB#
```

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。

```
RouterB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)# interface fastethernet 3/3
RouterB(config-if)# ip arp inspection trust
RouterB(config-if)# end
RouterB# 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>
RouterB#
```

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。

```
RouterB# 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
RouterB#
```

ステップ 5　DAI がパケットを処理する前後の統計情報を調べます。

```
RouterB# 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
```

```
RouterB#
```

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。

```
RouterB# 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
RouterB#
```

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])
RouterB#
```

この場合に表示される統計情報は次のようになります。

```
RouterB# 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
RouterB#
```

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、図 42-2（P.42-4）に示すルータ B が、DAI または 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。

ルータ B が DAI または DHCP スヌーピングをサポートしていない場合は、ルータ 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、ルータ A およびホスト 1 が、ルータ 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、ルータ 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、ルータ A に ACL 設定を適用できなくなるため、レイヤ 3 でルータ B からルータ A を切り離す必要があります。これらのルータ間では、ルータを使用してパケットをルーティングします。

ルータ 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。

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# arp access-list H2
RouterA(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
RouterA(config-arp-nacl)# end
RouterA# 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。

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# ip arp inspection filter H2 vlan 1
RouterA(config)# end
RouterA#

RouterA# 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
RouterA#
```

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。

```
RouterA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)# interface fastethernet 6/3
RouterA(config-if)# no ip arp inspection trust
RouterA(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 がルータ 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」要求がルータ 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 43

トラフィック ストーム制御の設定

この章では、Cisco 7600 シリーズ ルータに、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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.43-1）
-
- 「トラフィック ストーム制御のデフォルト設定」（P.43-3）
- 「設定時の注意事項および制約事項」（P.43-3）
- 「トラフィック ストーム制御のイネーブル化」（P.43-4）

トラフィック ストーム制御の概要

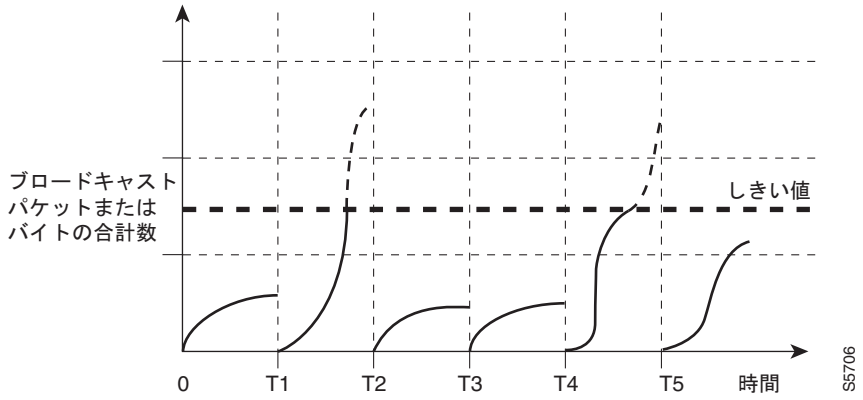
トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、LAN ポートが、物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャスト トラフィック ストームによって中断されるのを防ぎます。

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割合です。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 ストーム制御インターバルで、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 43-1 は、一定時間における LAN インターフェイスのブロードキャスト トラフィック パターンを示しています。この例では、トラフィック ストーム制御が時間 T1 と T2 の間、および T4 と T5 の間で発生します。これらのインターバル中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過しています。

図 43-1　　ブロードキャストの抑制



トラフィック ストーム制御しきい値の数値とタイム 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粒度で機能します。しきい値が高いほど、通過できるパケット数が多くなります。

Cisco 7600 シリーズ ルータ上のトラフィック ストーム制御は、ハードウェアに実装されています。LAN インターフェイスからスイッチング バスへ流れるパケットはトラフィック ストーム制御回路でモニタされます。パケットの宛先アドレスの個別/グループ ビットを使用すると、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またはブロードキャストの場合、1 秒のインターバル内の現在のパケット数を追跡します。この値がしきい値に達すると、以降のパケットは排除されます。

ハードウェアによるトラフィック ストーム制御では、トラフィックの測定に帯域ベースの方式が使用されるので、制御されたトラフィックが使用できる総帯域幅に対する割合の設定が、実装上の最も重要な要素になります。パケットは均等な間隔で着信するわけではないので、制御されたトラフィック アクティビティが測定される 1 秒のインターバルによって、トラフィック ストーム制御の動作が影響を受ける場合があります。

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 ストーム制御インターバル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 トラフィックをドロップします。
- 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 ストーム制御インターバル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 トラフィックをドロップします。
- 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 ストーム制御インターバル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 トラフィックをドロップします。

- 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 ストーム制御インターバル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 トラフィックをドロップします。

トラフィック ストームの検出および制御

このようなストーム イベントを検出して制御するメカニズムを、ストーム制御またはブロードキャスト抑制と呼びます。

トラフィック ストームは、次のことが発生した場合に検出されます。

- ポートが **storm-control** コマンドで設定された帯域幅の値を超えるマルチキャストおよびブロードキャスト トラフィックを受信した場合。
- **show interface gig**<*slot/port*> **counters storm-control** コマンドで表示される TotalSuppDiscards カウンタの値が増加した場合。

Cisco IOS Release 15.0(1)S には、67xx、6196、ES20 および ES+ ラインカードで次のストーム制御機能の強化が含まれています。

- ポートチャネル インターフェイス：ポートチャネル インターフェイスのサポート。
- シャットダウン：ストームが検出され、ストーム トラフィックが同意済みのしきい値を超えた場合、影響を受けるインターフェイスは error disable 状態に移行します。トラフィックのしきい値は、ポートの合計帯域幅に対するパーセンテージ（%BW）として算出されます。error disable の検出およびリカバリ機能、または shut/no shut コマンドを使用して、影響を受けるインターフェイス上のポートを再度イネーブルにします。
- トラップ：ストームの検出時に、SNMP トラップを送信できます。

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です。

設定時の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、次の注意事項および制約事項に従ってください。

- マルチキャストおよびユニキャストのストーム制御は、WS-X6148-RJ-45、WS-X6148-RJ21、WS-X6196-RJ21、6196-21AF、WS-X6148X2-RJ-45、WS-X6548-RJ-45、WS-X6548-RJ21 では機能しません。これらのラインカード（ポート ASIC COIL/Pentamak）でサポートされるのは、ブロードキャスト ストーム制御だけです。
- 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、トラフィック ストーム制御をサポートしません。
- ES+ ラインカードでは、ユニキャスト パケットのストーム制御をサポートしません。
- ルータは、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 ポートでのみサポートします。
- ルータは、ブロードキャスト トラフィック ストーム制御をすべての LAN ポートでサポートします。

- BPDU 以外、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、次のモジュールでマルチキャスト抑制しきい値が超過した場合に、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。
- 6196 ラインカードでは、ブロードキャスト トラフィックの抑制をサポートしますが、マルチキャスト トラフィックはサポートしません。
- ES20 および ES+ ラインカードのポートチャネル インターフェイスでのストーム制御は、Cisco IOS Release 15.0（1）S でサポートされます。
- ユニキャスト トラフィックは、67XX ラインカードでサポートされますが、ES20 および ES40 ラインカードではサポートされていません。
- ポートチャネル インターフェイス上のストーム制御設定に対して行われた追加または変更は、ポートチャネル メンバー リンク上で自動的に更新されます。
- メンバー リンクでは、ストーム制御の設定または削除はできません。
- インターフェイスとポートチャネルのストーム制御設定が同様の場合は、インターフェイスをポートチャネルに追加できます。
  - インターフェイスをポートチャネルに追加する前に、メンバーリンクをまとめてポートチャネルを形成してからポートチャネルを設定するか、ポートチャネルと一致するようにインターフェイス上のストーム制御設定を変更することができます。
- **default interface** コマンドを 2 回実行すると、ストーム制御機能がメンバーリンク インターフェイスから削除されます。

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)# snmp-server enable traps storm-control trap-rate traps per minute`	（任意）SNMP ストーム制御トラップ パラメータをイネーブルにします。trap-rate の範囲は、1 分あたり 0 ～ 1000 トラップです。ただし、ストーム制御用に生成されるトラップの数は、1 分あたり 6 を超えることはできません（設計上）。

	コマンド	目的
ステップ 3	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 4	Router(config-if)# **storm-control multicast level** *level*[*.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。 **（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。
	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 5	Router(config-if)# **storm-control unicast level** *level*[*.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。 **（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。
	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 6	Router(config-if)# **storm-control action** {**shutdown** | **trap**}	
ステップ 7		
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*	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。
  - レベルは 0 ～ 100 の範囲で指定できます。
  - 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。

（注）　次のモジュールでは、0.03 未満のレベル値になるとトラフィックすべてを抑制します。

- WS-X6704-10GE
- WS-X6748-SFP
- WS-X6748-GE-TX

ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、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、設定レベルと数パーセント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。この設定により、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 3/16 でイネーブルになっ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されます。

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control multicast level 70.5
Router(config-if)# end
```

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 43-1 に記載されているコマンドを使用します。

表 43-1　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た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 44

不明なユニキャスト フラッディングのブロック

この章では、Cisco 7600 シリーズ ルータに、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）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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

UUFB の概要

不明なユニキャスト トラフィックは、VLAN 内のすべてのレイヤ 2 ポートでフラッディングします。UUFB 機能を使用すると、この動作を防止できます。UUFB 機能は不明なユニキャスト トラフィックのフラッディングをブロックし、ポートから出力することがわかっている既知の 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 機能は、Private VLAN（PVLAN; プライベート VLAN）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。

UUFB の設定

UUFB 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 block unicast`	ポート上で UUFB をイネーブルにします。
ステップ 4	`Router(config-if)# do show interfaces [`*type*[1] *slot/port*`] switchport | include unicast`	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 を設定し、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 block unicast
Router(config-if)# do show interface fastethernet 5/12 switchport | include unicast
Unknown unicast blocked: enabled
```

CHAPTER 45

PFC QoS の設定

この章では、Cisco 7600 シリーズ ルータの Policy Feature Card（PFC; ポリシー フィーチャ カード）および Distributed Forwarding Card（DFC; 分散型フォワーディング カード）に実装される Quality of Service（QoS）の設定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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- QoS と MPLS の詳細については、第 48 章「PFC の MPLS QoS の設定」を参照してください。
- Cisco 7600 シリーズ ルータの QoS（PFC QoS）は、一部の Cisco IOS Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）を使用します。PFC QoS はハードウェアに実装されるので、MQC 構文のサブセットだけがサポートされます。
- PFC は、Network-Based Application Recognition（NBAR）をサポートしていません。

（注）

Cisco IOS Software Release 15.0(1)S で有効な QoS コマンドの一部がソフトウェア イメージに表示されません。代替 MQC コマンドの詳細については、『*Legacy QoS Command Deprecation*』機能マニュアルを参照してください。
http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/legacy_qos_cli_deprecation_xe.html
『*Legacy QoS Command Deprecation*』マニュアルには、**show queueing** が **show policy-map interface** に置き換えられたことの説明が記載されています。ただし、LAN カードが MQC 設定モデルに従っていないため、**show policy-map interface** では LAN カード上のキューイング情報が表示されません。そのため、Cisco 7600 ルータの LAN カード上のキューイング情報を表示する場合は、代替コマンドの **show mls qos queuing interface** を使用する必要があります。

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」（P.45-2）
- 「PFC QoS のデフォルト設定」（P.45-27）
- 「PFC QoS 設定時の注意事項および制約事項」（P.45-42）
- 「PFC QoS の設定」（P.45-48）
- 「一般的な QoS のシナリオ」（P.45-102）
- 「PFC QoS の用語」（P.45-112）

PFC QoS の機能概要

用語「PFC QoS」は、Cisco 7600 シリーズ ルータの QoS を示します。PFC QoS は、PFC および DFC に加えて、各種のルータ 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 でサポートされるポート タイプ」（P.45-2）
- 「概要」（P.45-2）
- 「コンポーネントの概要」（P.45-5）
- 「分類とマーキングの概要」（P.45-14）
- 「ポートベースのキュー タイプの概要」（P.45-20）
- 「サンプル ネットワークの設計の概要」（P.45-102）

PFC QoS で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/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

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 OSM は、WAN ポートに加えて 4 つのイーサネット LAN ポートを備えています。

PFC QoS は、Optical Service Module（OSM; オプティカル サービス モジュール）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。

概要

ネットワークは通常、*ベスト エフォート型*の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生すると、ドロップされる可能性はすべてのトラフィックで同じです。

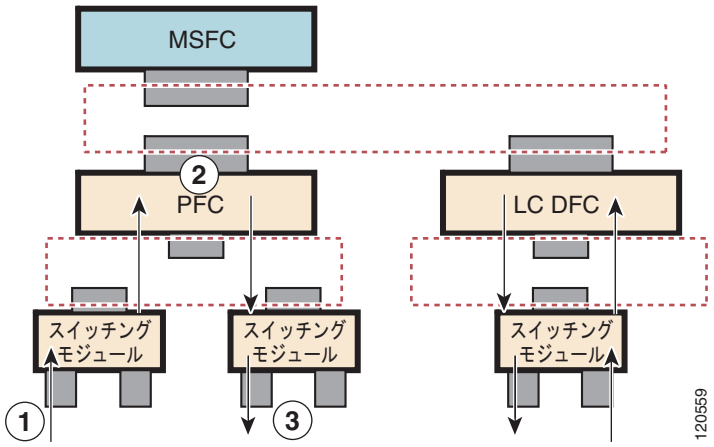
QoS を実装すると、ネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できます。QoS は、ネットワーク トラフィックを選択（分類）し、QoS ラベルを使用または割り当ててプライオリティを与え、設定されたリソース使用量にパケットを制限し（トラフィックをポリシングし、トラフィックをマーキングします）、リソースのコンテンションが存在する場所に輻輳回避を提供します。

PFC QoS の分類、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 ポートの特定用途向け集積回路（ASIC）のハードウェアに実装されます。

（注）　Cisco 7600 シリーズ ルータは、ハードウェアでレイヤ 3 スイッチングまたはレイヤ 2 スイッチングされるトラフィックに対して、すべての MQC 機能（たとえば、専用アクセス レート（CAR））をサポートしているわけではありません ポート ASIC にキューイングが実装されるため、Cisco 7600 シリーズ ルータは MQC 設定のキューイングをサポートしません。

図 45-1 に、Cisco 7600 シリーズ ルータの QoS プロセスの概要を示します。

図 45-1　PFC QoS 機能による処理の概要



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 では、*信頼（trust）*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。ポートはデフォルトで信頼できない（untrusted）に設定され、初期内部 DSCP 値が 0 に設定されます。受信した CoS、IP precedence、または DSCP を信頼するようにポートを設定できます。
   - レイヤ 2 CoS 再マーキング：PFC QoS は、レイヤ 2 CoS 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、着信フレームにポート CoS 値がマーキングされます。
     - ポートが untrusted として設定されている場合
     - ポートが trusted として設定されているが、トラフィックが ISL、802.1Q、または 802.1p フレーム タイプでない場合

     OSM ATM および POS ポートでは、PFC QoS は常に CoS = 0 に設定します。
   - 輻輳回避：イーサネット LAN ポートを trust CoS に設定した場合、QoS はレイヤ 2 CoS 値に基づいてトラフィックを分類し、入力キューに割り当てて、輻輳回避を提供します。レイヤ 3 DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートだけで使用できます。
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た初期内部 DSCP と最終内部 DSCP が存在します。最終内部 DSCP を初期値と同じ値にしたり、MQC ポリシー マップでその値を別の値に設定したりできます。
   - MQC ポリシー マップ：MQC ポリシー マップは、次のいずれかの処理を行うことができます。
     - 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 を使用したレイヤ 3 DSCP マーキング（オプションで PFC に対して）

- 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 ポートだけで使用できます）

次の図は、QoS とルータ コンポーネント間の関係の詳細を示します。

- 図 45-2、「PFC の PFC QoS 機能を使用したトラフィック フロー」
- 図 45-3、「PFC QoS 機能とコンポーネントの概要」

図 45-2　PFC の PFC QoS 機能を使用したトラフィック フロー

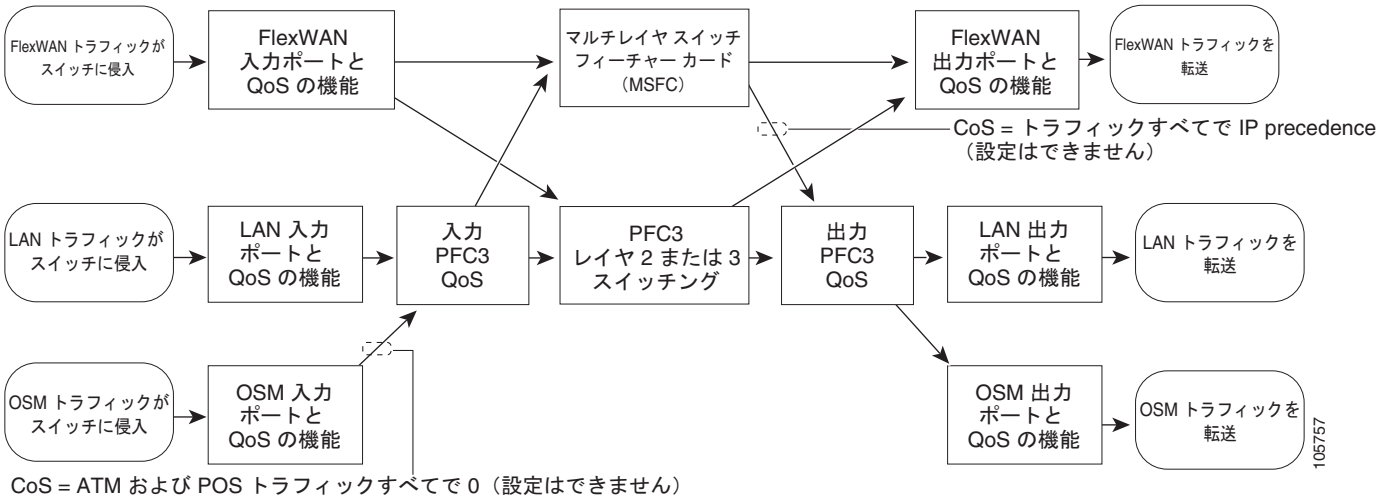
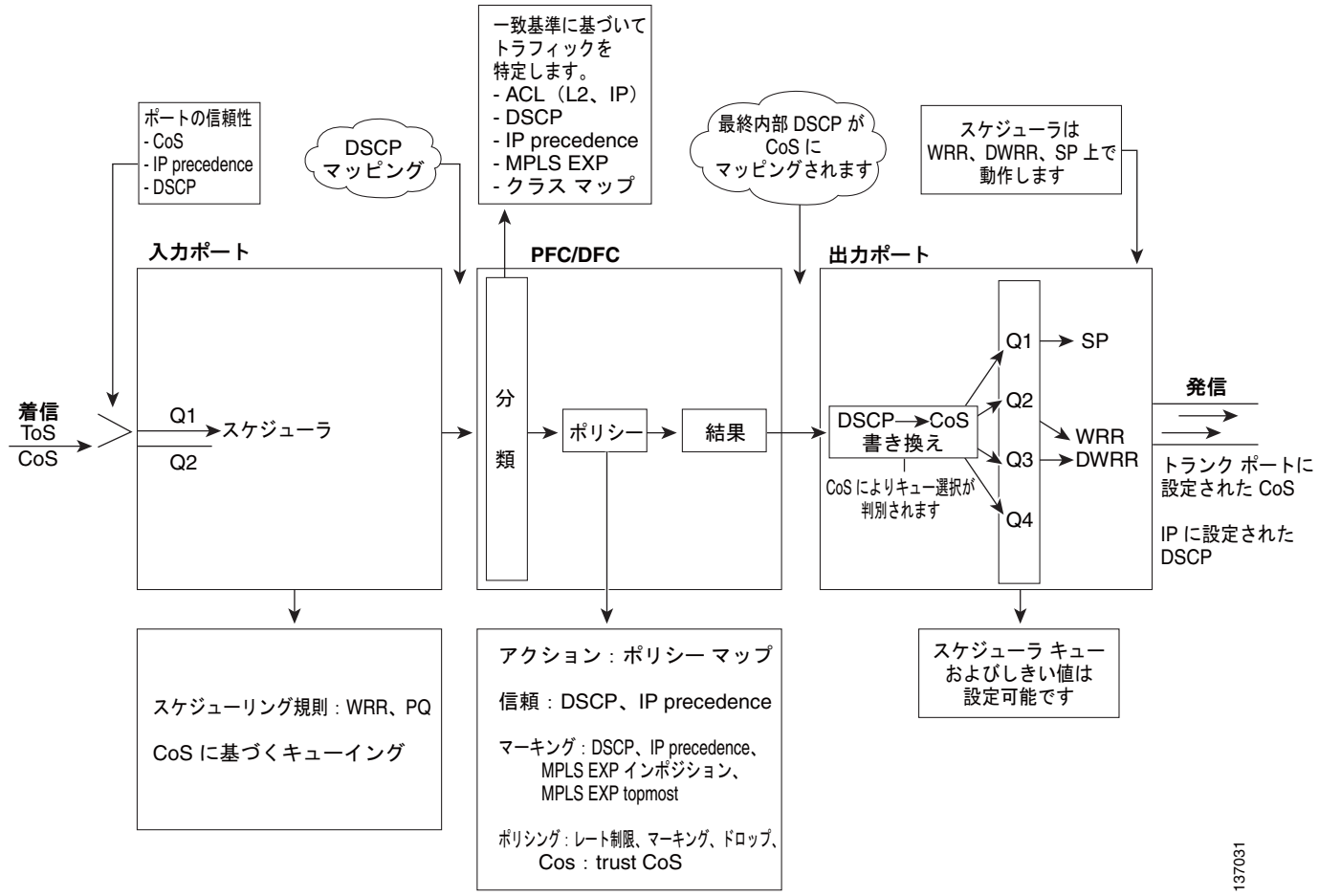


図 45-2 に、PFC の PFC QoS 機能を通過するトラフィック フローを示します。

- 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 トラフィックを PFC でレイヤ 3 スイッチングさせたり、MSFC によってソフトウェアでルーティングさせたりできます。
  - 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 ポートの QoS 機能を LAN ポートの入力トラフィックに適用させることができます。
  - 入力 PFC QoS を LAN ポートの入力トラフィックに適用させることができます。
  - 入力 LAN ポートのトラフィックを PFC でレイヤ 2 またはレイヤ 3 スイッチングさせたり、MSFC によるソフトウェアでルーティングさせたりできます。
  - 出力 PFC QoS および出力 LAN ポートの QoS を LAN ポートの出力トラフィックに適用させることができます。
- OSM トラフィックの場合
  - 入力 OSM ポートの QoS 機能を OSM ポートの入力トラフィックに適用させることができます。

- 入力 PFC QoS を OSM ポートの入力トラフィックに適用させることができます。
- 入力 OSM ポートのトラフィックを PFC でレイヤ 3 スイッチングさせたり、MSFC によってソフトウェアでルーティングさせたりできます。
- 出力 PFC QoS および出力 OSM ポートの QoS を OSM ポートの出力トラフィックに適用させることができます。

図 45-3　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.45-6）
- 「PFC および DFC の QoS 機能」（P.45-7）
- 「出力ポートの QoS 機能」（P.45-10）

入力 LAN ポートの PFC QoS 機能

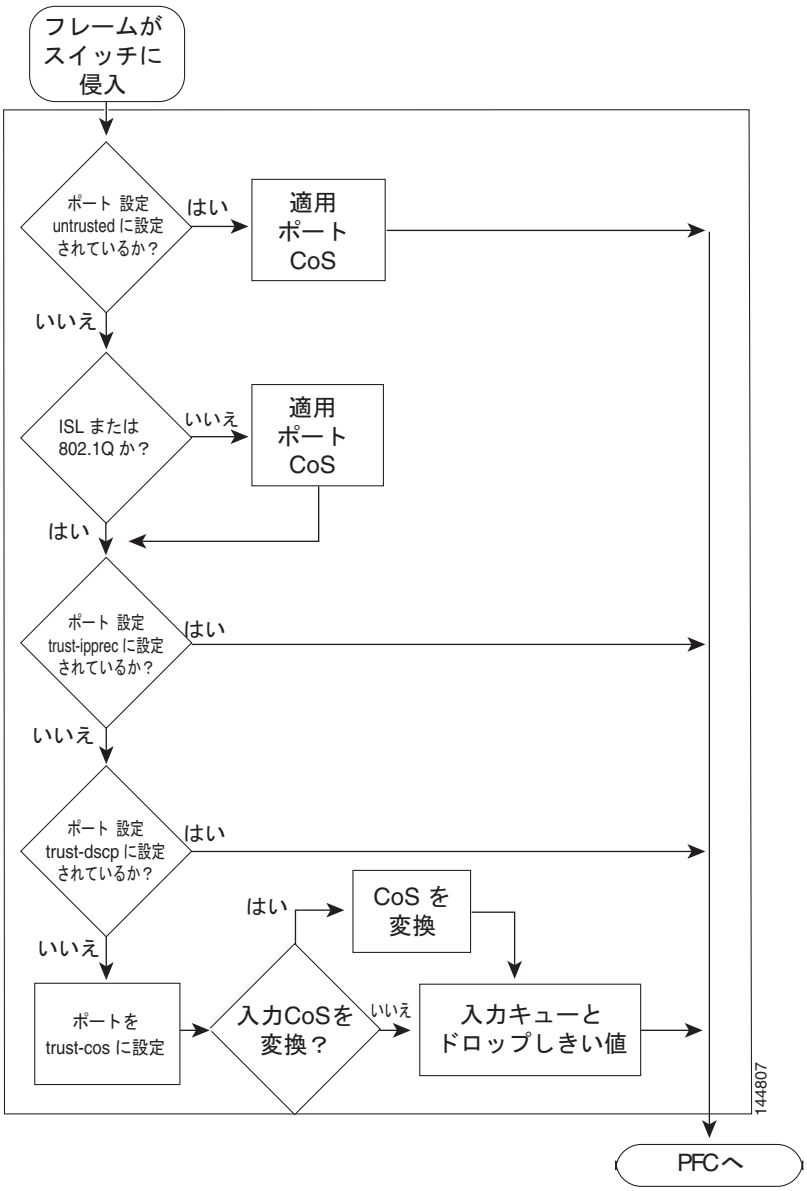
ここでは、入力ポートの QoS 機能の概要について説明します。

- 「入力 LAN ポート PFC QoS 機能のフローチャート」（P.45-6）
- 「ポートの信頼性」（P.45-7）
- 「輻輳回避」（P.45-7）

入力 LAN ポート PFC QoS 機能のフローチャート

図 45-4 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 45-4　　入力ポートの 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。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ています。

ポートの信頼性

PFC QoS では、*信頼（trust）*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（untrusted）に設定することも、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、trust CoS ポートといいます。
  - trust 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、trust CoS トラフィックといいます。

（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。受信した CoS 値は、CoS を信頼するように設定されたポートでだけ維持されます。

- IP precedence
  - IP precedence を信頼するように設定されたポートを、trust IP precedence ポートといいます。
  - trust 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、trust IP precedence トラフィックといいます。
- DSCP
  - DSCP を信頼するように設定されたポートは、trust DSCP ポートといいます。
  - trust DSCP ポート経由で受信されたトラフィック、または、DSCP を信頼するようにポリシー マップによって設定されたトラフィックは、trust DSCP トラフィックといいます。

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いいます。

輻輳回避

PFC QoS は、trust CoS ポートに輻輳回避を実装します。trust CoS ポートでは、QoS が、レイヤ 2 の CoS 値に基づいてトラフィックを分類し、入力キューに割り当てることによって、輻輳回避を実現します。Release 12.2(33)SRC 以降のリリースでは、受信した DSCP 値を輻輳回避に使用するように WS-X6708-10GE trust DSCP ポートを設定できます。入力側の輻輳回避の詳細については、「trust CoS 入力 LAN ポートでの分類とマーキング」（P.45-15）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」（P.45-8）
- 「サポートされている DFC」（P.45-8）

- 「PFC および DFC の QoS 機能リストおよびフローチャート」（P.45-8）
- 「内部 DSCP 値」（P.45-9）

サポートされるポリシー フィーチャ カード

PFC は、スーパーバイザ エンジンに取り付けられたドータカードです。PFC は、他の機能に加えて、QoS を提供します。Cisco 7600 シリーズ ルータでサポートされている PFC は、次のとおりです。

- PFC3B（Supervisor Engine 720 および Supervisor Engine 32）
- PFC3BXL（Supervisor Engine 720）
- Route Switch Processor 720（RSP720）の PFC3C および PFC3CXL

サポートされている DFC

PFC は QoS ポリシーのコピーを 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。

Cisco 7600 シリーズ ルータでサポートされている DFC は、次のとおりです。

- WS-F6K-DFC3B、WS-F6K-DFC3BXL（Supervisor Engine 720 の dCEF256 および CEF256 モジュール用）
- WS-F6700-DFC3B、WS-F6700-DFC3BXL（Supervisor Engine 720 の CEF720 モジュール用）

PFC および DFC の QoS 機能リストおよびフローチャート

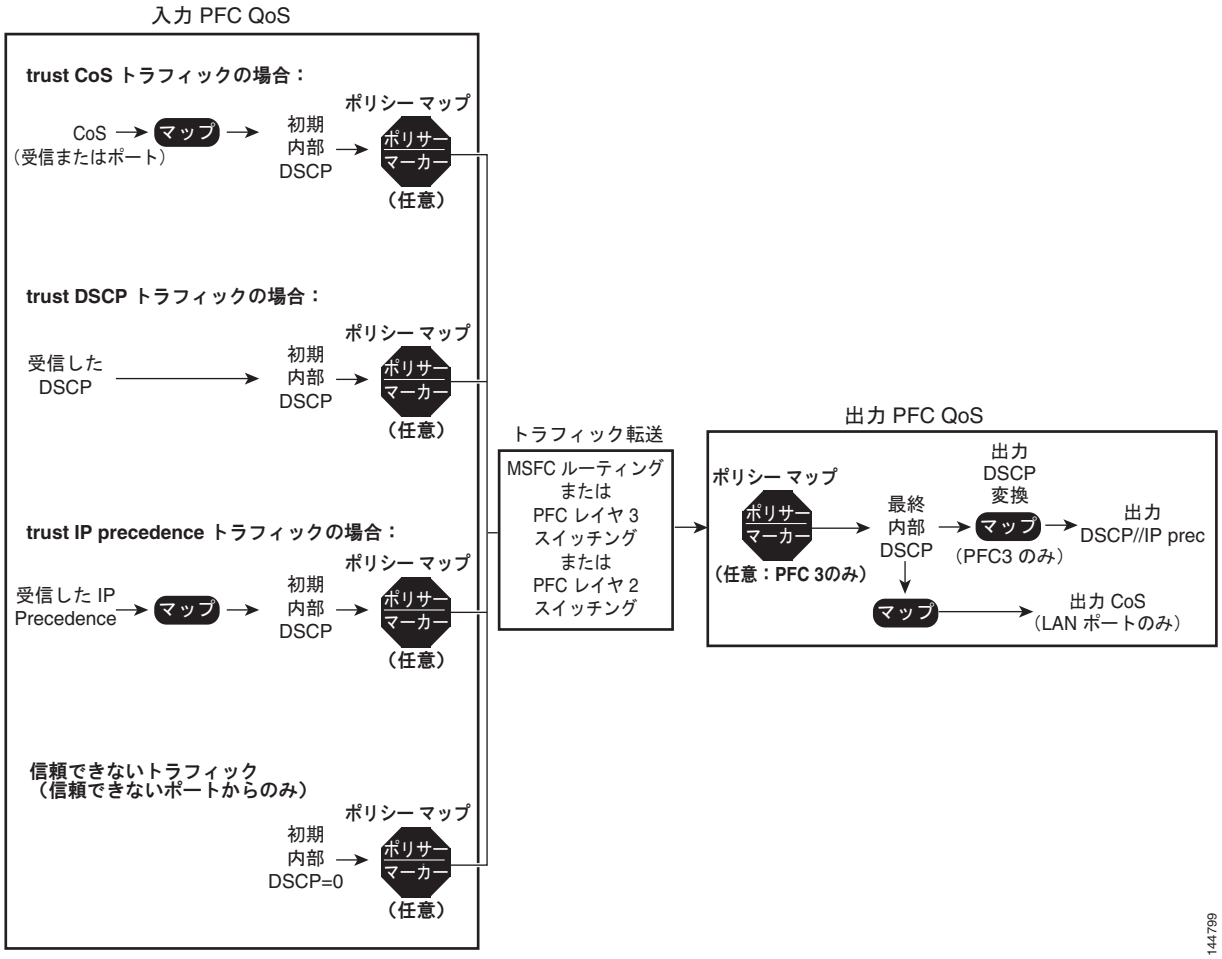
表 45-1 は、PFC および DFC の各バージョンでサポートされる QoS 機能の一覧を示します。

表 45-1　PFC および DFC でサポートされている QoS 機能

機能	PFC3B/DFC3B	PFC3BXL/DFC3BXL
DFC に対するサポート	Yes	Yes
フローの粒度	送信元 宛先	送信元 宛先
QoS ACL	IP、MAC	IP、MAC
DSCP 透過性 **（注）** DSCP 透過性をイネーブルにすると、出力 ToS の書き換えがディセーブルになります。	オプション	オプション
出力 ToS の書き換え	オプション	オプション
ポリシング：		
入力集約ポリサー	Yes	Yes
出力集約ポリサー	Yes	Yes
集約ポリサーの数	1022	1022
マイクロフロー ポリサー	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	110,000	240,000
ポリサーによる統計情報の計測単位	バイト	バイト
ポリサー処理の基準	レイヤ 2 の長さ	レイヤ 2 の長さ

図 45-5 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 45-5　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。PFC では、マーキングまたはポリシングが行われる前に、PFC QoS が、次のように初期内部 DSCP 値を導出します。

- trust CoS トラフィックの場合、受信した CoS 値またはポートの CoS 値

（注）　信頼できない入力ポートからのトラフィックには、ポート CoS 値があります。信頼できないポートからのトラフィックが trust CoS ポリサーと一致する場合、PFC QoS は入力ポート CoS 値から内部 DSCP 値を導出します。

- trust IP precedence トラフィックの場合、受信した IP precedence 値からのマッピング

- trust DSCP トラフィックの場合、受信した DSCP 値
- 信頼できないトラフィックの場合、ポリシー マップに設定されたポートの CoS 値または DSCP 値からのマッピング

trust CoS トラフィックおよび trust IP precedence トラフィックの場合、PFC QoS は、設定変更可能なマップを使用して、それぞれ 3 ビット値である CoS または IP precedence から、6 ビットの内部 DSCP 値を導出します。

PFC でのマーキングおよびポリシングによって初期内部 DSCP 値が最終内部 DSCP 値に変更されます。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 マップを対応付けることができます。

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。

- ポート ベースの PFC QoS 用に設定された非トランク入力 LAN ポート上では、そのポート経由で受信されたすべてのトラフィックが、ポートに対応付けられたポリシー マップに従います。
- 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 トラフィックが、ポートに対応付けられたポリシー マップに従います。

VLAN ベースの PFC QoS 用に設定された非トランク入力 LAN ポート上では、ポート経由で受信されたトラフィックが、ポートの VLAN に対応付けられたポリシー マップに従います。

VLAN ベースの PFC QoS 用に設定されたトランク入力 LAN ポート上では、ポート経由で受信されたトラフィックが、トラフィックの VLAN に対応付けられたポリシー マップに従います。

出力ポートの QoS 機能

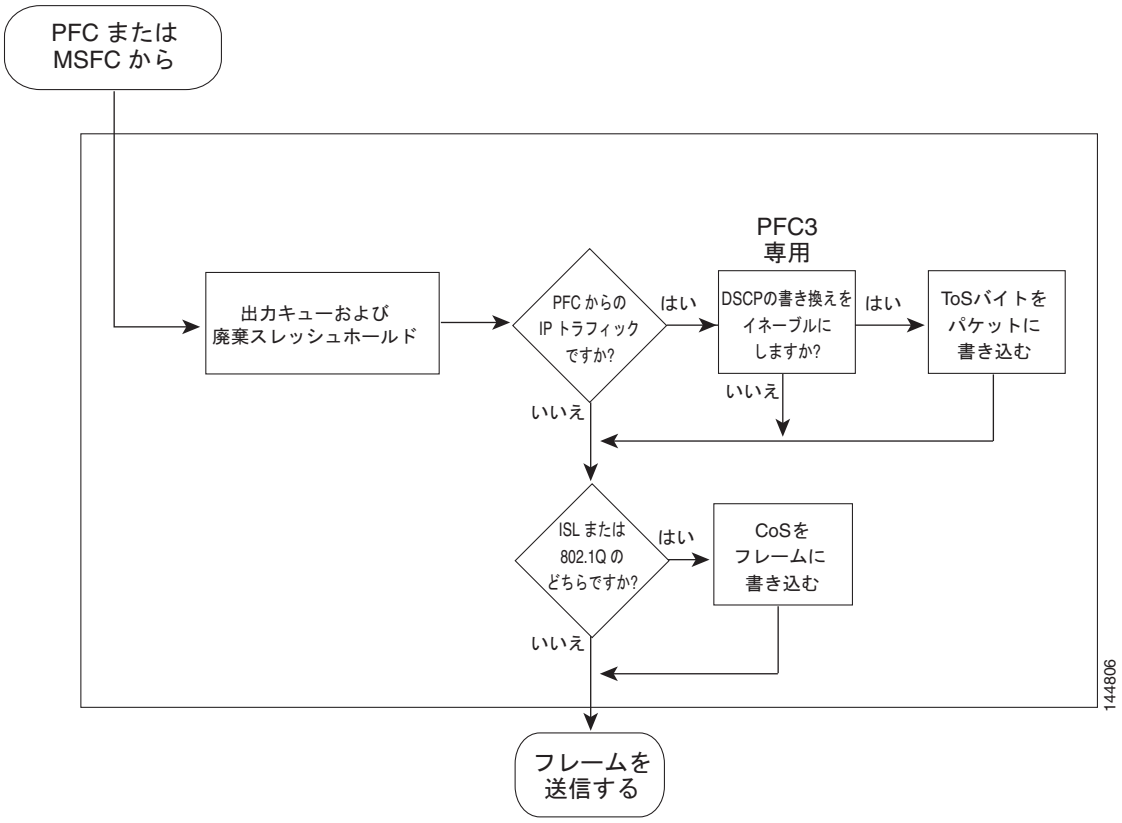
ここでは、出力ポートの QoS 機能について説明します。

- 「出力 LAN ポート機能のフローチャート」（P.45-11）
- 「出力 CoS 値」（P.45-11）
- 「出力 DSCP 変換」（P.45-12）
- 「出力 ToS バイト」（P.45-12）
- 「出力 PFC QoS インターフェイス」（P.45-12）
- 「再マーキングされた DSCP に対する出力 ACL のサポート」（P.45-12）
- 「出力 OSM ポートのマーキング」（P.45-13）

出力 LAN ポート機能のフローチャート

図 45-6 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 45-6　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、トラフィックと対応付けられた最終内部 DSCP 値から CoS 値を導出します。PFC QoS は出力 LAN ポートに導出された CoS 値を送信し、それがスケジューリングに使用され、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(33)SRC およびそれ以降では、最終内部 DSCP 値を入力 LAN ポートでの分類および輻輳回避に使用するように WS-X6708-10GE ポートを設定できます。「DSCP ベースのキュー マッピングの設定」（P.45-90）を参照してください。

出力 DSCP 変換

15 の出力 DSCP 変換マップを設定することにより、内部 DSCP 値が出力 ToS バイトに書き込まれる前に、内部 DSCP 値を変換することができます。出力 DSCP 変換マップを、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。

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。trust DSCP トラフィックと信頼できない IP トラフィックの場合は、ToS バイトに、受信された ToS バイトの元の最下位 2 ビットが含まれています。

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.45-48）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）に対応付けることで、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。
- ARP 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。
- 出力ポリシーで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。

再マーキングされた DSCP に対する出力 ACL のサポートにより、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングで、入力 PFC QoS によって変更された IP precedence、DSCP ポリシング、またはマーキングを使用できるようになります。

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。

PFC 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、PFC 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 回めの処理では入力 PFC QoS を適用し、2 回めの処理では出力 PFC QoS を適用します。

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 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ドロップされます。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。

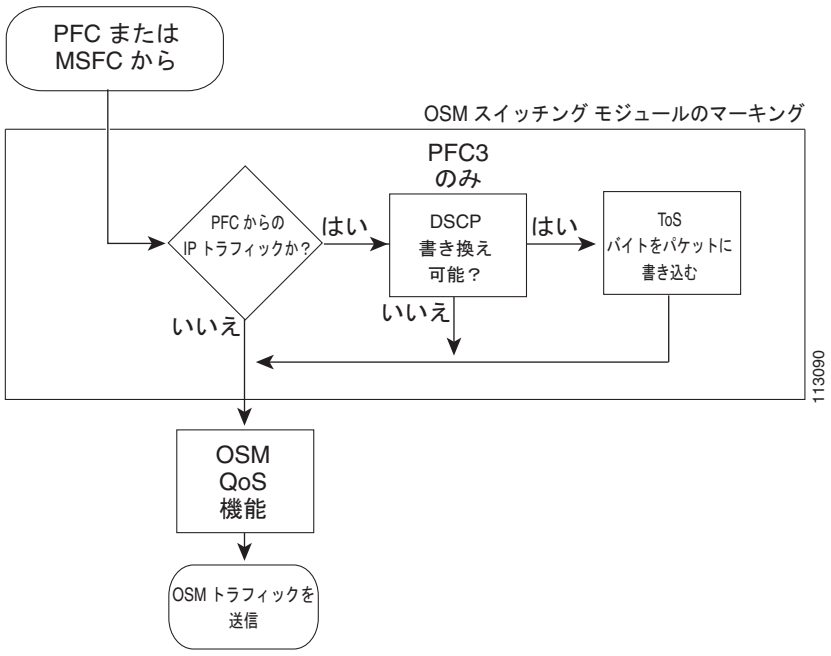
入力 PFC QoS によってパケットが処理され、すべてのポリシングまたはマーキング変更が行われると、このパケットは出力 PFC QoS によって処理される前に、すべての設定済みレイヤ 3 機能（たとえば、入力 Cisco IOS ACL、Policy-Based Routing（PBR; ポリシー ベース ルーティング）など）によって入力インターフェイス上で処理されます。

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ドロップ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 45-7 を参照）。

図 45-7　出力 WAN 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、Cisco 7600 シリーズ ルータで行われる分類とマーキングの場所と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.45-14）
- 「入力 OSM ポートでの分類とマーキング」（P.45-16）
- 「サービス ポリシーとポリシー マップを使用した PFC での分類とマーキング」（P.45-16）
- 「MSFC での分類とマーキング」（P.45-17）

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

入力 LAN ポート上での分類、マーキング、および輻輳回避では、レイヤ 3 の IP precedence 値または DSCP 値は使用または設定されず、レイヤ 2 CoS 値が使用されます。

Release 12.2(33)SRC およびそれ以降では、受信 DSCP 値を入力 LAN ポートでの分類および輻輳回避に使用するように WS-X6708-10GE ポートを設定できます（「DSCP ベースのキュー マッピングの設定」（P.45-90）を参照）。

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.45-14）
- 「信頼できる入力ポートでの分類とマーキング」（P.45-14）

信頼できない入力ポートでの分類とマーキング

PFC QoS レイヤ 2 の再マーキングは、信頼できない入力ポート経由で受信したすべてのフレームに、ポート CoS 値（デフォルトは 0）をマーキングします。

信頼できない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 trust 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。ルータ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、trust CoS ポートからルータ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。

- 「trust CoS 入力 LAN ポートでの分類とマーキング」（P.45-15）
- 「trust IP precedence 入力ポートでの分類とマーキング」（P.45-15）
- 「trust DSCP 入力ポートでの分類とマーキング」（P.45-15）

trust CoS 入力 LAN 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 フレームがルータに入ると、PFC QoS はユーザ 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 フレームがルータに入ると、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。

（注） ルータに入ったあと、ポリシー マップはトラフィックの信頼状態を変更し、初期内部 DSCP 値の基準として、受信した IP precedence または DSCP を使用できます。

- PFC QoS では、CoS ベースの入力キューおよびしきい値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。入力キューおよびしきい値の詳細については、「ポートベースのキュー タイプの概要」（P.45-20）を参照してください。

trust 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。trust IP precedence ポートからのトラフィックの場合、トラフィックの信頼状態を変更するポリシー マップが存在する場合を除き、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しきい値では、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。

trust DSCP 入力ポートでの分類とマーキング

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にだけ、ポートを trust DSCP に設定する必要があります。trust DSCP ポートからのトラフィックの場合、トラフィックの信頼状態を変更するポリシー マップが存在する場合を除き、PFC QoS は、受信した DSCP 値を初期内部 DSCP 値として使用します。入力ポート キューとしきい値はレイヤ 2 CoS を使用するため、PFC QoS は、DSCP を信頼するように設定されたポートに入力ポートの輻輳回避を実装しません。PFC は、受信した DSCP を信頼するように設定された入力ポートのトラフィックをマーキングしません。

Release 12.2(33)SRC およびそれ以降では、DSCP ベースの入力キューとしきい値を WS-X6708-10GE ポートでイネーブルにして、輻輳回避を提供します（「DSCP ベースのキュー マッピングの設定」（P.45-90）を参照）。

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 を対応付けます。入力 OSM ポートの信頼状態を設定し、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 ポート上ではポート CoS 値を設定できないため、POS および ATM OSM ポート上では、CoS は常に 0 です）

サービス ポリシーとポリシー マップを使用した PFC での分類とマーキング

PFC QoS は、1 つのポリシー マップを次のインターフェイス タイプに対応付けることによって入力 PFC QoS を適用するサービス ポリシーを使用した分類とマーキングをサポートします。

- 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

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 マップを対応付けることで、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 コントロール 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 マップの **set** コマンド：信頼できないトラフィックでは、PFC QoS は、設定された IP precedence または DSCP 値を最終内部 DSCP 値として使用できます。「IP precedence 値と DSCP 値」（P.45-48）に、IP precedence および DSCP のビット値を示します。
- 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、ポートで信頼されていた 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。

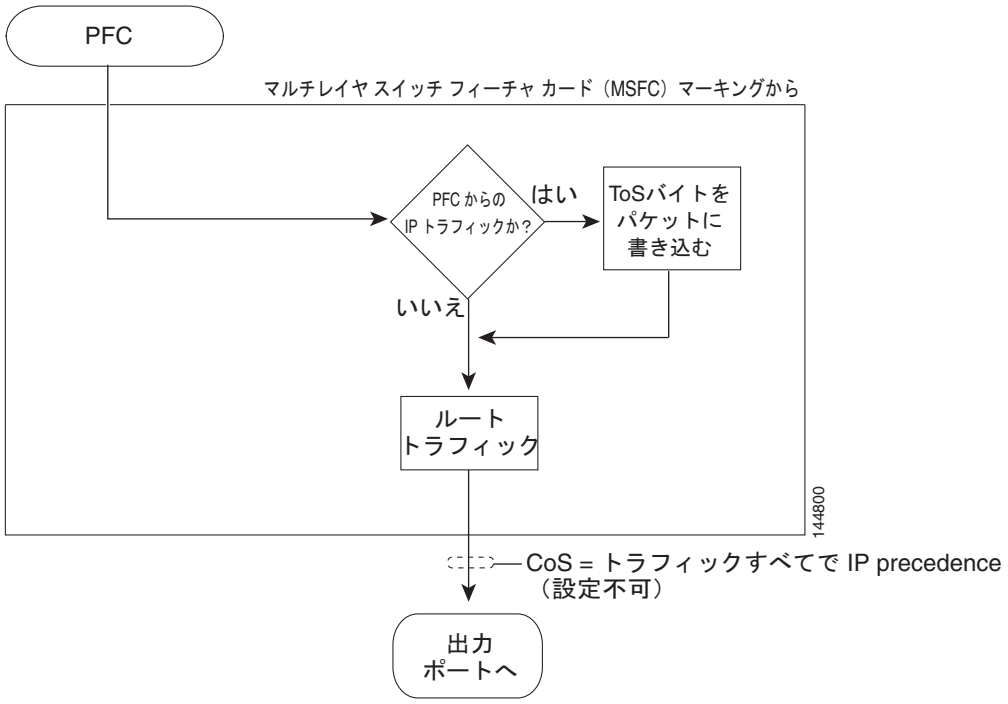
（注） trust CoS ポリシー マップは、信頼できない入力 LAN ポートからのトラフィックで受信した CoS を戻すことはできません。信頼できない入力 LAN ポートからのトラフィックには、常にポート CoS 値があります。

- 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、マーキングまたはドロップのいずれかを実行できます。

MSFC での分類とマーキング

PFC QoS は、最終内部 DSCP 値を使用して IP トラフィックを MSFC に送信します。CoS は、MSFC から出力ポートへ送られるすべてのトラフィックの IP precedence と一致します。

図 45-8　　PFC3 および MSFC2A または MSFC3 によるマーキング



（注）　PFC 上でレイヤ 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.45-17）*
- *「集約ポリサー」（P.45-18）*
- 「マイクロフロー ポリサー」（P.45-19）

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、着信および発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、またはドロップされます。

ポリシングでは、アウトオブプロファイル パケットがバッファに保存されません。したがって、ポリシングが伝搬遅延に影響することはありません。逆に、トラフィック シェーピングではアウトオブプロファイル 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）。

PFC は、入力および出力ポリシングを含む、入力および出力の両方の PFC QoS をサポートします。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。

（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。PFC の出力トラフィックの場合、VLAN 単位でポリサーを適用できます。

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
- 帯域利用率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 TFTP 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対応付けると、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対応付けると、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 の 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場合、VLAN 1 および VLAN 3 の各フローで 1 Mbps が許可されます。つまり、VLAN 1 上に 3 つのフロー、VLAN 3 上に 4 つのフローが存在する場合、マイクロフロー ポリサーは、これらの各フローに対して 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 通りのレートとバースト 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 ポリサーが適用されます。
- 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 が異なるトラフィックでも、同じフローの一部であると見なします。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。
- 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。
- ARP 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。

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ー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 はいずれかのポリサーに基づいてアウトオブプロファイル 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、またはパケットをドロップします。両方のポリ

サーからアウトオブプロファイル ステータスが戻された場合には、いずれかのポリサーでパケットのドロップが指定されていれば、パケットはドロップされます。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。

ポリシングでは、レイヤ 2 フレーム サイズを使用します。帯域利用率限度は、Committed Information Rate（CIR; 認定情報レート）で指定します。より高い PIR（Peak Information Rate; 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、「アウト オブ プロファイル」または「不適合」です。

ポリサーごとに、アウトオブプロファイル パケットをドロップするか、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）。アウトオブプロファイル パケットは、元のプライオリティを維持しないため、インプロファイル パケットが消費した帯域幅の一部としてカウントされません。

PIR を設定する場合は、PIR アウトオブプロファイル アクションを CIR アウトオブプロファイル アクションよりも厳密なものする必要があります。たとえば、CIR アウトオブプロファイル アクションがトラフィックをマークダウンするアクションの場合、PIR アウトオブプロファイル アクションはトラフィックを送信するアクションにできません。

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ドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップ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ドロップ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、Cisco 7600 シリーズ ルータ LAN モジュールでサポートされているキュー タイプ、廃棄しきい値、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」（P.45-21）
- 「入力キュー タイプ」（P.45-23）
- 「出力キューのタイプ」（P.45-23）
- 「モジュールとキュー タイプのマッピング」（P.45-24）

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 には、固定数のキューに分割されたバッファがあります。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、スイッチを中継する際、一時的にフレームを保存します。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。

Cisco 7600 シリーズ ルータ LAN モジュールは、次のタイプのキューをサポートしています。

- 標準キュー
- 完全優先キュー

Cisco 7600 シリーズ ルータ LAN モジュールは、キュー間で次のタイプのスケジューリング アルゴリズムをサポートしています。

- Weighted Round-Robin（WRR; 重み付きラウンドロビン）: WRR は、キューに対する帯域幅を明示的に確保しておきません。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は、キューに割り当てられる帯域幅の量を定義します。
- Deficit Weighted Round Robin（DWRR）: WRR によって提供される動作に加えて、DWRR では、送信中のロー プライオリティ キューを常に把握し、次回に未処理分の送信が補われます。
- 完全優先キューイング：完全優先キューイングは、他のキューのパケットがデキューイングされる前に、音声などの遅延に影響されやすいデータのデキューイングおよび送信を許可し、遅延に影響されやすいデータを他のトラフィックより優先させます。ルータは、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。標準キューのパケットが送信されたあと、スイッチが完全優先キュー内のトラフィックを確認します。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。

Cisco 7600 シリーズ ルータ LAN モジュールは、キュー内で次のタイプのしきい値による輻輳回避を提供します。

- Weighted Random Early Detection（WRED; 重み付きランダム早期検出）: WRED 廃棄しきい値が設定されたポートでは、所定の CoS 値のフレームは、バッファ輻輳を回避するために設計されたランダム確率に基づいてキューに格納されます。所定の CoS によるフレームがキューに格納される確率または廃棄される確率は、その CoS 値に割り当てられている重み値としきい値によって左右されます。

  たとえば、しきい値が 2 のキュー 1 に CoS 2 が割り当てられ、しきい値 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ドロップされません。キュー項目数が 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 フレームはすべてドロップされます。キュー レベルが低しきい値と高しきい値の間にあるときにスイッチが廃棄するフレームは、フロー単位または FIFO 方式ではなく、ランダムに抽出されます。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 ドロップ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。
- テール廃棄しきい値：テール廃棄しきい値を設定したポートでは、所定の CoS 値に対応付けられた廃棄しきい値を超過するまで、その CoS 値のフレームがキューに格納されます。その CoS 値の後続のフレームは、しきい値を超過しなくなるまで廃棄されます。たとえば、しきい値が 2 のキュー 1 に CoS 1 が割り当てられ、しきい値 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% 占有されるまではドロップされません。以降のすべての CoS 1 フレームは、キューの占有率が 60 % 未満になるまでドロップされます。一部のポート タイプでは、テールドロップしきい値および WRED ドロップしきい値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しきい値にマッ

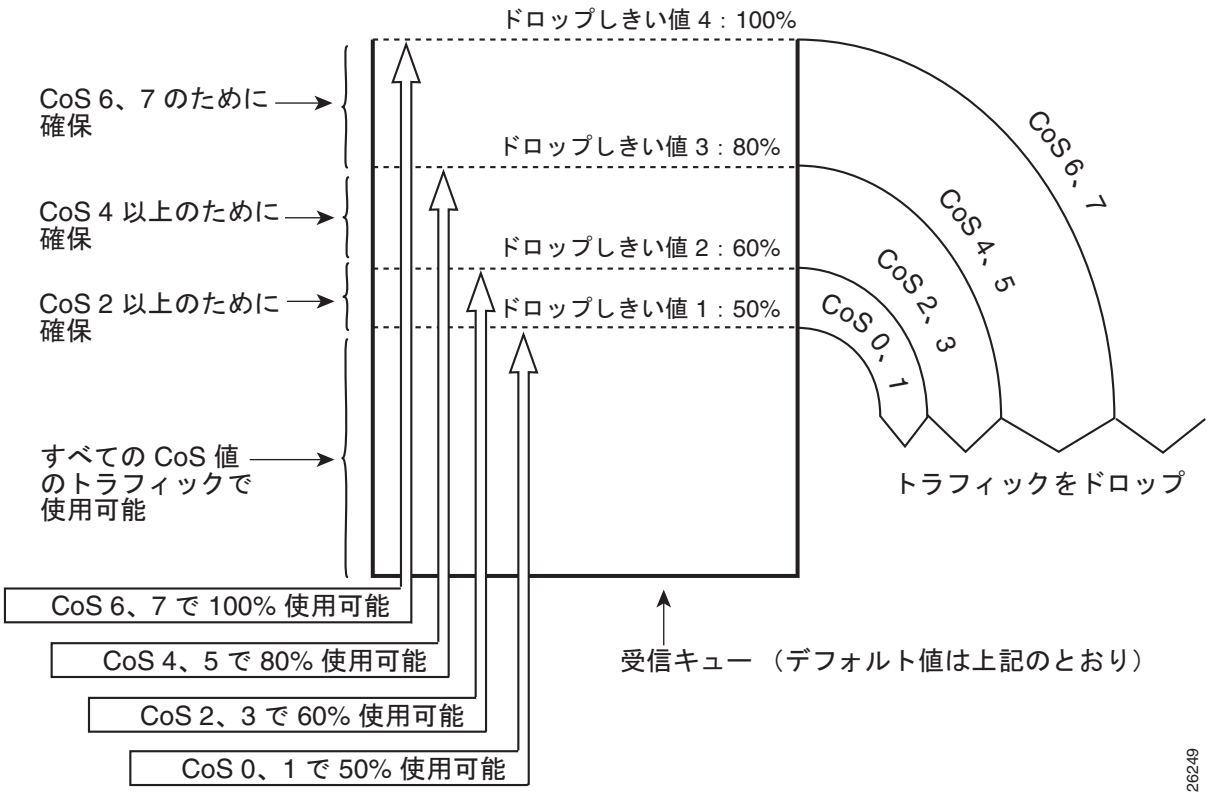
ピングします。スイッチでは、キューにだけマッピングされている CoS 値を伝送するトラフィックには、テール ドロップしきい値が使用されます。キューとしきい値にマッピングされた CoS 値を伝送するトラフィックには、WRED ドロップしきい値が使用されます。同じタイプの LAN ポートは、すべて同じドロップしきい値の設定を使用します。

（注）　Release 12.2(33)SRC およびそれ以降では、DSCP ベースのキューとしきい値を WS-X6708-10GE ポートで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.45-90）を参照してください。

複数のキュー、および各キューに対応付けられたスケジューリング アルゴリズムの組み合わせることにより、スイッチで輻輳回避を提供できます。

図 45-9 に、**1q4t** 入力 LAN ポートのドロップしきい値を示します。他の設定でも、ドロップしきい値は同様に機能します。

図 45-9　受信キューのドロップしきい値



入力キュー タイプ

LAN ポートのキュー構造を表示するには、**show mls qos queuing 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ドロップしきい値および 1 つの設定変更できないテールドロップしきい値がある、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ドロップしきい値がある 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ドロップしきい値がある 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ドロップしきい値がある 2 つの標準キューを意味します。
- **8q8t** は、それぞれ WRED ドロップまたはテールドロップとして設定変更可能な 8 つのしきい値がある 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ドロップしきい値がある 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
  - 設定変更可能なしきい値がない 1 つの標準キュー（実質的には 100% のテールドロップしきい値）
- **1p1q8t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のしきい値を持つ 1 つの標準キュー：
    - それぞれ WRED ドロップまたはテールドロップとして設定変更可能な 8 つのしきい値
    - 設定変更できない（100%）1 つのテール廃棄しきい値

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 mls qos queuing 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ドロップしきい値がある 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 ドロップしきい値がある 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
  - 次のしきい値を持つ 3 つの標準キュー：
    - WRED ドロップまたはテールドロップとして設定変更可能な 1 つのしきい値
    - 設定変更できない（100%）1 つのテールドロップしきい値

- **1p2q1t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のしきい値を持つ 2 つの標準キュー
    - 1 つの WRED ドロップしきい値
    - 設定変更できない（100%）1 つのテール廃棄しきい値
- **1p3q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED ドロップまたはテールドロップのどちらかとして設定変更可能なしきい値が 8 つずつある 3 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 ドロップまたはテールドロップのいずれかとして設定変更可能なしきい値が 8 つずつある 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 45-2　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	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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
RSP720-3C-10GE RSP720-3CXL-10GE							
ギガビット イーサネット ポートがイネーブルな場合	2q4t	WRR	1p3q4t	DWRR または SRR		108 MB	98 MB
ギガビット イーサネット ポートがディセーブルな場合	8q4t		1p7q4t				
WS-SUP720	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-SUP720-3B							
WS-SUP720-3BXL							
RSP720-3C-GE							
RSP720-3CXL-GE							

表 45-2　スーパーバイザ エンジン モジュールの QoS キュー構造 （続き）

スーパーバイザ エンジン	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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-SUP32-10GE	2q8t	WRR	1p3q8t	DWRR または 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

表 45-3　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	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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	WRR	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6548-RJ-21							
WS-X6548-RJ-45							
WS-X6324-100FX-MM	1q4t	WRR	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-X6148X2-RJ-45	1p1q0t	WRR	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6148X2-45AF							
WS-X6024-10FL-MT	1q4t	WRR	2q2t	WRR	64 KB	8 KB	56 KB

表 45-4　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	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
DFC3 を搭載した WS-X6748-GE-TX	2q8t	WRR	1p3q8t	DWRR	1.3 MB	166 KB	1.2 MB
CFC を搭載した WS-X6748-GE-TX	1q8t	WPR					
DFC3 を搭載した WS-X6748-SFP	2q8t	WRR					
CFC を搭載した WS-X6748-SFP	1q8t	WRR					
DFC3 を搭載した WS-X6724-SFP	2q8t	WRR					
CFC を搭載した WS-X6724-SFP	1q8t	WRR					
WS-X6548-GE-TX	1q2t	WRR	1p2q2t	WRR	1.4 MB	185 KB	1.2 MB
WS-X6548V-GE-TX							
WS-X6548-GE-45AF							
WS-X6516-GBIC	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6516A-GBIC		WRR		WRR	1 MB	135 KB	946 KB
WS-X6516-GE-TX		WRR		WRR	512 KB	73 KB	439 KB
WS-X6408-GBIC	1q4t	WRR	2q2t	WRR		80 KB	432 KB
WS-X6408A-GBIC	1p1q4t	WRR	1p2q2t	WRR		73 KB	439 KB
WS-X6416-GBIC		WRR					
WS-X6416-GE-MT		WRR					
WS-X6316-GE-TX		WRR					
WS-X6148-GE-TX	1q2t	WRR			1.4 MB	185 KB	1.2 MB
WS-X6148V-GE-TX							
WS-X6148-GE-45AF							

表 45-5　10 ギガビット イーサネット モジュール

モジュール	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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	198 MB	108 MB	90 MB

表 45-5　10 ギガビット イーサネット モジュール （続き）

モジュール	入力キューおよびドロップしきい値	入力キュースケジューラ	出力キューおよびドロップしきい値	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
DFC3 を搭載した WS-X6704-10GE	8q8t	WRR	1p7q8t	DWRR	16 MB	2 MB	14 MB
CFC を搭載した WS-X6704-10GE	1q8t	WRR					
WS-X6502-10GE	1p1q8t	WRR	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.45-27）
- 「PFC QoS がイネーブルの場合のデフォルト値」（P.45-28）
- 「PFC QoS がディセーブルの場合のデフォルト値」（P.45-42）

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 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 CoS から初期内部 DSCP へのマップ（受信 CoS 値から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

機能	デフォルト値
受信 IP precedence から初期内部 DSCP へのマップ（受信 IP precedence 値から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 から出力 CoS へのマップ（最終内部 DSCP から設定された出力 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 マップからマークダウンされた DSCP	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。

- 「受信キュー サイズの割合」（P.45-28）
- 「送信キュー サイズの割合」（P.45-29）
- 「帯域幅割り当て比率」（P.45-29）
- 「デフォルトのドロップしきい値の割合および CoS 値マッピング」（P.45-29）

（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 サイズの割合

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%
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 サイズの割合

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%
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	10:90
8q8t	10:0:0:0:0:0:0:90
1p3q8t	22:33:45
1p7q8t	22:33:45:0:0:0:0
1p2q1t	100:255
2q2t、**1p2q2t**、および **1p2q1t**	5:255
1p3q1t	100:150:255

デフォルトのドロップしきい値の割合および CoS 値マッピング

次の表に、キュー タイプ別のデフォルトのドロップしきい値と CoS 値マッピングを示します。

- 「1q4t 受信キュー」（P.45-30）
- 「1p1q4t 受信キュー」（P.45-32）
- 「1p1q0t 受信キュー」（P.45-32）
- 「1p1q8t 受信キュー」（P.45-33）
- 「1q8t 受信キュー」（P.45-34）

- 「2q8t 受信キュー」（P.45-35）
- 「8q8t 受信キュー」（P.45-35）
- 「2q2t 送信キュー」（P.45-37）
- 「1p2q2t 送信キュー」（P.45-37）
- 「1p3q8t 送信キュー」（P.45-38）
- 「1p7q8t 送信キュー」（P.45-40）
- 「1p3q1t 送信キュー」（P.45-41）
- 「1p2q1t 送信キュー」（P.45-41）

1q2t 受信キュー

次の表に、**mls qos** および **mls qos trust cos** を設定する場合のデフォルト値を示します。

機能			デフォルト値
標準受信キュー	しきい値 1	CoS	0、1、2、3、4
		テールドロップ	80%
		WRED ドロップ	非サポート
	しきい値 2	CoS	5、6、7
		テールドロップ	100%（設定はできません）
		WRED ドロップ	非サポート

1q4t 受信キュー

次の表に、**mls qos** および **mls qos trust cos** を設定する場合のデフォルト値を示します。

機能			デフォルト値
標準受信キュー	しきい値 1	CoS	0 および 1
		テールドロップ	50%
		WRED ドロップ	非サポート
	しきい値 2	CoS	2 および 3
		テールドロップ	60%
		WRED ドロップ	非サポート
	しきい値 3	CoS	4 および 5
		テールドロップ	80%
		WRED ドロップ	非サポート
	しきい値 4	CoS	6 および 7
		テールドロップ	100%
		WRED ドロップ	非サポート

1p1q4t 受信キュー

機能			デフォルト値
標準受信キュー	しきい値 1	CoS	0 および 1
		テールドロップ	50%
		WRED ドロップ	非サポート
	しきい値 2	CoS	2 および 3
		テールドロップ	60%
		WRED ドロップ	非サポート
	しきい値 3	CoS	4
		テールドロップ	80%
		WRED ドロップ	非サポート
	しきい値 4	CoS	6 および 7
		テールドロップ	100%
		WRED ドロップ	非サポート
完全優先受信キュー		CoS	5
		テールドロップ	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
	テールドロップ	100%（設定はできません）
	WRED ドロップ	非サポート
完全優先受信キュー	CoS	5
	テールドロップ	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	しきい値 1	CoS	0
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 3	CoS	2
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：80%
	しきい値 4	CoS	3
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：80%
	しきい値 5	CoS	4
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：60%、ハイ：90%
	しきい値 6	CoS	6
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：60%、ハイ：90%
	しきい値 7	CoS	7
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
完全優先受信キュー		CoS	5
		テールドロップ	100%（設定はできません）

1q8t 受信キュー

次の表に、**mls qos** および **mls qos trust cos** を設定する場合のデフォルト値を示します。

機能			デフォルト値
標準受信キュー	しきい値 1	CoS	0
		テールドロップ	50%
		WRED ドロップ	非サポート
	しきい値 2	CoS	なし
		テールドロップ	50%
		WRED ドロップ	非サポート
	しきい値 3	CoS	1、2、3、4
		テールドロップ	60%
		WRED ドロップ	非サポート
	しきい値 4	CoS	なし
		テールドロップ	60%
		WRED ドロップ	非サポート
	しきい値 5	CoS	6 および 7
		テールドロップ	80%
		WRED ドロップ	非サポート
	しきい値 6	CoS	なし
		テールドロップ	80%
		WRED ドロップ	非サポート
	しきい値 7	CoS	5
		テールドロップ	100%
		WRED ドロップ	非サポート
	しきい値 8	CoS	なし
		テールドロップ	100%
		WRED ドロップ	非サポート

2q8t 受信キュー

次の表に、**mls qos** および **mls qos trust cos** を設定する場合のデフォルト値を示します。

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）	しきい値 1	CoS	0 および 1
		テールド ロップ	70%
		WRED ドロップ	非サポート
	しきい値 2	CoS	2 および 3
		テールド ロップ	80%
		WRED ドロップ	非サポート
	しきい値 3	CoS	4
		テールド ロップ	90%
		WRED ドロップ	非サポート
	しきい値 4	CoS	6 および 7
		テールド ロップ	100%
		WRED ドロップ	非サポート
	しきい値 5 ～ 8	CoS	なし
		テールド ロップ	100%
		WRED ドロップ	非サポート
標準受信キュー 2 （ハイ プライオリティ）	しきい値 1	CoS	5
		テールド ロップ	100%
		WRED ドロップ	非サポート
	しきい値 2 ～ 8	CoS	なし
		テールド ロップ	100%
		WRED ドロップ	非サポート

8q8t 受信キュー

次の表に、**mls qos** および **mls qos trust cos** または **mls qos trust dscp** を設定する場合のデフォルト値を示します。

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）	しきい値 1	CoS	0 および 1
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	2 および 3
		テールドロップ	ディセーブル、80%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：80%
	しきい値 3	CoS	4
		テールドロップ	ディセーブル、90%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：90%
	しきい値 4	CoS	6 および 7
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%
	しきい値 5 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：50%、ハイ：100%
標準受信キュー 2 ～ 7 （中間プライオリティ）	しきい値 1 ～ 8	CoS	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	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）	しきい値 1	CoS	5
		テールドロップ	イネーブル、100%
		WRED ドロップ	ディセーブル、ロー：100%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		テールドロップ	イネーブル、100%
		WRED ドロップ	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）	しきい値 1	CoS	0 および 1
		テールド ロップ	80%
		WRED ドロップ	非サポート
	しきい値 2	CoS	2 および 3
		テールド ロップ	100%
		WRED ドロップ	非サポート
標準送信キュー 2 （ハイ プライオリティ）	しきい値 1	CoS	4 および 5
		テールド ロップ	80%
		WRED ドロップ	非サポート
	しきい値 2	CoS	6 および 7
		テールド ロップ	100%
		WRED ドロップ	非サポート

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）	しきい値 1	CoS	0 および 1
		テールド ロップ	非サポート
		WRED ドロップ	ロー：40%、ハイ：70%
	しきい値 2	CoS	2 および 3
		テールド ロップ	非サポート
		WRED ドロップ	ロー：70%、ハイ：100%

機能			デフォルト値
標準送信キュー 2 （ハイ プライオリティ）	しきい値 1	CoS	4
		テールド ロップ	非サポート
		WRED ド ロップ	ロー：40%、ハイ：70%
	しきい値 2	CoS	6 および 7
		テールド ロップ	非サポート
		WRED ド ロップ	ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テールド ロップ	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）	しきい値 1	CoS	0
		テールド ロップ	ディセーブル、70%
		WRED ド ロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		テールド ロップ	ディセーブル、100%
		WRED ド ロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3	CoS	なし
		テールド ロップ	ディセーブル、100%
		WRED ド ロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 4	CoS	なし
		テールド ロップ	ディセーブル、100%
		WRED ド ロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 5 ～ 8	CoS	なし
		テールド ロップ	ディセーブル、100%
		WRED ド ロップ	イネーブル、ロー：50%、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）	しきい値 1	CoS	2
		テールド ロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	3 および 4
		テールド ロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		テールド ロップ	ディセーブル、100%
		WRED ドロップ	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）	しきい値 1	CoS	6 および 7
		テールド ロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		テールド ロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テールド ロップ	100%（設定はできません）

1p7q8t 送信キュー

次の表に、**mls qos** および **mls qos trust cos** または **mls qos trust dscp** を設定する場合のデフォルト値を示します。

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）	しきい値 1	CoS	0
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	1
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 2 （中間プライオリティ）	しきい値 1	CoS	2
		テールドロップ	ディセーブル、70%
		WRED ドロップ	イネーブル、ロー：40%、ハイ：70%
	しきい値 2	CoS	3 および 4
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 3 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 3 （中間プライオリティ）	しきい値 1	CoS	6 および 7
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
	しきい値 2 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	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 （中間プライオリティ）	しきい値 1 ～ 8	CoS	なし
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：100%、ハイ：100%
完全優先送信キュー		CoS	5
		テールドロップ	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）	しきい値 1	CoS	0 および 1
		テールドロップ	ディセーブル、100%
		WRED ドロップ	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）	しきい値 1	CoS	2、3、4
		テールドロップ	ディセーブル、100%
		WRED ドロップ	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）	しきい値 1	CoS	6 および 7
		テールドロップ	ディセーブル、100%
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テールドロップ	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）	しきい値 1	CoS	0、1、2、3
		テールドロップ	非サポート
		WRED ドロップ	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）	しきい値 1	CoS	4、6、7
		テールド ロップ	非サポート
		WRED ドロップ	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テールド ロップ	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 ドロップしきい値の割合	すべてのしきい値を 100% に設定
送信キュー ドロップしきい値の割合	すべてのしきい値を 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 値およびドロップしきい値のマッピング	ロー プライオリティ キューにマップされたすべての CoS 値。

（注）　mls qos だけをイネーブルにして、信頼の設定を行わない場合、キュー 1p1q4t、1q2t、1q4t、1q8t、2q8t、8q8t または 1p7q8t のデフォルト値は、PFC QoS がディセーブルの場合の値と同じです。

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」（P.45-43）
- 「PFC の注意事項」（P.45-44）
- 「クラス マップ コマンドの制約事項」（P.45-45）
- 「ポリシー マップ コマンドの制約事項」（P.45-45）
- 「ポリシー マップ クラス コマンドの制約事項」（P.45-46）
- 「CIR および PIR レート値に対してサポートされる粒度」（P.45-46）
- 「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」（P.45-46）

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。
- **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。
- **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。
- PFC QoS では、IPv4 および IPv6 トラフィック用の **setdscp** および **set precedence** ポリシー マップ クラス コマンドがサポートされます。
- 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 Data Export（NDE; NetFlow データ エクスポート）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。
- 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ドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップ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ドロップ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**

PFC の注意事項

- PFC の全バージョンにより、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 をサポートします。
- 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。
- PFC 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。
- PFC 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を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）演算子の両方を設定した場合は、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。
- IPv6 トラフィックには、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。
- 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、PFC 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 代行受信
  - Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）
  - ネットワーク アドレス変換（NAT）
- ARP 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。
- PFC は、MSFC 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。
- PFC は、MSFC 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。
- 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。

クラス マップ コマンドの制約事項

- 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 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 Mbps）	65536（64 Kb）
4194305 ～ 8388608（8 Mbps）	131072（128 Kb）
8388609 ～ 16777216（16 Mbps）	262144（256 Kb）
16777217 ～ 33554432（32 Mbps）	524288（512 Kb）
33554433 ～ 67108864（64 Mbps）	1048576（1 Mb）
67108865 ～ 134217728（128 Mbps）	2097152（2 Mb）
134217729 ～ 268435456（256 Mbps）	4194304（4 Mb）
268435457 ～ 536870912（512 Mbps）	8388608（8 Mb）
536870913 ～ 1073741824（1 Gps）	16777216（16 Mb）
1073741825 ～ 2147483648（2 Gps）	33554432（32 Mb）
2147483649 ～ 4294967296（4 Gps）	67108864（64 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 6 MSb[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 6 MSb[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 = 最上位ビット

PFC QoS の設定

ここでは、Cisco 7600 シリーズ ルータ上で PFC QoS を設定する手順について説明します。

- 「PFC QoS のグローバルなイネーブル化」（P.45-49）
- 「DSCP 透過性の設定」（P.45-50）
- 「信頼状態の設定」（P.45-50）
- 「queueing-only モードのイネーブル化」（P.45-51）

- 「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」（P.45-51）
- 「レイヤ 2 LAN ポートでの VLAN ベース PFC QoS のイネーブル化」（P.45-52）
- 「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」（P.45-53）
- 「名前付き集約ポリサーの作成」（P.45-54）
- 「PFC QoS ポリシーの設定」（P.45-56）
- 「PFC による出力 DSCP 変換の設定」（P.45-74）
- 「IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定」（P.45-76）
- 「DSCP 値マッピングの設定」（P.45-78）
- 「イーサネット LAN ポートおよび OSM 入力ポートの信頼状態の設定」（P.45-82）
- 「入力 LAN ポート CoS 値の設定」（P.45-83）
- 「標準キューのドロップしきい値の割合設定」（P.45-84）
- 「QoS ラベルのキューおよびドロップしきい値へのマッピング」（P.45-89）
- 「標準送信キュー間での帯域幅の割り当て」（P.45-99）
- 「1p1q0t および 1p1q8t ポートでの受信キュー サイズ比の設定」（P.45-100）
- 「LAN ポート送信キューのサイズ比の設定」（P.45-101）

（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`	ルータで PFC QoS をグローバルにイネーブルにします。
	`Router(config)# no mls qos`	ルータで 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#
```

DSCP 透過性の設定

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)# **no mls qos rewrite ip dscp**	ルータ出力で 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**	ルータ出力で 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 [**ipv6**]	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 バイトを保持する例を示します。

```
Router# configure terminal
Router(config)# no mls qos rewrite ip dscp
Router(config)# end
Router#
```

信頼状態の設定

内部再循環パス上の信頼状態をイネーブルまたは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 **mls qos recirc untrust** コマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **no mls qos recirc untrust**	内部再循環パス上の信頼状態をディセーブルにします。
	Router(config)# **mls qos recirc untrust**	内部再循環パス上の信頼状態を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 [**ipv6**]	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 バイトを保持する例を示します。

```
Router# configure terminal
Router(config)# no mls qos recirc untrust
Router(config)# end
Router#
```

queueing-only モードのイネーブル化

ルータで 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`	ルータで queueing-only モードをイネーブルにします。
	`Router(config)# no mls qos queueing-only`	ルータで PFC QoS をグローバルにディセーブルにします。 （注）　queueing-only モードを個別にディセーブルにすることはできません。
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 [ipv6]`	設定を確認します。

queueing-only モードをイネーブルにする場合、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）　ルータ 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

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）
- PFC QoS は、DFC3 が搭載されているときに VLAN ベースの QoS をサポートします。
- 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 マップを対応付けることができます。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 に対応付けられたポリシー 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 に対応付けられません。

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、ポート FastEthernet 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に対してだけ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、ポート FastEthernet 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。
- 集約ポリサーを IPv6 トラフィックに適用できます。
- ポリシングでは、レイヤ 2 フレーム 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.45-42）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。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：10 Gbps（10000000000 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 32 MB（32000000 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。
  - 最小値 : 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）
  - 最大 : 10 Gbps（10000000000 と入力）
- （任意）一致するインプロファイル 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ドロップするには、**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。

  - 一致したアウトオブプロファイル 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、一致するアウトオブプロファイル 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。
  - 一致したアウトオブプロファイル 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、一致したアウトオブプロファイル 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ドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップ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ドロップ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、アウトオブプロファイル 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。

- 「PFC QoS ポリシー設定作業の概要」（P.45-57）
- 「MAC ACL の設定」（P.45-58）
- 「QoS フィルタリングに対する ARP ACL の設定」（P.45-62）
- 「クラス マップの設定」（P.45-62）
- 「クラス マップの設定の確認」（P.45-65）
- 「ポリシー マップの設定」（P.45-65）
- 「ポリシー マップの設定の確認」（P.45-72）
- 「インターフェイスへのポリシー マップの対応付け」（P.45-72）

（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）　帯域利用率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対応付けられます。

- **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	Yes： 1 ～　99 1300 ～ 1999	Yes： 100 ～　199 2000 ～ 2699	Yes
IPv6	—	Yes（名前付き）	Yes
MAC レイヤ	No	No	Yes
ARP	No	No	Yes

  - PFC 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。
  - PFC は ARP ACL をサポートします。

（注）　- PFC は IP ACL を ARP トラフィックに適用しません。

- ARP 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。

  - PFC は IPX ACL をサポートしません。PFC 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。
  - 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 を除き、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/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html
  - 第 35 章「ネットワーク セキュリティの設定」の ACL の詳細については、Cisco 7600 シリーズ ルータを参照してください。
- **class-map**（任意）：**class-map** コマンドを入力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。

- 「プロトコル独立型 MAC ACL フィルタリングの設定」（P.45-58）
- 「VLAN ベースの MAC QoS フィルタリングのイネーブル化」（P.45-59）
- 「MAC ACL の設定」（P.45-60）

（注） VLAN ACL（VACL）で MAC ACL を使用できます。詳細については、第 37 章「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

PFC 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、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、IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に MAC ACL が適用されます。

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は、出力 IP ACL を適用できません。

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 PFC3BXL または PFC3CXL によってハードウェアでブリッジングされる、またはレイヤ 3 スイッチングされた場合、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 または MSFC4（RSP720 の一部）によってソフトウェアでルーティングされた場合、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、インターフェイス GigabitEthernet 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、インターフェイス GigabitEthernet 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

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。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、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。

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 MAC ACL を設定できます。

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 コントロール 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。

- **ipx-arpa** および **ipx-non-arpa** キーワードがサポートされています。
- **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。
- MAC ACL の VLAN ベースの QoS フィルタリング用の **vlan** キーワードを、グローバルにイネーブルまたはディセーブルにすることができます（デフォルトではディセーブル）。
- MAC アドレスは、ドット付き 16 進表記の 3 つの 4 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 4 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 として入力できます）。
- EtherType および EtherType マスクを 16 進値で入力できます。
- protocol パラメータなしの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。
- 新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することができません。
- 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; メンテナンス オペレーション プロトコル）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; ローカルエリア トランスポート）
  - 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 - 不正な形式、無効、または意図的に壊された 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）
- PFC は IP ACL を ARP トラフィックに適用しません。
- PFC が搭載されている場合、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。

ARP トラフィック（EtherType 0x0806）をフィルタリングする名前付き ACL を QoS に設定できます。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 コントロール 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。

- ここでは、PFC 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 CLI 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、入力した順序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。
- リストの末尾に **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。
- 新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することができません。

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.45-62）
- 「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.45-63）
- 「クラス マップでのフィルタリングの設定」（P.45-64）

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。

- 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。
- PFC 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を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）」演算子の両方を設定した場合は、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。
- PFC QoS では、IPv4 トラフィック用の **match protocol ip** コマンドがサポートされます。
- PFC QoS は、**match cos**、**match any**、**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。
- Cisco 7600 シリーズ ルータは、インターフェイスにポリシー マップが付加されないかぎり、サポートされていないコマンドが使用されているかどうかを検出しません。
- 出力 QoS の IP precedence または DSCP に基づいたフィルタリングは、受信 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） この章では、次の ACL に関する内容を説明します。

- 「MAC ACL の設定」（P.45-58）
- 「QoS フィルタリングに対する ARP ACL の設定」（P.45-62）

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.45-57）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、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 トラフィックのみ）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、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。
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、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、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対応付けできるポリシー 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.45-65）
- 「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.45-66）
- 「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.45-66）
- 「ポリシー マップ クラス アクションの設定」（P.45-66）

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。

- 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。
- 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かぎり、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 つ以上のポリシー 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 は **set mpls** または **set qos-group** ポリシー マップ クラス コマンドをサポートしません。
- PFC QoS は、IPv4 トラフィックに対して **set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドをサポートします。
  - 非 IP トラフィック上で **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。
  - **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。
- PFC QoS では、IPv4 および IPv6 トラフィック用の **setdscp** および **set 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 クラスで、次の 3 つすべてを実行することができません。

- **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、信頼できないトラフィックを **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.45-67）
- 「ポリシー マップ クラスの信頼状態の設定」（P.45-67）
- 「ポリシー マップ クラスのポリシングの設定」（P.45-68）

ポリシー マップ クラス マーキングの設定

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。

信頼できないトラフィックに対するポリシー 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。

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 マップを対応付けることができません。

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 マップが対応付けられない限り、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.45-68）
- 「インターフェイス別ポリサーの設定」（P.45-69）

（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。
- 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。
- 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ドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップ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ドロップをサポートしません。

- IPv6 トラフィックには、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。
- ポリシングでは、レイヤ 2 フレーム 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.45-42）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は、次の点に注意してください。
  - 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。IP トラフィックと MAC トラフィックの両方で **mask src-only** キーワードがサポートされています。
  - 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、各送信元アドレスへのすべてのトラフィックに適用されます。IP トラフィックと MAC トラフィックの両方で **mask dest-only** キーワードがサポートされています。
  - 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。
  - 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 Data Export（NDE; NetFlow データ エクスポート）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。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：10 Gbps（10000000000 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 32 MB（32000000 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）
  - 最大：10 Gbps（10000000000 と入力）
- （任意）一致するインプロファイル 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 値をマーキングするか、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 値をマーキングします。**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ドロップするには、**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。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル 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。

  - 一致したすべてのアウトオブプロファイル 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。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル 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。

– 一致したすべてのアウトオブプロファイル 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 マップで追加クラスを作成するには、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 マップの対応付け

ポリシー マップをインターフェイスに付加するには、次の作業を実行します。

	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。

	コマンド	目的
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対応付けます。
	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対応付ける場合は、次の点に注意してください。

- EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。
- PFC QoS は、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）上だけで、**output** キーワードをサポートします。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対応付けら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 マップを対応付けることができません。
- **output** キーワードを使用して対応付けられたポリシーの 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対応付けられたポリシーの 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。
- 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ドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップ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ドロップをサポートしません。

次に、ポリシー マップ **pmap1** をポート FastEthernet 5/36 に対応付ける例を示します。

```
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#
```

PFC による出力 DSCP 変換の設定

ここでは、PFC 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.45-74）
- 「インターフェイスへの出力 DSCP 変換マップの対応付け」（P.45-75）

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 output_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 変換マップ表示では、マークダウンされた DSCP 値がマトリクスの本体に表示されます。元の DSCP 値の 1 桁目が d1 列に表示され、2 桁目が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 変換マップの対応付け

出力 DSCP 変換マップをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **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*	出力 DSCP 変換マップをインターフェイスに対応付けます。
	Router(config-if)# **no mls qos dscp-mutation** *mutation_map_name*	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、出力 DSCP 変換マップ mutmap1 をファスト イーサネット ポート 5/36 に対応付ける例を示します。

```
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

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 変換がサポートされています（サポート対象モジュールについては、「IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用」（P.45-78）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、入力ドロップしきい値内および任意の 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.45-76）
- 「入力 CoS 変換マップの設定」（P.45-77）
- 「IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用」（P.45-78）

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。

- 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。
- WS-X6704-10GE、WS-X6748-SFP、WS-X6724-SFP、および WS-X6748-GE-TX スイッチング モジュールの入力 CoS 変換がサポートされています。
- 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 および 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、37 ～ 48）
- 入力 CoS 変換の設定エラーを回避するために、メンバー ポートのすべてが入力 CoS 変換をサポートしている、またはメンバー 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 のメンバー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 のすべてのメンバー ポートのポート グループに適用されます。任意のメンバー 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 番めの EtherChannel のメンバーである場合、入力 CoS 変換の設定は、2 番めのポートチャネル インターフェイスおよび 2 番めの EtherChannel のすべてのメンバー ポートのポート グループに適用されます。2 番めの EtherChannel の任意のメンバー ポートが入力 CoS 変換をサポートできない場合、1 番めの EtherChannel 上の設定がエラーになります。1 番めの EtherChannel のメンバー ポートがあるポート グループ内の非メンバー ポートで、設定が行われた場合、この設定は非メンバー 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、メンバー 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ー ポートがある他の EtherChannel のメンバー ポートを含むポート グループ内のポートをメンバー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ー 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ーがある EtherChannel のメンバー 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ー 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ー 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* Router(config)# **no mls qos map cos-mutation** *map_name*	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。 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 変換マップを対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **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対応付けます。 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、ポート GigabitEthernet 1/1 に対応付ける例を示します。

```
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手順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.45-78）
- 「受信 IP precedence 値から内部 DSCP 値へのマッピング」（P.45-79）
- 「DSCP マークダウン値の設定」（P.45-80）
- 「内部 DSCP 値から出力 CoS 値へのマッピング」（P.45-81）

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に発生）、**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 値を入力することができます。
- 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 1 つずつ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 表示では、マークダウンされた DSCP 値がマトリクスの本体に表示されます。元の DSCP 値の 1 桁目が d1 カラムに表示され、2 桁目が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 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 の最初の桁の数字は d1 のカラムに、2 番め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 入力ポートの信頼状態の設定

デフォルトでは、すべての入力ポートは信頼できない（untrusted）状態です。イーサネット LAN ポートおよび OSM ポートのすべてに入力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。

入力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 mls qos [ipv6]`	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。

入力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(33)SRC およびそれ以降では、**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しきい値を WS-X6708-10GE ポート上で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.45-90）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のドロップを防ぐには、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、受信キュー廃棄しきい値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のドロップを防ぐには、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。
- **mls qos trust cos** コマンドで設定される IEEE802.1Q 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.45-76）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ポート GigabitEthernet 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 mls qos queuing 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。

	コマンド	目的
ステップ 2	`Router(config-if)# mls qos cos port_cos`	入力 LAN ポートの CoS 値を設定します。
	`Router(config-if)# no mls qos cos port_cos`	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 mls qos 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 の 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 mls qos queuing interface fastethernet 5/24 | include Default COS
  Default COS is 5
Router#
```

標準キューのドロップしきい値の割合設定

ここでは、標準キューのドロップしきい値の割合を設定する手順を説明します。

- 「テールドロップ受信キューの設定」（P.45-85）
- 「WRED ドロップ送信キューの設定」（P.45-86）
- 「WRED ドロップおよびテールドロップ受信キューの設定」（P.45-86）
- 「WRED ドロップおよびテールドロップ送信キューの設定」（P.45-87）
- 「1q4t/2q2t テールドロップしきい値の割合設定」（P.45-88）

（注）

- LAN カードのポートのキュー構造を表示するには、**show mls qos queuing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを入力します。
- **1p1q0t** ポートに、設定変更可能なしきい値はありません。
- **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ドロップしきい値があります。

しきい値を設定する場合、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。

複数のしきい値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しきい値を設定します。
- 2 番めに入力したパーセント値は、2 番めにプライオリティが高いしきい値を設定します。
- 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しきい値を設定します。
- 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しきい値を意味します。

- プライオリティが一番高いしきい値は、常に 100% に設定してください。

WRED ドロップしきい値を設定する場合、次の点に注意してください。

- WRED ドロップしきい値には、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ドロップ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ドロップ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、ドロップされる可能性が高くなります。

テールドロップ受信キューの設定

次のポート タイプには、受信キューにテールドロップしきい値だけがあります。

- **1q2t**
- **1p1q4t**
- **2q8t**
- **1q8t**

ドロップしきい値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**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%}*	受信キューのドロップしきい値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ドロップしきい値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 mls qos queuing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

次に、ポート GigabitEthernet 1/1 について、受信キュー ドロップしきい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)# 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 mls qos queuing 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 ドロップ送信キューの設定

次のポート タイプでは、送信キュー内に WRED ドロップしきい値だけが含まれています。

- **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 ドロップしきい値を設定します。
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED ドロップしきい値に戻します。
ステップ 3	Router(config-if)# **wrr-queue random-detect max-threshold** *queue_id thr1% [thr2%]*	ハイ WRED ドロップしきい値を設定します。
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED ドロップしきい値に戻します。
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 mls qos queuing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

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

WRED ドロップおよびテールドロップ受信キューの設定

次のポート タイプは、受信キューに WRED ドロップおよびテールドロップしきい値の両方があります。

- **8q8t**（受信）
- **1p1q8t**（受信）

ドロップしきい値を設定するには、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)# **rcv-queue threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	テールドロップしきい値を設定します。
	Router(config-if)# **no rcv-queue threshold** [*queue_id*]	デフォルトのテールドロップしきい値に戻します。

	コマンド	目的
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 ドロップしきい値を設定します。
	Router(config-if)# **no rcv-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED ドロップしきい値に戻します。
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 ドロップしきい値を設定します。
	Router(config-if)# **no rcv-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED ドロップしきい値に戻します。
ステップ 5	Router(config-if)# **rcv-queue random-detect** *queue_id*	WRED ドロップしきい値をイネーブルにします。
	Router(config-if)# **no rcv-queue random-detect** [*queue_id*]	テールドロップしきい値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 mls qos queuing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

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

WRED ドロップおよびテールドロップ送信キューの設定

次のポート タイプでは、受信キュー内に WRED ドロップおよびテールドロップしきい値の両方が含まれています。

- **1p3q1t**（送信）
- **1p3q8t**（送信）
- **1p7q8t**（送信）

ドロップしきい値を設定するには、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)# **wrr-queue threshold** *queue_id thr1%* [*thr2% thr3% thr4% thr5% thr6% thr7% thr8%*]	テールドロップしきい値を設定します。
	Router(config-if)# **no wrr-queue threshold** [*queue_id*]	デフォルトのテールドロップしきい値に戻します。
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 ドロップしきい値を設定します。
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED ドロップしきい値に戻します。
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 ドロップしきい値を設定します。
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED ドロップしきい値に戻します。
ステップ 5	Router(config-if)# **wrr-queue random-detect** *queue_id*	WRED ドロップしきい値をイネーブルにします。
	Router(config-if)# **no wrr-queue random-detect** [*queue_id*]	テールドロップしきい値をイネーブルにします。

	コマンド	目的
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 mls qos queuing interface {fastethernet | gigabitethernet} slot/port`	設定を確認します。

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

次に、ポート GigabitEthernet 1/1 について、ロー プライオリティ送信キューのハイ WRED ドロップしきい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)# 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 mls qos queuing 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 テールドロップしきい値の割合設定

次に、**1q4t/2q2t** ポートでの受信キューおよび送信キューのドロップしきい値の関係を示します。

- 受信キュー 1（標準）しきい値 1 = 送信キュー 1（標準ロー プライオリティ）しきい値 1
- 受信キュー 1（標準）しきい値 2 = 送信キュー 1（標準ロー プライオリティ）しきい値 2
- 受信キュー 1（標準）しきい値 3 = 送信キュー 2（標準ハイ プライオリティ）しきい値 1
- 受信キュー 1（標準）しきい値 4 = 送信キュー 2（標準ハイ プライオリティ）しきい値 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ドロップしきい値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ドロップしきい値を設定します。
	`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ドロップしきい値に戻します。

	コマンド	目的
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 queuing 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ドロップしきい値を設定する場合、次の点に注意してください。

- 送信キュー番号およびしきい値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しきい値を意味します。
- しきい値は常に 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 テールドロップしきい値をサポートしません。

次に、ポート GigabitEthernet 2/1 について、受信キュー 1/ しきい値 1、および送信キュー 1/ しきい値 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 mls qos queuing 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ドロップしきい値へのマッピング

ここでは、QoS ラベルをキューおよびドロップしきい値にマッピングする方法について説明します。

（注）　Cisco IOS Software Release 15.0(1)S 以降で、LAN ポートのキュー構造を表示するには、**show mls qos queuing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを入力します。

ここでは、QoS ラベルをキューおよびドロップしきい値にマッピングする方法について説明します。

- 「キューおよびドロップしきい値へのマッピングに関する注意事項および制約事項」（P.45-90）
- 「DSCP ベースのキュー マッピングの設定」（P.45-90）
- 「CoS ベースのキュー マッピングの設定」（P.45-95）

キューおよびドロップしきい値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しきい値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 値をしきい値にマッピングできます。
- 最大 64 個の DSCP 値をしきい値にマッピングできます。
- しきい値 0 は、次のポート タイプの場合、設定変更できない 100% テールドロップしきい値を意味します。
  - **1p1q0t**（受信）
  - **1p1q8t**（受信）
  - **1p3q1t**（送信）
  - **1p2q1t**（送信）
- 標準キューしきい値は、次のポート タイプでテールドロップまたは WRED ドロップしきい値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.45-91）
- 「標準送信キューしきい値への DSCP 値のマッピング」（P.45-93）
- 「送信完全優先キューへの DSCP 値のマッピング」（P.45-94）

（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ています.

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 mls qos queuing interface tengigabitethernet** *slot/port* **| include Queueing Mode**	設定を確認します。

次に、DSCP ベースのキュー マッピングを 10 ギガビット イーサネット ポート 6/1 でイネーブルする例を示します。

```
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 mls qos queuing 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.45-91）
- 「標準受信キューしきい値への DSCP 値のマッピング」（P.45-92）

Trust 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 mls qos queuing interface tengigabitethernet** *slot/port* **| include Trust state**	設定を確認します。

次に、受信した DSCP 値を信頼するように 10 ギガビット イーサネット ポート 6/1 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 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 mls qos queuing interface gigabitethernet 6/1 | include Trust state
  Trust state: trust DSCP
```

標準受信キューしきい値への DSCP 値のマッピング

DSCP 値を標準受信キューしきい値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*]]]]]]]	標準受信キューしきい値に 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 mls qos queuing 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。

- キューおよびしきい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 値をキューおよびしきい値にマッピングできます。
- キューおよびしきい値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、標準受信キューのしきい値 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#
```

次に、設定を確認する例を示します。

```
Router# show mls qos queuing 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#
```

標準送信キューしきい値への DSCP 値のマッピング

標準送信キューしきい値に 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*]]]]]]]	標準送信キューのしきい値に 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 mls qos queuing 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。

- キューおよびしきい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 値をキューおよびしきい値にマッピングできます。
- キューおよびしきい値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/ しきい値 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#
```

次に、設定を確認する例を示します。

```
Router# show mls qos queuing 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*]]]]]]]	DSCP 値を送信完全優先キューにマッピングします。複数の **priority-queue dscp-map** コマンドを入力することで、9 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 mls qos queuing 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#
```

次に、設定を確認する例を示します。

```
Router# show mls qos queuing 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。

- 「標準受信キューしきい値への CoS 値のマッピング」（P.45-95）
- 「標準送信キューしきい値への CoS 値のマッピング」（P.45-96）
- 「完全優先キューへの CoS 値のマッピング」（P.45-97）
- 「1q4t/2q2t LAN ポートのテールドロップしきい値への CoS 値のマッピング」（P.45-98）

標準受信キューしきい値への CoS 値のマッピング

CoS 値を標準受信キューしきい値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*]]]]]]]	標準受信キューしきい値に 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 mls qos queuing interface** *type*[1] *slot/port*	設定を確認します。

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

次に、ポート GigabitEthernet 1/1 に対して、標準受信キューしきい値 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 mls qos queuing 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#
```

標準送信キューしきい値への CoS 値のマッピング

標準送信キューしきい値に 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*]]]]]]]	標準送信キューしきい値に 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 mls qos queuing 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 に関して、標準送信キュー 1/ しきい値 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 mls qos queuing 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 mls qos queuing 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、ポート GigabitEthernet 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 mls qos queuing 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 ポートのテールドロップしきい値への 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 mls qos queuing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを入力します。

1q4t/**2q2t** LAN ポート上では、受信キュー テールドロップしきい値と送信キュー テールドロップしきい値の間に次のような関係があります。

- 受信キュー 1（標準）しきい値 1 = 送信キュー 1（標準ロー プライオリティ）しきい値 1
- 受信キュー 1（標準）しきい値 2 = 送信キュー 1（標準ロー プライオリティ）しきい値 2
- 受信キュー 1（標準）しきい値 3 = 送信キュー 2（標準ハイ プライオリティ）しきい値 1
- 受信キュー 1（標準）しきい値 4 = 送信キュー 2（標準ハイ プライオリティ）しきい値 2

テールドロップしきい値に 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*]]]]]]]	テールドロップしきい値に 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 mls qos queuing interface** *type*[1] *slot/port*	設定を確認します。

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

テールドロップしきい値に CoS 値をマッピングする場合、次の点に注意してください。

- 送信キュー番号としきい値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 つのしきい値があります。
- しきい値にマッピングする、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 に関して、標準送信キュー 1/ しきい値 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 mls qos queuing 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

ルータは次の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 アルゴリズムは割合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帯域幅を割り当てます。

- Deficit Weighted Round Robin DWRR（DWRR）：**1p3q1t**、**1p2q1t**、**1p3q8t**、および **1p7q8t** ポートでサポートされます。DWRR は、送信の際にすべてのロー プライオリティ キューを追跡し、次のラウンドを補正します。
- Weighted Round Robin（WRR; 重み付きラウンドロビン）：他のすべてのポートでサポートされています。WRR では、他のキューが帯域幅を使用していない場合に、キューは割り当てられている以上の帯域幅（最大でポートの総帯域幅まで）を使用できます。

パーセント値または重み値を入力して、帯域幅を割り当てることができます。

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、ポート ハードウェアが設定済み割合または重み値に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` *low_priority_queue_percentage* [*intermediate_priority_queue_percentages*] *high_priority_queue_percentage* または： `Router(config-if)# wrr-queue bandwidth` *low_priority_queue_weight* [*intermediate_priority_queue_weights*] *high_priority_queue_weight* `Router(config-if)# no wrr-queue bandwidth`	標準送信キュー間で帯域幅を割り当てます。 • 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。 • 重み値の有効範囲は 1 ～ 255 です。ポート上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。 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 mls qos queuing interface` *type*[1] *slot/port*	設定を確認します。

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

次に、ポート GigabitEthernet 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 mls qos queuing interface gigabitethernet 1/2 | include bandwidth
WRR bandwidth ratios:    3[queue 1]   1[queue 2]
Router#
```

1p1q0t および 1p1q8t ポートでの受信キュー サイズ比の設定

1p1q0t または **1p1q8t** ポート上で完全優先キューと標準受信キューの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** *standard_queue_weight strict_priority_queue_weight*	完全優先キューと標準受信キューの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 mls qos queuing 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、完全優先トラフィックと標準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、ポート FastEthernet 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 mls qos queuing interface fastethernet 2/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  15[queue 2]
Router#
```

LAN ポート送信キューのサイズ比の設定

送信キュー 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*	複数の送信キュー間の送信キュー サイズ比を設定します。
	Router(config-if)# **no wrr-queue queue-limit**	デフォルトの送信キュー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 mls qos queuing 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。

- 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）。
- 出力完全優先キューを持つポートの場合：
  - リリース 12.2SR 以降では、priority-queue queue-limit インターフェイス コマンドを入力することによって、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）
  - リリース 12.2SR よりも前のリリースと他のモジュールでは、PFC QoS が、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。
- 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、ポート GigabitEthernet 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 mls qos queuing 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、この章内の他の項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.45-102）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」（P.45-102）
- 「アクセス レイヤ内の PC と IP 電話から送信されるトラフィックの分類」（P.45-104）
- 「スイッチ間リンク上でのトラフィック プライオリティ値の受け入れ」（P.45-106）
- 「スイッチ間リンクでのトラフィックの優先付け」（P.45-107）
- 「ポリサーによる PC からのトラフィック量の制限」（P.45-111）

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。このネットワークには、アクセス レイヤとディストリビューション レイヤ間にギガビット イーサネット リンク、ディストリビューション レイヤとコア レイヤ間にギガビットまたは 10 ギガビット イーサネット リンクがあります。

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 Type of Service（ToS; タイプ オブ サービス）または Ethernet 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 の注意事項については、RFC 2597 および RFC 2598 に加えて、シスコが発行している各種の QoS 設計マニュアル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、ルータ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 CoS 値（デフォルトで 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 になります。
  - 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 レイヤ内の PC と IP 電話から送信されるトラフィックの分類

アクセス レイヤ ルータには、IP Phone にデイジーチェーンされた PC が 100Mbps リンク上にあります。ここでは、IP 電話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、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 ルータに送られたときに信頼されます。

IP 電話と PC が接続されているアクセス ルータのポートは、音声 VLAN（VLAN 110）用に設定されています。これは、電話トラフィック（サブネット 10.1.110.0/24）と PC トラフィック（サブネット 10.1.10.0/24）を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 コントロール リスト（ACL）設定を示します。

IP 電話からの音声トラフィックを識別（VVLAN）

```
ip access-list extended CLASSIFY-VOICE
    permit udp 10.1.110.0 0.0.0.255 any range 16384 32767
```

IP 電話からの音声シグナリング トラフィックを識別（VVLAN）

```
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 トラフィックを識別（DVLAN）

```
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 ポリシーはポートまたは VLAN インターフェイスに適用できますが、出力サービス ポリシーは VLAN インターフェイスだけに適用できます。この例では、PC および IP Phone が接続されている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 ポリシーが正しく設定され、IP 電話と PC の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 mls qos queuing 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#
```

スイッチ間リンク上でのトラフィック 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。

着信プライオリティ設定を信頼するうえで有効であると考えられるポート例は、IP Phone/その他の IP 音声デバイス、ビデオ デバイス、または任意のデバイス（ユーザが既定の有効なプライオリティによるフレーム送信を信頼しているデバイス）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、ルータ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後は、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 mls qos queuing 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、ルータ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、加入過多が発生した場合に、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 レイヤ内の PC と IP 電話から送信されるトラフィックの分類」（P.45-104）および「スイッチ間リンク上でのトラフィック プライオリティ値の受け入れ」（P.45-106）で説明したマーキングおよび信頼アクションでは、加入過多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は提供できません。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。

Cisco 7600 シリーズ ルータ イーサネット モジュールは、1 つのキューから最大 8 つのキュー アーキテクチャの範囲で、各種のキュー構造をサポートしています。キュー構造は、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。スイッチはキュー構造を使用して、差別化サービスのこのようなレーンを提供しています。

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 しきい値を保持します（8t、ここでは説明しません）。

Cisco 7600 シリーズ ルータ イーサネット モジュールには入力キュー構造もありますが、あまり使用されません。スイッチ ファブリック内では輻輳が発生しないと考えられるためです（この例には、含まれません）。

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 値に対応付けてから、CoS とキューのマッピングを使用して、CoS 値をキューに対応付けます。

パケットがルータに入力されると、QoS の設定に応じて、そのパケットが分類されて設定済み DSCP 値の 1 つがマーキングされるか（「アクセス レイヤ内の PC と IP 電話から送信されるトラフィックの分類」（P.45-104）を参照）、パケットの着信 DSCP 値が信頼されてそのまま使用されます（「スイッチ間リンク上でのトラフィック プライオリティ値の受け入れ」（P.45-106）を参照）。これらのオプションに応じて、ルータ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 mls qos queuing 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>
```

（注）　Cisco IOS Software Release 15.0(1)S 以降で、LAN ポート上の設定を確認するには、**show mls qos queuing interface** コマンドを使用します。

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、しきい値 2
PC SAP	25	3	キュー 2、しきい値 2
その他のトラフィック	0	0	キュー 1、しきい値 1

ルータ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）にはそれぞれドロップしきい値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 値に数種類のドロップしきい値を割り当て、異なるプライオリティを区別することができます。しきい値は、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ドロップ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% のしきい値を使用できます。

DCSP-to-CoS および CoS-to-queue マッピングを変更して、特定のネットワークのニーズに適応させることができます。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、「標準送信キューしきい値への CoS 値のマッピング」（P.45-96）を参照してください。

ルータ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。

Cisco 7600 シリーズ ルータでは、LAN スイッチング モジュールで使用されるスケジューリング アルゴリズムは Strict Priority（SP; 完全優先）キューイングおよび 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。SP 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 などの高帯域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 つのキューが存在し、それぞれの重み値が 22:33:45（デフォルト設定）である場合、キュー 1 が利用可能な帯域幅の 22% だけを使用し、キュー 2 は 33%、キュー 3 は 45% を使用します。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（電話とそれ以外、PC とそれ以外）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。

トラフィックのマッピング後は、完全優先キューを設定する必要がありません。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.45-99）を参照）。

（注） Cisco IOS Software Release 15.0(1)S 以降で、LAN ポート上でパケット損失が発生した場所を特定するには、**show mls qos queuing interface** コマンドを使用します。

ルータが加入過多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 ドロップが最小限で行われているのを確認することです。パケット損失が発生した場所を特定するには、**show queueing interface** コマンドを使用します。このコマンドでは、各キューでドロップ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。Cisco 7600 シリーズ ルータ イーサネット ポートでサポートされているレート制限方法は、ポリシングと呼ばれます。ポリシングは PFC ハードウェアに実装され、パフォーマンスに影響することはありません。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かぎり、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、ドロップするか、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 Quality of Service 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 レイヤ内の PC と IP 電話から送信されるトラフィックの分類」（P.45-104）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 しきい値を超えるすべてのトラフィックはドロップされます。

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、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 レートを超えていない場合に送信される CLASSIFY-OTHER パケットに対してポリサーが実行するアクションを定義します。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ドロップされます。

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 720 のフォワーディング エンジンは、デュアルレートのポリサーもサポートしており、CIR および PIR の両方の粒度を提供しています。

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対応付けます。

```
interface FastEthernet5/1
service-policy input IPPHONE-PC
```

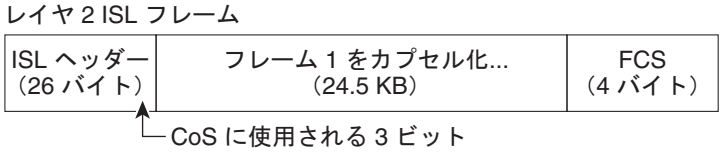
ポリシングの動作をモニタするには、次のコマンドを使用します。

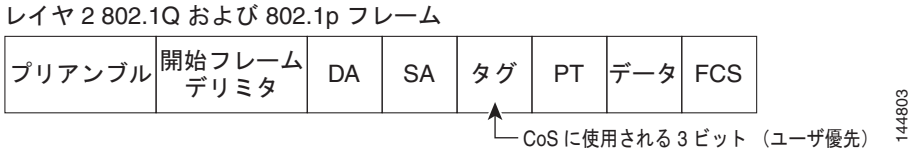
```
show policy-map interface fastethernet 5/1
show class-map
show mls qos ip fastethernet 5/1
```

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際に使用するストレージ領域。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。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）*：ISL、802.1Q、または 802.1p ヘッダーのいずれかの 3 ビットで伝送されるレイヤ 2 QoS ラベル。CoS 値は 0 ～ 7 の範囲の値です。

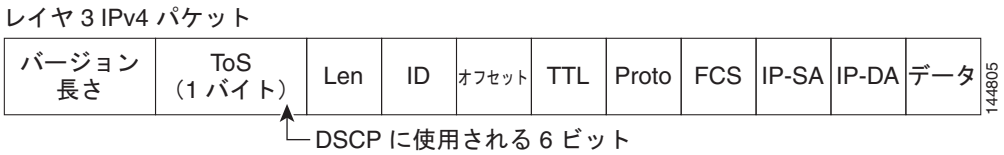




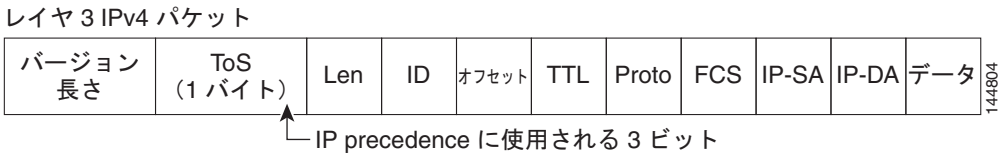
- *分類*：QoS をマーキングするトラフィックを選択する処理です。
- *輻輳回避*は、プライオリティの高いレイヤ 2 CoS 値を持つレイヤ 2 フレームのために、入力 LAN ポートおよび出力 LAN ポートの容量を PFC QoS で確保しておく処理です。PFC QoS では、レイヤ 2 CoS 値ベースのドロップしきい値によって輻輳回避を実行します。ドロップしきい値は、

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ドロップされ、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。

- *Diffserv コードポイント*（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。



- *フレーム*は、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。



- *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 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ドロップが可能になります。
- *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。
- *しきい値*：トラフィックをドロップする上限となる、キュー容量の割合です。
- *Type of Service*（ToS; タイプ オブ サービス）：パケットに適用されるプライオリティ値を指定するのに使用される IP バージョン 4 ヘッダーの 1 バイト フィールド。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比率

CHAPTER 46

PFC QoS 統計データ エクスポートの設定

この章では、Cisco 7600 シリーズ ルータの 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。

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.46-1）
- 「PFC QoS 統計データ エクスポートのデフォルト設定」（P.46-2）
- 「PFC QoS 統計データ エクスポートの設定」（P.46-2）

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使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。Cisco 7600 シリーズ ルータ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 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 46-1 に、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 46-1　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.46-2）
- 「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.46-3）
- 「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.46-4）
- 「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.46-5）
- 「PFC QoS 統計データ エクスポート間隔の設定」（P.46-7）
- 「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.46-8）
- 「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.46-9）

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、ポート FastEthernet 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#
```

名前付き集約でイネーブルにすると、PFC QoS 統計データ エクスポート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
- 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

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ルータ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 46-2 に、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を示します。

表 46-2　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確保
mail	メール システム	local1	ローカルで使用するために確保
daemon	システム デーモン	local2	ローカルで使用するために確保
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確保
syslog	内部 Syslog メッセージ	local4	ローカルで使用するために確保
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確保
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確保
uucp	uucp サブシステム	local7	ローカルで使用するために確保

表 46-3 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 46-3　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	クリティカルな状態
err	3	エラー
warning	4	警告

表 46-3　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 （続き）

重大度パラメータ		
名前	**番号**	**定義**
notice	5	正常だが重大な状態
info	6	情報
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 47

Label Switched Multicast（LSM）Multicast Label Distribution Protocol（MLDP）based Multicast VPN（MVPN）サポート

Label Switched Multicast（LSM）機能により、サービス プロバイダーは既存の IPv4 MPLS バックボーン ネットワークを IPv4 マルチキャスト サービス用に拡張できます。デフォルトでは、MPLS は各パケットの内側ラベルに対して外側ラベルを作成します。この機能は、単一の内側ラベルに対して複数の外側ラベルを作成するようにデフォルト機能を拡張します。IPv4 マルチキャスト サービスには、Point-to-Multipoint（P2MP; ポイントツーマルチポイント）および Multipoint-to-Multipoint（M2M; マルチポイントツーマルチポイント）パケット送信が含まれます。P2MP パケット送信は、Resource Reservation Protocol（RSVP; リソース予約プロトコル）P2MP – Traffic Engineering（P2MP-TE; P2MP- トラフィック エンジニアリング）を使用して実装され、M2M パケット送信は、Multicast Label Distribution Protocol（MLDP）を使用して、IPv4 Multicast VPN（MVPN; マルチキャスト VPN）経由で実装されます。パケットは、次の 3 つのタイプのルータを介して送信されます。

- ヘッドエンド ルータ：IP パケットを 1 つまたは複数のラベル付きでカプセル化します。
- 中間ルータ：内側ラベルを外側ラベルに置換します。
- テールエンド ルータ：パケットからラベルを削除します。

LSM は、入力と出力の 2 つのマルチキャスト レプリケーション モードをサポートする、EARL 7 または EARL 7.5 バージョンに基づいたシステムに実装されます。入力モードの場合は入力カードがレプリケーションを実行し、マルチキャスト トラフィック スループットは 20 Gb/ 秒に制限されます。出力レプリケーション モードでは、ファブリックのレプリケーション機能を使用して、パケットのコピーを各ラインカードに配信します。複数のラインカードにレプリケーション プロセスを分散させると、システムのスループットが大きく向上します。Cisco 7600 シリーズ ルータでは、LSM は出力モードで実装されます。

（注） LSM MLDP based MVPN 機能は、ES+ および ES20 ラインカードと、RSP720、SUP720、および RSP720-10GE スーパーバイザでサポートされます。MLDP は、出力レプリケーション対応のすべてのラインカードでサポートされます。

RSVP P2MP-TE の詳細については、http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_p2mp.html を参照してください。

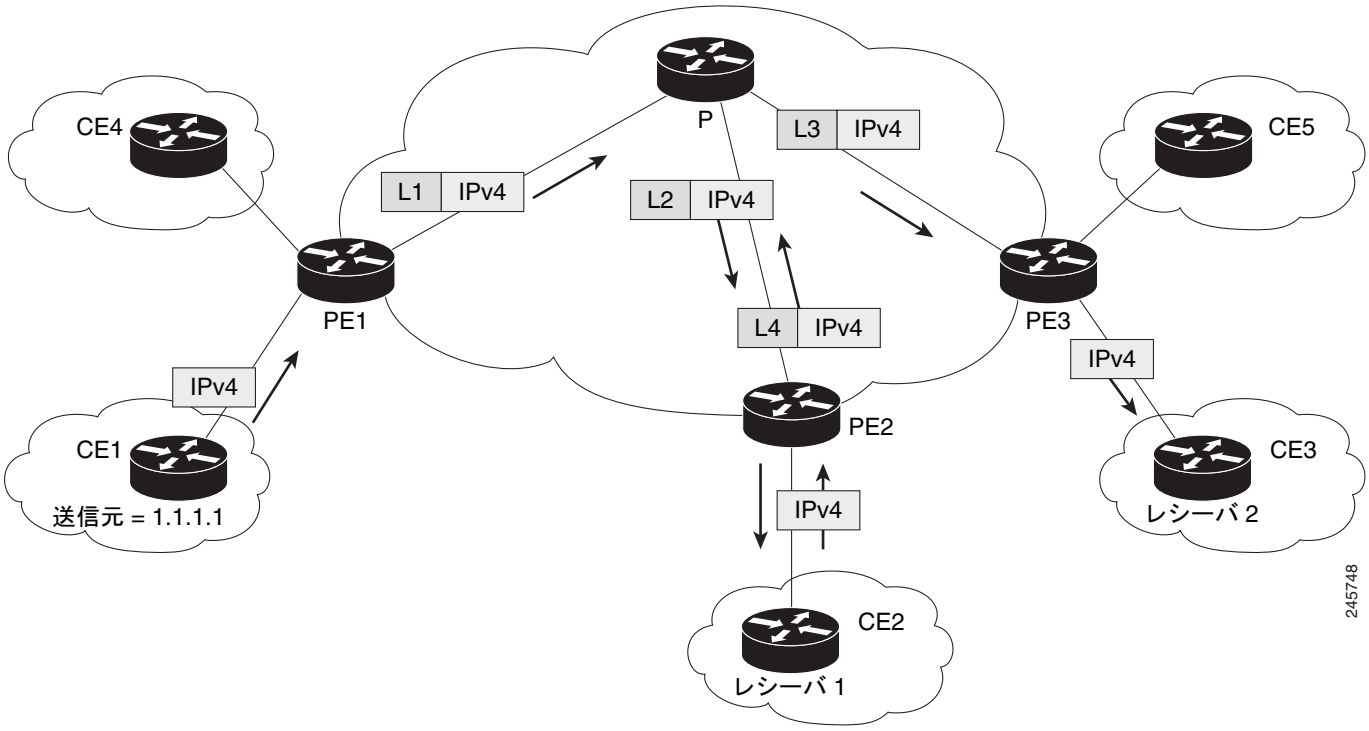
MLDP MVPN の設定

MLDP MVPN の設定により、MPLS を使用した IPv4 マルチキャスト パケット配信をイネーブルにします。この設定では、MPLS ラベルを使用して、デフォルトおよびデータ Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）を構築します。MPLS レプリケーションは、コア ネットワークの転送メカニズムとして使用されます。MLDP MVPN の設定を有効にするには、MPLS MLDP のグローバル設定がイネーブルであることを確認します。

MVPN エクストラネット サポートを設定するには、レシーバ プロバイダー エッジ（PE）ルータにソースの multicast VPN Routing and Forwarding（mVRF; マルチキャスト VPN ルーティングおよび転送）を設定するか、ソース PE にレシーバの mVRF を設定します。MLDP MVPN は、イントラネットとエクストラネットの両方に対してサポートされます。

図 47-1 に、MLDP based MVPN ネットワークを示します。

図 47-1　MLDP based MVPN ネットワーク



MLDP based MVPN ネットワークのパケット フロー

着信するパケットごとに、MPLS は複数の外側ラベルを作成します。ソース ネットワークからのパケットは、レシーバ ネットワークへのパス上で複製されます。CE1 ルータは、ネイティブの IP マルチキャスト トラフィックを送信します。PE1 ルータは着信マルチキャスト パケットにラベルを付加し、MPLS コア ネットワークへのラベル付きパケットを複製します。パケットは、コア ルータ（P）に到達すると、MP2MP のデフォルト MDT または P2MP のデータ MDT に対応する適切なラベル付きで複製され、すべての出力 PE に送信されます。パケットが出力 PE に到達すると、ラベルが削除され、IP マルチキャスト パケットは VRF インターフェイスに複製されます。

制約事項および使用上の注意事項

LSM MLDP based MVPN サポートを設定するときは、次の制約事項および使用上の注意事項に従ってください。

- MLDP は、出力レプリケーション モードでのみサポートされます。
- ヘッドエンド ルータは、同じ物理インターフェイス経由で異なるトンネルに属する複数の sub Label Switched Path（subLSP; サブ ラベル スイッチド パス）をサポートしません。
- P2MP TE を使用した NAT はサポートされていません。
- プロセス レベルのソフトウェア転送はサポートされません。
- MLDP based MVPN は、グローバル IPv4 マルチキャストに対してはサポートされません。
- 次に、MLDP based MVPN の規模に関する考慮事項を示します。
  - サポートされている MVRF の最大数は 100 です。
  - 各 MVRF でサポートされているマルチキャスト ルートの最大数は 100 です。
- エクストラネットのコンテンツ グループ モードは、すべての VRF で一貫している必要があります。有効なコンテンツ グループ モードには、Supported、Unsupported、および PM-sparse モードがあります。
- Supported コンテンツ グループ モードは、Protocol Independent Multicast（PIM）Sparse Mode（PIM-SM; PIM スパース モード）および Source Specific Multicast（SSM）トラフィックです。
- Unsupported コンテンツ グループ モードは、PIM Dense Mode（PIM-DM; PIM デンス モード）と bidirectional PIM（bidir-PIM; 双方向 PIM）トラフィックです。
- PIM-sparse コンテンツ グループ モードは、PE ルータの裏側（CE 上）で RP が設定されている場合にサポートされます。
- fallback-lookup オプションが指定されたスタティック マルチキャスト ルートのみが、エクストラネットの RPF ルックアップ用にサポートされます。
- MLDP は、FRR TE を使用したリンク保護のみを提供します。MLDP TE では 1 つのホップだけがサポートされ、バックアップ パスには複数のホップを設定できます。

7600 での Label Switched Multicast の設定

LSM MLDP based MVPN の展開には、デフォルトの MDT と 1 つ以上のデータ MDT の設定が含まれます。

各マルチキャスト ドメインに対してデフォルトのスタティック MDT が確立されます。デフォルト MDT は、PE ルータがマルチキャスト ドメインにある他の PE ルータに、マルチキャスト データとコントロール メッセージを送信するために使用するパスを定義します。デフォルト MDT は、単一の MP2MP LSP を使用してコア ネットワークに作成されます。

また、MLDP ベースの MLDP based MVPN は、高帯域幅の送信用にデータ MDT の動的な作成をサポートします。レートの高いデータ ソースの場合、ストリームに属さない PE への帯域幅を無駄に廃棄しないよう、デフォルト MDT からのトラフィックをオフロードするため、P2MP LSP を使用してデータ MDT が作成されます。イントラネットとエクストラネットの両方に MLDP MVPN を設定できます。

（注）　MLDP based MVPN を設定する前に、コア側のインターフェイスで MPLS がイネーブルであることを確認します。MPLS の設定の詳細については、『Cisco IOS Multiprotocol Label Switching Configuration Guide』を参照してください。または、コア ルータで BGP および任意の Interior Gateway Protocol（OSPF または ISIS）がイネーブルであることを確認します。

MLDP MVPN の設定（イントラネット）

イントラネットに MLDP MVPN を設定するには、次の手順を実行します。

- MPLS MLDP のイネーブル化
- MVPN ルーティング/転送インスタンスの設定
- VRF エントリの設定
- ルート識別子の設定
- VPN ID の設定
- ルートターゲット拡張コミュニティの設定
- デフォルト MDT の設定
- データ MDT の設定（任意）
- BGP MDT アドレス ファミリの設定
- BGP vpnv4 アドレス ファミリの設定
- BGP IPv4 VRF アドレス ファミリの設定
- VRF の PIM SM/SSM モードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls mldp**
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **vpn id** *vpn_id*
7. **route-target** [**import** | **export** | **both**] *route-target-ext-community*
8. **route-target** [**import** | **export** | **both**] *route-target-ext-community*
9. **mdt default mpls mldp** *root-node*
10. **mdt data mpls mldp** *numberofdataMDTs*
11. **mdt data threshold** *bandwidth*
12. **exit**
13. **ip multicast-routing vrf** *vrf-name*
14. **end**

（注）　MVPN に MDT ピアリング セッションが確立されるよう、PE ルータに MDT および vpnv4 アドレス ファミリ セッションを設定する方法については、「Configuring the MDT Address Family in BGP for Multicast VPN」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**mpls mldp** **例：** `Router(config)# mpls mldp`	MPLS MLDP サポートをイネーブルにします。 （注）　MPLS MLDP をディセーブルにするには、**no mpls mldp** コマンドを使用します。
ステップ 4	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf blue`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • vrf-name 引数は、VRF に割り当てる名前です。
ステップ 5	**rd** *route-distinguisher* **例：** `Router(config-vrf)# rd 10:3`	ルーティング テーブルと転送テーブルを作成します。route-distinguisher 引数で、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。RD 値は、次のいずれかの形式で入力できます。 • 16 ビット自律システム番号。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 6	**vpn id** *vpn-id* **例：** `Router(config-vrf)# vpn id 10:3`	VRF で VPN ID を設定または更新します。

	コマンド	目的
ステップ 7	**route-target import** *route-target-ext-community* **例：** `Router(config-vrf)# route-target import 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • import キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 8	**route-target export** *route-target-ext-community* **例：** `Router(config-vrf)# route-target export 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • export キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティからエクスポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 9	**mdt default mpls mldp** *root-node* **例：** `Router(config-vrf)# mdt default mpls mldp 2.2.2.2`	VRF に MLDP MDT を設定します。ルート ノードは、プロバイダー ネットワーク内の任意のルータ（ソース PE、レシーバ PE、またはコア ルータ）にあるループバックまたは物理インターフェイスの IP アドレスにすることができます。ルート ノード アドレスは、ネットワーク内のすべてのルータから到達できる必要があります。シグナリングが発生するルータは、ルート ノードとして機能します。 デフォルト MDT を各 PE ルータで設定しないと、PE ルータは、この特定 MVRF のマルチキャスト トラフィックを受信できません。 **（注）** デフォルトでは、MPLS MLDP はイネーブルになります。ディセーブルにするには、**no mpls mldp** コマンドを使用します。 **（注）** **mdt default mpls mldp** *root-node* コマンドを実行すると、LSPVIF トンネルが作成されます。
ステップ 10	**mdt data mpls mldp** *numberofdataMDTs* **例：** `Router(config-vrf)# mdt data mpls mldp 100`	MLDP データ MDP を設定します。

	コマンド	目的
ステップ 11	**mdt data threshold** *bandwidth* **例：** `Router(config-vrf)# mdt data threshold 20`	データ MDT にしきい値を設定します。 **（注）** bandwidth は、Kb/秒単位のトラフィック レートです。
ステップ 12	**exit** **例：** `Router(config-vrf)# exit`	コンフィギュレーション セッションを終了します。
ステップ 13	**ip multicast-routing vrf** *vrf-name* **例：** `Router(config)# ip multicast-routing vrf blue`	指定された VRF に対して IPv4 マルチキャスト ルーティングをイネーブルにします。
ステップ 14	**end** **例：** `Router(config)# end`	コンフィギュレーション セッションを終了します。

（注） MVPN に MDT ピアリング セッションが確立されるように、PE ルータに MDT アドレス ファミリ セッションを設定する方法については、「Configuring the MDT Address Family in BGP for Multicast VPN」を参照してください。

例

次に、イントラネットに MLDP MVPN を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# mpls mldp
Router(config)# ip vrf blue
Router(config-vrf)# rd 10:3
Router(config-vrf)# vpn id 10:3
Router(config-vrf)# route-target import 10:3
Router(config-vrf)# route-target export 10:3
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
Router(config-vrf)# mdt data mpls mldp 100
Router(config-vrf)# mdt data threshold 20
Router(config-vrf)# exit
Router(config)# ip multicast-routing vrf blue
Router(config)# end
```

検証

次のコマンドを使用して、LSM MLDP based MVPN サポートのイントラネットの設定を確認します。

- MLDP ネイバーをチェックするには、**show mpls mldp neighbor** コマンドを使用します。

```
Router# show mpls mldp neighbors
MLDP peer ID    : 3.3.3.3:0, uptime 00:41:41 Up,
  Target Adj     : Yes
  Session hndl   : 2
  Upstream count : 2
  Branch count   : 0
  Path count     : 1
  Path(s)        : 3.3.3.3           No LDP Tunnel20
  Nhop count     : 1
  Nhop list      : 3.3.3.3

 MLDP peer ID    : 2.2.2.2:0, uptime 00:17:42 Up,
  Target Adj     : No
  Session hndl   : 4
  Upstream count : 0
  Branch count   : 0
  Path count     : 1
  Path(s)        : 3.3.3.3           No LDP Tunnel20
  Nhop count     : 0
```

- PIM ネイバーをチェックするには、**show ip pim vrf** ***vrf-name*** **neighbor** コマンドを使用します。

```
Router# show ip pim vrf blue neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
3.3.3.3           Lspvif1                 00:06:21/00:01:17 v2    1 / DR S P G
```

- 特定の VRF のマルチキャスト ルートをチェックするには、**show ip mroute vrf** *vrf_name* **verbose** コマンドを使用します。

```
Router# show ip mroute vrf blue verbose
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(40.0.0.2, 232.0.1.4), 00:00:16/00:03:13, flags: sT
  Incoming interface: GigabitEthernet3/2/1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif1, LSM MDT: B0000004 (default), Forward/Sparse, 00:00:16/00:03:13

(*, 224.0.1.40), 00:47:09/00:02:56, RP 0.0.0.0, flags: DPL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

- パケット カウンタをチェックするには、**show ip mroute vrf** *vrf_name* **count** コマンドを使用します。

```
Router# show ip mroute vrf blue count
IP Multicast Statistics
2 routes using 1208 bytes of memory
2 groups, 0.50 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: 232.0.1.4, Source count: 1, Packets forwarded: 1333, Packets received: 1334
```

```
  Source: 40.0.0.2/32, Forwarding: 1333/20/46/7, Other: 1334/0/1

Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

- MPLS フォワーディングをチェックするには、**show mpls forwarding-table** コマンドを使用します。

```
Router# show mpls forwarding-table
Local Outgoing Prefix Bytes Label Outgoing Next Hop
Label      Label      or Tunnel Id     Switched      interface
16 Pop Label IPv4 VRF[V] 0 aggregate/blue
17 Pop Label  IPv4 VRF[V] 0 aggregate/red
18 [T] Pop Label  3.3.3.3/32 0 Tu20 point2point
19 [T]  25 2.2.2.2/32 0 Tu20 point2point
20 [T]  Pop Label 19.0.0.0/24 0 Tu20 point2point
22 [T]  No Label [mdt 55:1111 0][V] \9422 aggregate/red
23 [T]  No Label [mdt 55:2222 0][V] \9708          aggregate/blue
[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option
```

- SP/DFC 上のラベルの内容をチェックするには、**show mls cef mpls labels** *mldp_label* コマンドを使用します。

```
Router# show mls cef mpls labels op
Codes: + - Push label, - - Pop Label         * - Swap Label, E - exp1
Index  Local            Label                 Out i/f
       Label             Op
2189   23   (EOS)       (-)                   recirc
```

エクストラネット サービスに対する MLDP MVPN の設定

次の方法を使用して、エクストラネット サービスに MLDP MVPN を設定できます。

- Source Side Chaining（SSC）：ソース側のルータにファントムのレシーバ MVRF を設定します。ソース PE には、フォールバック ループバックを指定したマルチキャスト ルートを設定する必要があります。
- Receiver Side Chaining（RSC）：レシーバ側のルータにファントムのソース MVRF を設定します。レシーバ VRF には、フォールバック ルックアップを指定したマルチキャスト ルートを設定する必要があります。

Cisco 7600 シリーズ ルータの MVPN エクストラネット サポートの詳細については、「Multicast VPN Extranet Support」を参照してください。MVPN は、PFC3B、PFC3BXL、PFC3C、または PFC3CXL ルータ インストールでサポートされます。

SSC を使用したエクストラネット用 MLDP MVPN の設定

SSC を使用して MLDP MVPN エクストラネット サポートを設定するには、次の手順を実行します。

- ソース PE でのレシーバ MVRF の設定。
- ソース PE でのレシーバ VRF のループバック アドレスの設定。
- ソース PE でのソース アドレスに対するフォールバック マルチキャスト ルートの設定。
- SM モードの場合のソース PE での RP アドレスに対するフォールバック マルチキャスト ルートの設定。
- ソース PE に設定されたレシーバ VRF のループバック IP に対する、レシーバ PE でのスタティック マルチキャスト ルートの設定。

（注）　この設定は、図 47-1 に基づいています。マルチキャスト ルートは PE1 ルータに設定します。

手順の概要

ソース PE での設定：

1. **enable**
2. **configure terminal**
3. **ip vrf** ***vrf-name***
4. **rd** *route-distinguisher*
5. **vpn id** *vpn_id*
6. **route-target import** *route-target-ext-community*
7. **route-target import** *route-target-ext-community*
8. **mdt default mpls mldp** *root-node*
9. **end**
10. **interface type** *instance*
11. **ip vrf forwarding** *vrf-name*
12. **ip address** *ip-address subnet*
13. **ip mroute** [**vrf** *receiver-vrf-name*] *source-address mask* **fallback-lookup** {**global** | **vrf** *source-vrf-name*} [*distance*]
14. （SM モードの場合）**ip mroute** [**vrf** *receiver-vrf-name*] *rp-address mask* **fallback-lookup** {**global** | **vrf** *source-vrf-name*} [*distance*]
15. **end**

レシーバ PE での設定：

1. **enable**
2. **configure terminal**
3. **ip vrf** ***vrf-name***
4. **rd** *route-distinguisher*
5. **vpn id** *vpn_id*
6. **route-target import** *route-target-ext-community*
7. **route-target import** *route-target-ext-community*
8. **mdt default mpls mldp** *root-node*
9. **end**
10. **interface type** *instance*
11. **ip vrf forwarding** *vrf-name*
12. **ip address** *ip-address subnet*
13. **ip mroute vrf** *receiver_vrf source_address subnet_mask loopback_ip*
14. **end**

手順の詳細

ソース PE での設定：

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf blue`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • vrf-name 引数は、VRF に割り当てる名前です。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-if)# rd 10:4`	ルーティング テーブルと転送テーブルを作成します。route-distinguisher 引数で、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。RD 値は、次のいずれかの形式で入力できます。 • 16 ビット自律システム番号。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**vpn id** *vpn-id* **例：** `Router(config-if)# vpn id 10:4`	VRF で VPN ID を設定または更新します。
ステップ 6	**route-target import** *route-target-ext-community* **例：** `Router(config-vrf)# route-target import 10:4`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • import キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。

	コマンド	目的
ステップ 7	**route-target export** *route-target-ext-community* **例：** `Router(config-vrf)# route-target export 10:4`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • export キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 8	**mdt default mpls mldp** *root-node* **例：** `Router(config-vrf)# mdt default mpls mldp 2.2.2.2`	VRF に対して MLDP Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）を設定します。 **（注）** このコマンドによって、LSPVIF トンネルが作成されます。
ステップ 9	**end** **例：** `Router(config-vrf)# end`	コンフィギュレーション セッションを終了します。
ステップ 10	**interface type** *instance* **例：** `Router(config)# interface loopback 3`	インターフェイス コンフィギュレーション モードを開始して、新しいループバック インターフェイスの名前を指定します。
ステップ 11	**ip vrf forwarding** *vrf-name* **例：** `Router(config-if)# ip vrf forwarding red`	VRF インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • vrf-name は、VRF に割り当てる名前です。
ステップ 12	**ip address** *ip-address subnet-mask* **例：** `Router(config-if)# ip address 1.1.1.1 255.255.255.255`	インターフェイス IP アドレスとサブネット マスクを指定します。 • ip-address は、インターフェイスの IP アドレスを指定します。 • subnet-mask は、インターフェイスのサブネット マスクを指定します。

	コマンド	目的
ステップ 13	**ip mroute** [**vrf** receiver-vrf-name] source-address mask {**fallback-lookup vrf** source-vrf-name} [*distance*] **例：** Router(config)# ip mroute vrf red 40.0.0.0 255.255.255.0 fallback-lookup vrf blue	レシーバ MVRF またはグローバル ルーティング テーブルで発生する RPF ルックアップが、ソース MVRF またはグローバル ルーティング テーブルで解決されるように設定します。 • オプションの vrf キーワードおよび receiver-vrf-name 引数を使用して、receiver-vrf-name 引数に指定された VRF で発生する RPF ルックアップにグループベースの VRF 選択ポリシーを適用します。オプションの vrf キーワードと receiver-vrf-name 引数が指定されない場合、グループベースの VRF 選択ポリシーは、グローバル テーブルで発生する RPF ルックアップに適用されます。
ステップ 14	**ip mroute** [**vrf** receiver-vrf-name] rp-address mask {**fallback-lookup vrf** source-vrf-name} [distance] **例：** Router(config-if)# ip mroute vrf red 44.44.44.44 255.255.255.0 fallback-lookup vrf blue	レシーバ MVRF または Rendezvous Point（RP; ランデブー ポイント）のグローバル ルーティング テーブルで発生する RPF ルックアップが、ソース MVRF またはグローバル ルーティング テーブルで解決されるように設定します。 **（注）** このコマンドは、SM モードにのみ必要です。
ステップ 15	**end** **例：** Router(config-vrf)# end	コンフィギュレーション セッションを終了します。

レシーバ PE での設定：

	コマンド	目的
ステップ 1	**enable** **例：** Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** 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	**ip vrf** *vrf-name* **例：** Router(config)# ip vrf blue	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • vrf-name 引数は、VRF に割り当てる名前です。

	コマンド	目的
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-if)# rd 10:4`	ルーティング テーブルと転送テーブルを作成します。route-distinguisher 引数で、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。RD 値は、次のいずれかの形式で入力できます。 • 16 ビットの自律システム番号：32 ビット数値。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**vpn id** *vpn-id* **例：** `Router(config-if)# vpn id 10:4`	VRF で VPN ID を設定または更新します。
ステップ 6	**route-target import** *route-target-ext-community* **例：** `Router(config-vrf)# route-target import 10:4`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • import キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 7	**route-target export** *route-target-ext-community* **例：** `Router(config-vrf)# route-target export 10:4`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • export キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 8	**mdt default mpls mldp** *root-node* **例：** `Router(config-vrf)# mdt default mpls mldp 2.2.2.2`	VRF に対して MLDP Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）を設定します。 **（注）** このコマンドによって、LSPVIF トンネルが作成されます。
ステップ 9	**end** **例：** `Router(config-vrf)# end`	コンフィギュレーション セッションを終了します。

	コマンド	目的
ステップ 10	**interface type** *instance* **例：** `Router(config)# interface loopback 3`	インターフェイス コンフィギュレーション モードを開始して、新しいループバック インターフェイスの名前を指定します。
ステップ 11	**ip vrf forwarding** *vrf-name* **例：** `Router(config-if)# ip vrf forwarding blue`	VRF インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • vrf-name は、VRF に割り当てる名前です。
ステップ 12	**ip address** *ip-address subnet-mask* **例：** `Router(config-if)# ip address 3.3.3.3 255.255.255.255`	インターフェイス IP アドレスとサブネット マスクを指定します。 • ip-address は、インターフェイスの IP アドレスを指定します。 • subnet-mask は、インターフェイスのサブネット マスクを指定します。
ステップ 13	**ip mroute vrf** *receiver_vrf source_address subnet_mask loopback_ip* **例：** `Router(config-if)# ip mroute vrf red 40.0.0.0 255.255.255.0 1.1.1.1`	レシーバ VRF のソース アドレスにスタティック マルチキャスト ルートを設定します。 loopback ip は、ソース PE でレシーバ VRF に設定されたループバックの IP アドレスです。
ステップ 14	**end** **例：** `Router(config-vrf)# end`	コンフィギュレーション セッションを終了します。

例

次に、SSC を使用してエクストラネットを設定するための MLDP MVPN の設定例を示します。

ソース PE での設定（red と blue の両方の VRF に対して次の設定を行います）

```
Router> enable
Router# configure terminal
Router(config)# ip vrf blue
Router(config-if)# rd 10:4
Router(config-if)# vpn id 10:4
Router(config-vrf)# route-target import 10:4
Router(config-vrf)# route-target export 10:4
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
Router(config-vrf)# end
Router(config)# interface loopback 3
Router(config-if)# ip vrf forwarding red
Router(config-if)# ip address 1.1.1.1 255.255.255.255
Router(config)# ip mroute vrf red 40.0.0.0 255.255.255.0 fallback-lookup vrf blue
Router(config)# ip mroute vrf red 44.44.44.44 255.255.255.0 fallback-lookup vrf blue
Router(config-vrf)# end
```

レシーバ PE での設定

```
Router> enable
Router# configure terminal
Router(config)# ip vrf blue
Router(config-if)# rd 10:4
Router(config-if)# vpn id 10:4
Router(config-vrf)# route-target import 10:4
Router(config-vrf)# route-target export 10:4
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
Router(config-vrf)# end
Router(config)# interface loopback 3
Router(config-if)# ip vrf forwarding blue
Router(config-if)# ip address 3.3.3.3 255.255.255.255 Remove
Router(config-if)# ip mroute vrf red 40.0.0.0 255.255.255.0 1.1.1.1
Router(config-vrf)# end
```

RSC を使用したエクストラネット サービスに対する MLDP MVPN の設定

RSC を使用してエクストラネット サービスに MLDP MVPN を設定するには、次の手順を実行します。

- レシーバ PE ルータでのソース mVRF の設定。
- レシーバ PE のスタティック マルチキャスト ルートを使用する MLDP based MVPN エクストラネット サポートに対する RPF の設定。

（注）　この設定は、図 47-1 に基づいています。PE2 ルータと PE3 ルータにマルチキャスト ルートを設定します。

手順の概要

ソース PE での設定：

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **vpn id** *vpn_id*
6. **route-target import** *route-target-ext-community*
7. **route-target import** *route-target-ext-community*
8. **mdt default mpls mldp** *root-node*
9. **end**

レシーバ PE での設定（red と blue の両方の VRF に対して次の設定を行います）

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **vpn id** *vpn_id*
6. **route-target import** *route-target-ext-community*

7. **route-target import** *route-target-ext-community*
8. **mdt default mpls mldp** *root-node*
9. **ip mroute** [**vrf** *recevier-vrf-name*] *source-address mask* **fallback-lookup** {**global** | **vrf** *source-vrf-name*} [*distance*]
10. **end**

手順の詳細

ソース PE での設定

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf blue`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • vrf-name 引数は、VRF に割り当てる名前です。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-if)# rd 10:3`	ルーティング テーブルと転送テーブルを作成します。route-distinguisher 引数で、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。RD 値は、次のいずれかの形式で入力できます。 • 16 ビットの自律システム番号：32 ビット数値。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**vpn id** *vpn-id* **例：** `Router(config-if)# vpn id 10:3`	VRF で VPN ID を設定または更新します。

	コマンド	目的
ステップ 6	**route-target import** *route-target-ext-community* **例：** `Router(config-vrf)# route-target import 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • import キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 7	**route-target export** *route-target-ext-community* **例：** `Router(config-vrf)# route-target export 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • export キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 8	**mdt default mpls mldp** *root-node* **例：** `Router(config-vrf)# mdt default mpls mldp 2.2.2.2`	VRF に対して MLDP Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）を設定します。 **（注）** このコマンドによって、LSPVIF トンネルが作成されます。
ステップ 9	**end** **例：** `Router(config-vrf)# end`	コンフィギュレーション セッションを終了します。

レシーバ PE での設定

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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。

	コマンド	目的
ステップ 3	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf blue`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • vrf-name 引数は、VRF に割り当てる名前です。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-if)# rd 10:3`	ルーティング テーブルと転送テーブルを作成します。route-distinguisher 引数で、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。RD 値は、次のいずれかの形式で入力できます。 • 16 ビット自律システム番号。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**vpn id** *vpn-id* **例：** `Router(config-if)# vpn id 10:3`	VRF で VPN ID を設定または更新します。
ステップ 6	**route-target import** *route-target-ext-community* **例：** `Router(config-vrf)# route-target import 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • import キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 7	**route-target export** *route-target-ext-community* **例：** `Router(config-vrf)# route-target export 10:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • export キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • route-target-ext-community 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 8	**mdt default mpls mldp** *root-node* **例：** `Router(config-vrf)# mdt default mpls mldp 2.2.2.2`	VRF に対して MLDP Multicast Distribution Tree（MDT; マルチキャスト配信ツリー）を設定します。 **（注）** このコマンドによって、LSPVIF トンネルが作成されます。

	コマンド	目的
ステップ 9	**ip mroute** [**vrf** receiver-vrf-name] source-address mask {**fallback-lookup vrf** source-vrf-name} [*distance*] **例：** Router(config)# ip mroute vrf red 40.0.0.0 255.255.255.0 fallback-lookup vrf blue	レシーバ MVRF またはグローバル ルーティング テーブルで発生する RPF ルックアップが、ソース MVRF またはグループ アドレス ベースのグローバル ルーティング テーブルで解決されるように設定します。このコマンドは、レシーバ PE に使用します。 • オプションの vrf キーワードおよび receiver-vrf-name 引数を使用して、receiver-vrf-name 引数に指定された VRF で発生する RPF ルックアップにグループベースの VRF 選択ポリシーを適用します。オプションの vrf キーワードと receiver-vrf-name 引数が指定されない場合、グループベースの VRF 選択ポリシーは、グローバル テーブルで発生する RPF ルックアップに適用されます。
ステップ 10	**end** **例：** Router(config-vrf)# end	コンフィギュレーション セッションを終了します。

例

次に、RSC を使用してエクストラネットを設定するための MLDP MVPN の設定例を示します。

ソース PE での設定：

```
Router# enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf blue1
Router(config-if)# rd 10:3
Router(config-if)# vpn id 10:3
Router(config-vrf)# route-target import 10:3
Router(config-vrf)# route-target export 10:3
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
mdt default mpls mldp root-node
Router(config-if)# end
Router(config)# ip mroute vrf red 40.0.0.0 255.255.255.0 fallback-lookup vrf blue
Router(config-if)# end
```

レシーバ PE での設定：

```
Router# enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf blue1
Router(config-if)# rd 10:3
Router(config-if)# vpn id 10:3
Router(config-vrf)# route-target import 10:3
Router(config-vrf)# route-target export 10:3
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
Router(config)# ip mroute vrf red 40.0.0.0 255.255.255.0 fallback-lookup vrf blue
Router(config-if)# end
```

MLDP TE-FRR サポートの設定

TE-FRR はリンク保護を提供しますが、MLDP の TE-FRR は単一ホップのプライマリ パスにのみリンク保護を提供します。ノード保護はサポートされません。次に、重要事項を示します。

- バックアップ トンネル サポート
- バックアップ帯域幅保護

MPLS TE-FRR の詳細については、『MPLS Point-to-Multipoint Traffic Engineering』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast mpls traffic-eng** [**range** {*access-list-number* | *access-list-name*}]
4. **mpls mldp path traffic-eng**
5. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**ip multicast mpls traffic-eng** [**range** {access-list-number | access-list-name}] **例：** `Router(config)# ip multicast mpls traffic-eng [range {access-list-number | access-list-name}]`	MPLS TE P2MP 機能でイネーブルになっているテール エンド ルータの IP マルチキャスト トラフィックをイネーブルにします。

	コマンド	目的
ステップ 4	**mpls mldp path traffic-eng** **例：** `Router(config)# mpls mldp path traffic-en`	traffic-eng トンネルを使用するように、MLDP を設定します。
ステップ 5	**end** **例：** `Router(config)# end`	コンフィギュレーション セッションを終了します。

詳細については、『MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection』を参照してください。

PIM based MVPN での MLDP の設定

PIM based MVPN での MLDP は、MLDP と PIM based MVPN の展開の共存をサポートします。この機能を使用すると、既存の PIM based MVPN 環境に MLDP を徐々に導入して、完全な LSM based MVPN ネットワーク インフラへの段階的な移行を容易に行うことができます。MLDP based MVPN と GRE based MVPN の両方が設定されている場合、MDT はデフォルトで PIM based MVPN を選択します。**mdt preference** ***option1 option2*** コマンドを使用して、MLDP MVPN と PIM based MVPN の優先順位を設定します。次の例では、PIM based MVPN よりも MLDP MVPN を優先するように設定されています。

```
Router(config-vrf)# mdt preference mldp pim
```

ロード バランシングを伴う MLDP のサポート

MLDP は、Equal Cost Multipath（ECMP; 等コスト マルチパス）リンクを使用したマルチキャスト トラフィックのロード バランシングをサポートします。MLDP でロード バランシングを有効にするには、**disable mpls mldp forwarding recursive** コマンドを使用します。これは、デフォルトでイネーブルになっています。また、ロード バランシングが予期したとおりに機能するように、**mpls mldp path multipath** コマンドがイネーブルになっていることを確認します。

ルート ノード冗長性

mdt default mpls mldp ***ip_address*** コマンドを使用して、ネットワーク内に複数のルート ノードを設定します。コントロール プレーンは、設定されたノードをルートとした対応するツリーを構築し、効率的な転送を可能にします。ネットワーク内のノードは、帯域幅の使用を最適化するために最も近くのルートを選択します。また、ルート ノードが到達不可能な場合（リンク障がいやルータ クラッシュなどによる）、ノードは次に使用できるルートに切り替えます。

次に、ルート ノード冗長性の設定例を示します。

```
Router(config)# ip vrf blue1
Router(config-if)# rd 10:3
Router(config-if)# vpn id 10:3
Router(config-vrf)# route-target import 10:3
Router(config-vrf)# route-target export 10:3
Router(config-vrf)# mdt default mpls mldp 2.2.2.2
```

```
Router(config-vrf)# mdt default mpls mldp 5.5.5.5
```

検証

次のコマンドを使用して、LSM MLDP based MVPN サポートの設定を確認します。

- MLDP ネイバーをチェックするには、**show mpls mldp neighbor** コマンドを使用します。

```
Router# show mpls mldp neighbors
MLDP peer ID    : 3.3.3.3:0, uptime 00:41:41 Up,
  Target Adj     : Yes
  Session hndl   : 2
  Upstream count : 2
  Branch count   : 0
  Path count     : 1
  Path(s)        : 3.3.3.3           No LDP Tunnel20
  Nhop count     : 1
  Nhop list      : 3.3.3.3

 MLDP peer ID    : 2.2.2.2:0, uptime 00:17:42 Up,
  Target Adj     : No
  Session hndl   : 4
  Upstream count : 0
  Branch count   : 0
  Path count     : 1
  Path(s)        : 3.3.3.3           No LDP Tunnel20
  Nhop count     : 0
```

- PIM ネイバーをチェックするには、**show ip pim vrf *vrf_name* neighbor** コマンドを使用します。

```
Router# show ip pim vrf blue neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
3.3.3.3           Lspvif1                 00:06:21/00:01:17 v2    1 / DR S P G
```

- 特定の VRF のマルチキャスト ルートをチェックするには、**show ip mroute vrf *vrf_name* verbose** コマンドを使用します。

```
Router# show ip mroute vrf blue verbose
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(40.0.0.2, 232.0.1.4), 00:00:16/00:03:13, flags: sT
  Incoming interface: GigabitEthernet3/2/1, RPF nbr 0.0.0.0
  Outgoing interface list:
    Lspvif1, LSM MDT: B0000004 (default), Forward/Sparse, 00:00:16/00:03:13

(*, 224.0.1.40), 00:47:09/00:02:56, RP 0.0.0.0, flags: DPL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

- パケット カウンタをチェックするには、**show ip mroute vrf** *vrf_name* **count** コマンドを使用します。

```
Router# show ip mroute vrf blue count
IP Multicast Statistics
2 routes using 1208 bytes of memory
2 groups, 0.50 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: 232.0.1.4, Source count: 1, Packets forwarded: 1333, Packets received: 1334
  Source: 40.0.0.2/32, Forwarding: 1333/20/46/7, Other: 1334/0/1

Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

- MFIB 出力をチェックし、ハードウェア スイッチングまたはソフトウェア スイッチングがイネーブルかどうかを確認するには、**show ip mfib vrf** *vrf_name group_address* **verbose** コマンドを使用します。

```
Router# show ip mfib vrf blue 232.0.1.4 verbose
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform Entry flags: HF - Hardware Forwarding, NP - Not platform switched,
                      PF - Partial Hardware Forwarding
Platform Interface flags: HW - Hardware Switched, NP - Not platform switched
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
VRF blue
 (40.0.0.2,232.0.1.4) Flags: K HW
   Platform Flags:  HW
   Slot 6: HW Forwarding: 912/41952, Platform Flags:  HF
   SW Forwarding: 0/0/0/0, Other: 1/0/1
   HW Forwarding:   912/20/46/7, Other: 0/0/0
   GigabitEthernet3/2/1 Flags: RA A MA
     Platform Flags:
   Lspvif1, LSM/B0000004 Flags: RF F NS
     Platform Flags:  HW
     CEF: Mid chain adjacency
     Pkts: 0/0
```

- Switched Processor /Distributed Forwarding Card（SP/DFC; スイッチ プロセッサ / 分散型フォワーディング カード）上のハードウェア エントリをチェックするには、**show platform software multicast ip cmfib vrf** *vrf_name group_add* **verbose** コマンドを使用します。

```
Router# show platform software multicast ip cmfib vrf blue 232.0.1.4 verbose
Multicast CEF Entries for VPN#1
(40.0.0.2, 232.0.1.4) IOSVPN:256  (1) PI:1 (1) CR:0 (1) Recirc:0 (1)
Vlan:1033 AdjPtr:442371 FibRpfNf:1 FibRpfDf:1 FibAddr:0x800C0 rwvlans:1033
rwindex:0x7FFA adjmac:000a.f330.2480 rdt:1 E:0 CAP1:0 fmt:Mcast l3rwvld:1 DM:0
mtu:1532 rwtype:L2&L3 met2:0x8002 met3:0x8003
packets:0000000002184 bytes:000000000000139776
Starting Offset: 0x8002
V E L0 C:1026 I:0x02014 Starting Offset: 0x8003 V E C:1034 IOSVPN:256  (1) PI:0 (1)
CR:1 (1) Recirc:0 (1)
Vlan:1026 AdjPtr:442372 FibRpfNf:0 FibRpfDf:1 FibAddr:0x800C2
rwvlans:1026 rwindex:0x7FFA adjmac:000a.f330.2480 rdt:1 E:0 CAP1:0
```

```
fmt:Mcast l3rwvld:1 DM:0 mtu:1532 rwtype:L3 met2:0x0 met3:0x8003
packets:0000000000000 bytes:000000000000000000
Starting Offset: 0x8003
           V E C:1034
Annotation-data: [0x4B417730]
        A-vlan: 1033 NS-vlan: 0 RP-rpf-vlan: 0
        Anntn flags: [0x10]  H
        MTU: 1514 Retry-count: 0
        Sec-entries count: 1
Met-handle: 0x4510801C New-Met-handle: 0x0
        Met2-handle: 0x595389D4
HAL L3-data : [0x46ED8D00]
Flags: 0x4 FIB-index: 0x853 ADJ-index: 0x6C003 NF-addr: 0x0
ML3 entry type: 0x0 [(S,G) shortcut]
        Flags: 0xA1000000 Vpn: 256 Rpf: 1033 Rw_index: 0x7FFA
Adj_mtu: 1528 Met2: 0x8002 Met3: 0x8003
        V6-data: NULL
---Secondary entry [1]---
HAL L3-data : [0x47206CD0]
Flags: 0x4 FIB-index: 0x854 ADJ-index: 0x6C004 NF-addr: 0x0 ML3 entry type: 0x0 [(S,G)
shortcut]
Flags: 0x90000000 Vpn: 256 Rpf: 1026 Rw_index: 0x7FFA
Adj_mtu: 1528 Met2: 0x0 Met3: 0x8003
        V6-data: NULL
---LSM entries---
Sublsp:13, if_number:21, met3_vlan:1034, fib_index:0x800C4, adj_addr:30,
l3_id:0x5C107AA0, ml3_entry:0x5C107AC0
HAL L3-data : [0x5C107AA0]
        Flags: 0x0 FIB-index: 0x855 ADJ-index: 0x1E NF-addr: 0x0
        ML3 entry type: 0xE [MPLS LABEL PUSH shortcut]
        Flags: 0x32000000 Vpn: 260 Rpf: 0 Rw_index: 0x0
Adj_mtu: 0 Met2: 0x0 Met3: 0x0 V6-data: NULL
```

- LSM 隣接関係の内容をチェックするには、**show mls cef adjacency entry** *mpls_label* **detail** コマンドを使用します。

```
Router# show mls cef adjacency entry 30 detail
Index: 30      smac: 000a.f330.2480, dmac: 001b.0de4.2b00
               mtu: 65535, vlan: 1031, dindex: 0x2117, l3rw_vld: 1
               format: MPLS, flags: 0x8610
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 20, exp: 0, ovr: 0
               op: PUSH_LABEL2
               packets: 6432, bytes: 411648
```

- 内部 VLAN をチェックするには、**show vlan internal usage** コマンドを使用します。

```
Router# sh vlan internal usage
VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Ls0 Label Replication (0) (0)
1014 Ls1 Label Replication (0) (0)
1015 Control Plane Protection
1016 vrf_0_vlan
1017 Lspvif0
1018 Container0
```

```
1019 Lspvif1
1020 IPv6-mpls RSVD VLAN
1021 IPv4 VPN 0 Egress multicast
1022 IP Multicast Partial SC vpn(2)
1023 IPv4 VPN 2 Egress multicast
1024 Multicast VPN 2 QOS Vlan
1025 IP Multicast Partial SC vpn(1)

VLAN Usage
---- --------------------
1026 IPv4 VPN 1 Egress multicast
1027 Multicast VPN 1 QOS Vlan
1028 IP Multicast Partial SC vpn(0)
1029 Multicast VPN 0 QOS Vlan
1030 GigabitEthernet6/2
1031 FastEthernet2/1/0
1032 GigabitEthernet3/2/2
1033 GigabitEthernet3/2/1
1034 Fa2/1/0 Label Replication (1000000200000000) (1)
1035 Fa2/1/0 Label Replication (1000000200000000) (2)
1036 Gi3/2/2 Label Replication (1600000200000000) (1)
1037 Gi3/2/2 Label Replication (1600000200000000) (2)
```

- ラベル レプリケーション VLAN をチェックするには、**show mpls platform vlan lsm** コマンドを使用します。

```
Router# show mpls platform vlan lsm
VLAN Interface            Opaque          Vrf id   MLS VPN  hw_id    subblock
1013 Lspvif0              0                0        0        258      0x4BC4A190
1014 Lspvif1              0                0        1        259      0x4BC491C0
1034 FastEthernet2/1/0    1000000200000000 1        2        260      0x4BC481F0
1035 FastEthernet2/1/0    1000000200000000 2        3        261      0x4BC481F0
1036 GigabitEthernet3/2/2 1600000200000000 1        4        262      0x4BC47220
1037 GigabitEthernet3/2/2 1600000200000000 2        5        263      0x4BC47220
```

- ラベルをチェックするには、**show mpls forwarding-table** コマンドを使用します。

```
Router# show mpls forwarding-table
Local Outgoing Prefix Bytes Label Outgoing Next Hop
Label      Label      or Tunnel Id     Switched      interface
16 Pop Label IPv4 VRF[V] 0 aggregate/blue
17 Pop Label  IPv4 VRF[V] 0 aggregate/red
18 [T] Pop Label  3.3.3.3/32 0 Tu20 point2point
19 [T]  25 2.2.2.2/32 0 Tu20 point2point
20 [T]  Pop Label 19.0.0.0/24 0 Tu20 point2point
22 [T]  No Label [mdt 55:1111 0][V] \9422 aggregate/red
23 [T]  No Label [mdt 55:2222 0][V] \9708          aggregate/blue
[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option
```

- SP/DFC 上のラベルの内容をチェックするには、**show mls cef mpls labels** *mlpls_label* コマンドを使用します。

```
Router# show mls cef mpls labels 23
Codes: + - Push label, - - Pop Label         * - Swap Label, E - expl
Index  Local            Label                  Out i/f
       Label             Op
2189   23  (EOS)        (-)                    recirc
```

- 詳細な内容をチェックするには、**show mls cef mpls labels** *mpls_label* **detail** コマンドを使用します。

```
Router# show mls cef mpls labels 23 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
```

```
       D - FIB Don't short-cut, m - mod-num, E - ELSP?
Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2 eos2)
V(2184   ): B | 1 0    0 0 0 22      0 1 0 0       0 0 (A:163840 ,P:0,D:0,m:0 :E:1)
M(2184   ): F | 1 FFF  0 0 1 FFFFF   0 1 0 0       0 0
```

- ラベルの Ternary Content Addressable Memory（TCAM）隣接関係の内容をチェックするには、**show mls cef adj entry** *adjacency_pointer* **detail** コマンドを使用します。

```
Router# show mls cef adjacency entry 163840 detail
Index: 163840  smac: 000a.f330.2480, dmac: 0100.5e00.000d
               mtu: 65535, vlan: 1017, dindex: 0x7FFA, l3rw_vld: 1
               format: MPLS, flags: 0x1000008600
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 0, exp: 0, ovr: 0
               op: POP
               packets: 0, bytes: 0
```

MLDP MVPN のサンプル設定

MLDP MVPN は、次の 2 つのモードで設定できます。

- Source Specific Mode（SSM）
- Sparse Mode（SM）

SSM モードを使用した設定例

次の例は、図 47-1 のトポロジに基づいています。SSM モードを使用して MLDP MVPN を設定するときは、次のシナリオを考慮してください。

- MLDP MVPN エクストラネット SSC
- MLDP MVPN エクストラネット RSC
- MLDP MVPN イントラネット

MLDP MVPN エクストラネット SSC

PE1 ルータでの設定（ソース PE）：

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red2
```

```
ip multicast-routing vrf red3

interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 101.3.0.2 255.255.255.255
 ip pim sparse-mode

interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
```

```
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family

ip pim vrf red2 ssm default
ip pim vrf red3 ssm default
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
```

P ルータでの設定：

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255

interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp

interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
```

```
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
```

PE2 ルータでの設定（レシーバ PE）：

```
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3

interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 102.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet4/0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
```

```
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red3 ssm default
ip mroute vrf red3 12.2.0.0 255.255.0.0 101.3.0.2
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 103.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
```

```
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red3 ssm default
ip mroute vrf red3 12.2.0.0 255.255.0.0 101.3.0.2
```

MLDP MVPN エクストラネット RSC

PE1 ルータでの設定（ソース PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
```

```
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
```

```
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 ssm default
```

P ルータでの設定（コア ルータ）

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp
!
interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
 mls qos trust dscp
!
router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
!
```

PE2 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
```

```
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 102.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 102.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet4/0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
```

```
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red3 ssm default
ip pim vrf red2 ssm default
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
```

```
ip multicast-routing vrf red3
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 103.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 103.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
```

```
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red3 ssm default
ip pim vrf red2 ssm default
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
```

MLDP MVPN イントラネット

PE1 ルータでの設定（ソース PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
```

```
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 ssm default
```

P ルータでの設定（コア ルータ）

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
```

```
interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp
!
interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
 mls qos trust dscp
!
router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
!
```

PE2 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 102.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
```

```
interface GigabitEthernet4/0/1.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 ssm default
!
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
```

```
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 103.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
```

```
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red2 ssm default
!
```

SM モードを使用した設定例

次の例は、図 47-1 のトポロジに基づいています。SSM モードを使用して MLDP MVPN を設定するときは、次のシナリオを考慮してください。

- MLDP MVPN エクストラネット SSC
- MLDP MVPN エクストラネット RSC
- MLDP MVPN イントラネット

MLDP MVPN エクストラネット SSC

PE1 ルータでの設定（ソース PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red2
ip multicast-routing vrf red3

interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 101.3.0.2 255.255.255.255
```

```
 ip pim sparse-mode

interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
```

```
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family

ip pim vrf red2 rp-address 11.11.11.11
ip pim vrf red3 rp-address 11.11.11.11
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
ip mroute vrf red3 11.11.11.11 255.255.0.0 fallback-lookup vrf red2
```

P ルータでの設定

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255

interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp

interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp

router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
```

PE2 ルータでの設定（レシーバ PE）

```
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
```

```
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3

interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 102.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet4/0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
```

```
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red3 rp-address 11.11.11.11
ip mroute vrf red3 12.2.0.0 255.255.0.0 101.3.0.2
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 103.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
```

```
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red3 rp-address 11.11.11.11
ip mroute vrf red3 12.2.0.0 255.255.0.0 101.3.0.2
```

MLDP MVPN エクストラネット RSC

PE1 ルータでの設定（ソース PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
```

```
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
```

P ルータでの設定（コア ルータ）

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
```

```
interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp
!
interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
 mls qos trust dscp
!
router ospf 1
 router-id 4.4.4.4
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
!
```

PE2 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3
ip multicast-routing vrf red2
!
```

```
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 102.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 102.3.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet4/0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
```

```
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
ip pim vrf red3 rp-address 11.11.11.11
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
ip mroute vrf red3 11.11.11.11 255.255.255.255 fallback-lookup vrf red2
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip vrf red3
 rd 10:3
 vpn id 10:3
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:3
 route-target import 10:3
!
ip multicast-routing
ip multicast-routing vrf red3
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 103.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback103
 ip vrf forwarding red3
 ip address 103.3.0.2 255.255.255.255
 ip pim sparse-mode
```

```
!
interface GigabitEthernet3/2/0.3
 encapsulation dot1Q 3
 ip vrf forwarding red3
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red3
  redistribute static
  redistribute connected
```

```
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
ip pim vrf red3 rp-address 11.11.11.11
ip mroute vrf red3 12.2.0.0 255.255.0.0 fallback-lookup vrf red2
ip mroute vrf red3 11.11.11.11 255.255.255.255 fallback-lookup vrf red2
```

MLDP MVPN イントラネット

PE1 ルータでの設定（ソース PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 101.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet1/22.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 12.2.0.1 255.255.0.0
 ip pim sparse-mode
!
interface TenGigabitEthernet8/1
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
```

```
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
```

P ルータでの設定（コア ルータ）

```
interface Loopback1
 ip address 4.4.4.4 255.255.255.255
!
interface GigabitEthernet2/10
 ip address 20.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet2/20
 ip address 30.1.1.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
 mpls label protocol ldp
!
interface TenGigabitEthernet4/0/0
 ip address 10.1.1.2 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 mpls ip
 mpls label protocol ldp
 mls qos trust dscp
!
router ospf 1
 router-id 4.4.4.4
```

```
 network 4.4.4.4 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 2.2.2.2 remote-as 100
 neighbor 3.3.3.3 remote-as 100
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
 exit-address-family
!
```

PE2 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 102.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet4/0/0
 ip address 20.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet4/0/1.2
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 22.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 3.3.3.3 remote-as 100
```

```
 neighbor 3.3.3.3 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 remote-as 100
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
!
```

PE3 ルータでの設定（レシーバ PE）

```
ip vrf red2
 rd 10:2
 vpn id 10:2
 mdt default mpls mldp 4.4.4.4
 mdt data mpls mldp 100
 mdt data threshold 20
 route-target export 10:2
 route-target import 10:2
!
ip multicast-routing
ip multicast-routing vrf red2
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
interface Loopback102
 ip vrf forwarding red2
 ip address 103.2.0.2 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0.2
```

```
 encapsulation dot1Q 2
 ip vrf forwarding red2
 ip address 32.2.0.1 255.255.0.0
 ip pim sparse-mode
 ip igmp version 3
!
interface GigabitEthernet3/2/1
 ip address 30.1.1.1 255.255.255.0
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback1
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback1
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback1
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  neighbor 4.4.4.4 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf red2
  redistribute static
  redistribute connected
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
!
ip pim vrf red2 rp-address 11.11.11.11
!
```

LSM MLDP based MVPN サポートのトラブルシューティング

C7600 シリーズ ルータで LSM MLDP based MVPN サポートをトラブルシューティングするには、次のデバッグ コマンドを使用します。

コマンド	目的
debug platform software multicast ip cmfib event **debug platform software multicast ip cmfib error**	CMFIB の問題に使用。
debug platform software multicast ip hal error **debug platform software multicast ip hal event**	MET 関連の問題に使用（SP/DFC）。
debug mpls platform lsm vm error **debug mpls platform lsm vm event**	ラベル レプリケーション VLAN 関連の問題に使用（RP/SP/DFC）。
debug mpls mldp packet **debug mpls mldp neighbor** **debug mpls mldp all**	MLDP デバッグに使用（RP）。
debug ip igmp vrf blue	IGMP デバッグに使用。
debug ip pim vrf blue hello **debug ip pim vrf blue timer** **debug ip pim vrf blue bsr** **debug ip pim vrf blue auto-rp**	PIM デバッグに使用（RP）。

CHAPTER 48

PFC の MPLS QoS の設定

この章では、Cisco 7600 Policy Feature Card（PFC; ポリシー フィーチャ カード）3B、PFC3BXL、PFC3C、および PFC3CXL カードの 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）を設定する手順について説明します。特に説明がない場合、MPLS QoS の動作は、これらの PFC カードすべてで同じです。

（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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- PFC モード MPLS QoS では、第 45 章「PFC QoS の設定」で説明している PFC QoS 機能を備えた MPLS トラフィックが提供されます。
- この章では、PFC の MPLS QoS 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。
- PFC の MPLS QoS で利用できるすべてのポリシングおよびマーキングは、Modular QoS（MQC; モジュラ QoS）コマンドライン インターフェイス（CLI）から管理されます。QoS CLI（MQC）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）を作成して設定し、これらのトラフィック ポリシーをインターフェイスに付加することを可能にするコマンドライン インターフェイスです。MQC 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/qcfintro.html#wp998197

この章で説明する内容は、次のとおりです。

- 「用語」（P.48-2）
- 「PFC モード MPLS QoS 機能」（P.48-3）
- 「PFC モード MPLS QoS の概要」（P.48-4）
- 「PFC モード MPLS QoS」（P.48-5）
- 「PFC モード MPLS QoS の機能概要」（P.48-8）
- 「PFC MPLS QoS のデフォルト設定」（P.48-15）
- 「MPLS QoS コマンド」（P.48-16）
- 「PFC モード MPLS QoS の注意事項および制約事項」（P.48-17）
- 「PFC の MPLS QoS の設定」（P.48-17）
- 「MPLS DiffServ トンネリング モード」（P.48-31）

- 「ショート パイプ モードの設定」（P.48-35）
- 「均一モードの設定」（P.48-40）

用語

ここでは、MPLS QoS 用語を定義します。

- *サービス クラス*（CoS）：スイッチド ネットワークを通過するときにイーサネット フレームのプライオリティを示すスイッチ間リンク（ISL）ヘッダーまたは 802.1Q ヘッダーどちらかの 3 ビットのことです。802.1Q ヘッダーの CoS ビットは通常 802.1p ビットと呼ばれます。パケットがレイヤ 2 およびレイヤ 3 ドメインの両方を横断するときに QoS を維持するため、タイプ オブ サービス（ToS）値と CoS 値は互いにマッピングすることができます。
- *分類*：QoS をマーキングするトラフィックを選択する処理です。
- *DiffServ コード ポイント*（DSCP）：IP ヘッダーの ToS バイトの上位 6 ビットです。DSCP は、IP パケットだけに存在します。
- *E-LSP*：ラベル スイッチド パス（LSP）の 1 つであり、ノードはここで MPLS ヘッダーの Experimental（EXP）ビットから排他的に MPLS パケットの QoS 処理を判断します。QoS 処理が EXP（クラスおよびドロップ優先順位の両方）から判断されるため、いくつかのクラスのトラフィックを 1 つの LSP に多重化することができます（同じラベルを使用）。EXP フィールドは 3 ビット フィールドであるため 1 つの LSP は最大 8 つのトラフィックのクラスをサポートすることができます。コントロール プレーン トラフィック用にいくつかの値が予約されている場合、またはクラスのいくつかがそれらに対応するドロップ優先順位を持っている場合、クラスの最大数はさらに少なくなります。
- *EXP ビット*：ノードがパケットに与える QoS 処理（Per-Hop Behavior）を定義します。これは、IP ネットワークの DiffServ コード ポイント（DSCP）に相当します。DSCP は、クラスとドロップ優先順位を定義します。EXP ビットは、一般に IP DSCP でエンコードされた情報をすべて伝送するのに使用されます。ただし、ドロップ優先順位をエンコードするために EXP ビットが排他的に使用される場合もあります。
- *フレーム*は、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*：IP ヘッダーの ToS バイトの最上位 3 ビットです。
- *QoS タグ*：レイヤ 3 パケットおよびレイヤ 2 フレームで伝達されるプライオリティ値です。レイヤ 2 CoS ラベルは、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲です。レイヤ 3 IP precedence ラベルは、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲です。IP precedence 値は、1 バイトの ToS バイトの最上位 3 ビットで定義されます。レイヤ 3 DSCP ラベルは、0 ～ 63 の値を持つことができます。DSCP 値は 1 バイトの IP ToS フィールドのうち最上位 6 ビットで定義されます。
- *LER*（ラベル エッジ ルータ）：パケット上のラベルのインポーズおよびディスポーズを行うデバイスであり、プロバイダー エッジ（PE）ルータとも呼ばれます。
- *LSR*（ラベル スイッチング ルータ）：パケット上のラベルに基づいてトラフィックを転送するデバイスであり、プロバイダー（P）ルータとも呼ばれます。
- *マーキング*：パケットのレイヤ 3 DSCP 値を設定するプロセスです。マーキングはまた、MPLS EXP フィールドで異なった値を選択してパケットにマーキングし、輻輳時にパケットが必要なプライオリティを持つようにするプロセスでもあります。
- *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。ポリシングによって、トラフィックのマーキングまたはドロップが可能になります。

PFC モード MPLS QoS 機能

QoS により、ネットワークは選択されたネットワーク 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 PFC 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 実験フィールド」（P.48-3）
- 「信頼」（P.48-3）
- 「分類」（P.48-3）
- 「ポリシングおよびマーキング」（P.48-4）
- 「IP ToS の保持」（P.48-4）
- 「EXP 変換」（P.48-4）
- 「MPLS DiffServ トンネリング モード」（P.48-4）

MPLS 実験フィールド

MPLS EXP（実験）フィールド値を設定すると、サービス プロバイダーが自己のネットワークで伝送された IP パケット内で変更された IP precedence フィールドの値を望まない場合に、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 フィールドで異なった値を選択することにより、輻輳時にパケットが必要なプライオリティを持つようパケットをマーキングすることができます。

デフォルトでは、IP precedence 値はインポジション中に MPLS EXP フィールドにコピーされます。PFC モード MPLS QoS ポリシーにより MPLS EXP ビットをマーキングすることができます。

信頼

受信レイヤ 3 MPLS パケットに対し、PFC は、通常、受信最上位ラベルの 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

受信レイヤ 2 MPLS パケットの場合、PFC は、CoS および出力キュー処理の目的で、受信最上位ラベルの EXP 値を信頼するか、ポートまたはポリシーの信頼を MPLS パケットに適用できます。

分類

分類とはマーキングするトラフィックを選択するプロセスです。分類は、トラフィックを複数の優先順位レベル、つまり、サービス クラスに分割することによりこのプロセスを実施します。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プライマリ コンポーネントです。PFC は、（ポリシーのインストール後）受信 MPLS パケットの受信最上位ラベルの EXP ビットに基づいて分類を決定します。詳細については、「MPLS パケットを分類するためのクラス マップの設定」（P.48-20）を参照してください。

ポリシングおよびマーキング

ポリシングを行うと、設定レートを超えたトラフィックは廃棄されるか、またはより高いドロップ優先順位にマークダウンされます。マーキングは、パケット フローを識別して、これらを区別する手法です。パケット マーキングを利用すれば、ネットワークを複数の優先プライオリティ レベルまたはサービス クラスに分割することができます。

どの PFC モード MPLS QoS のポリシングおよびマーキング機能を実装できるかは、受信トラフィック タイプおよびトラフィックに適用される転送動作によって異なります。詳細については、「ポリシーマップの設定」（P.48-23）を参照してください。

IP ToS の保持

PFC は、インポジション、スワッピング、ディスポジションを含むすべての MPLS 動作中、自動的に IP ToS を保持します。IP ToS を保存する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 値を変換することができます。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。

- Optical Service Module（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、「PFC モード MPLS QoS の出力 EXP 変換の設定」（P.48-29）を参照してください。

MPLS DiffServ トンネリング モード

PFC は、MPLS DiffServ トンネリング モードを使用します。トンネリングは、ネットワークの 1 つのエッジから、そのネットワークの別のエッジまでの QoS 透過性を提供します。詳細については、「MPLS DiffServ トンネリング モード」（P.48-31）を参照してください。

PFC モード MPLS QoS の概要

ネットワーク管理者は PFC 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。差別化サービスは、QoS によって各送信パケットに指定されたサービスを提供することにより、幅広い要件を満たします。サービスは、IP パケット内の IP precedence ビット設定を使用するなどさまざまな方法で指定することができます。

IP precedence フィールドでの QoS の指定

IP パケットを 1 つのサイトから別のサイトへ送信する場合、IP precedence フィールド（IP パケットのヘッダーの DSCP フィールドの上位 3 ビット）が QoS を指定します。IP precedence マーキングに基づき、パケットにはその QoS に対して設定された処理が適用されます。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、ネットワークのエッジで IP precedence ビットが MPLS EXP フィールドにコピーされます。ただし、サービス プロバイダーは、ある MPLS パケットの QoS に、提供するサービスによって決定される異なった値を設定することが必要な場合もあります。

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 ヘッダーはカスタマーが利用できるよう引き続き利用可能であり、IP パケットの QoS はパケットが MPLS ネットワークを移動する間は変更されません。

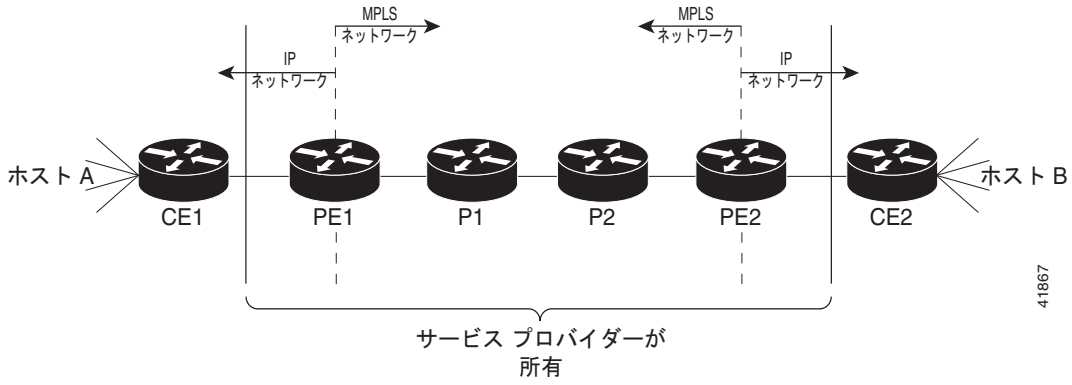
詳細については、「MPLS DiffServ トンネリング モード」（P.48-31）を参照してください。

PFC モード MPLS QoS

ここでは、PFC モード MPLS QoS の動作方法について説明します。

図 48-1 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 48-1　カスタマーの 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



このネットワークは両方向ですが、ここではパケットは左から右へ移動します。

図 48-1 の記号の意味は次のとおりです。

- CE1：カスタマー装置 1
- PE1：サービス プロバイダー入力ラベル エッジ ルータ（LER）
- P1：サービス プロバイダーのネットワークのコア内のラベル スイッチ ルータ（LSR）
- P2：サービス プロバイダーのネットワークのコア内の LSR
- PE2：サービス プロバイダー出力 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あります。

ここでは、MPLS ネットワーク内の LER と 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.48-6）
- 「MPLS ネットワークのコアにある LSR」（P.48-7）
- 「MPLS ネットワークの出力エッジでの LER」（P.48-7）

（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 ポートであるか、OSM 上の WAN ポートであるか、FlexWAN または拡張 FlexWAN モジュール上のポート アダプタであるかによって異なります。ここでは、LAN ポートの場合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、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 検索を通して着信 MPLS または MPLS VPN 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は、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 がパケットを次のように処理します。

1. レイヤ 2 またはレイヤ 3 トラフィックはエッジ LER（PE1）で MPLS ネットワークのエッジに入ります。
2. PFC 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 ビットを判別し、分類、マーキング、ポリシングを実行します。着信 IP パケットの分類については、入力サービス ポリシーもアクセス コントロール リスト（ACL）を使用することができます。
3. PFC または IP は各着信パケットについて IP アドレスで検索を実行し、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 決定の結果としての EXP 値はラベル ヘッダーの MPLS EXP フィールドにコピーされます。
5. PFC は、ラベル付きパケットを適切な処理用出力インターフェイスに転送します。
6. PFC はまた、802.1p ビットまたは IP ToS ビットを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クラスごとに区別され、マーキングまたはポリシングが行われます。LAN インターフェイスについては、出力分類はまだ MPLS ではなく IP に基づいて行われています。
8. （EXP によってマーキングされた）ラベル付きパケットは、コア MPLS ネットワークに送信されます。

MPLS ネットワークのコアにある 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方法について説明します。

1. エッジ LER（または他のコア デバイス）からの着信 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）がコア LSR に着信します。
2. PFC 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. PFC または LSR は、テーブル ルックアップを実施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配置（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. PFC は、ラベル付きパケットを適切な処理用出力インターフェイスに転送します。
6. PFC はまた、802.1p ビットまたは IP ToS ビットを出力インターフェイスに転送します。
7. 送信パケットは、MPLS EXP フィールドによって区別され、マーキングまたはポリシングが行われます。
8. （EXP によってマーキングされた）ラベル付きパケットは、コア MPLS ネットワークの別の LSR または出力エッジの LER に送信されます。

（注）　パケットは MPLS パケットであるため、サービス プロバイダー 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 フィールドはありません。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 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 がパケットを次のように処理します。

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）が MPLS ネットワーク バックボーンから接続される出力 LER（PE2）に着信します。
2. PFC は、パケットから MPLS ラベルをポップします（ディスポジション）。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、PFC 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、PFC 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。非集約ラベルについては、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 ルータではなく最後から 2 番めのホップ ルータでポップされます。
4. PFC はまた、802.1p ビットまたは IP ToS ビットを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、それに従って処理されます。

（注）　MPLS EXP ビットを使用すると、MPLS パケットの QoS を指定することができます。IP precedence および DSCP ビットを使用すると、IP パケットの QoS を指定することができます。

PFC モード MPLS QoS の機能概要

PFC モード MPLS QoS は、IP QoS をサポートします。MPLS パケットについては、PFC 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については、PFC モード MPLS QoS マーキングおよびポリシングの決定が、入力 PFC 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用に別途 QoS TCAM でプログラミングされます。Ternary Content Addressable Memory（TCAM）出力検索は、IP 転送テーブル（FIB）および NetFlow の検索が完了したあとで行われます。

各 QoS TCAM の検索結果により、ポリサー設定とポリシング カウンタを含む RAM へのインデックスが生成されます。追加 RAM マイクロフロー ポリサー設定が含まれ、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 エントリ内に維持されます。

入力および出力集約とマイクロフロー ポリシングの結果は統合されて最終ポリシング決定となります。アウトオブプロファイル パケットは、ドロップするか、DSCP 内でマークダウンすることがきます。

ここでは、次の PFC モード MPLS QoS について説明します。

- 「EoMPLS エッジの LER」（P.48-8）
- 「IP エッジ（MPLS、MPLS VPN）での LER」（P.48-9）
- 「MPLS コアでの LSR」（P.48-13）

（注）　ここでは、LAN ポート、OSM ポート、FlexWAN ポートの QoS 機能について説明します。別の機能がどのように動作するかについては、適切な資料を参照してください。

EoMPLS エッジの LER

ここでは、LER で機能する Ethernet over MPLS（EoMPLS）QoS の概要を説明します。EoMPLS QoS サポートは、IP から MPLS の QoS に似ています。

- EoMPLS では、ポートが untrusted の場合、CoS の信頼状態は自動的に 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。
- トンネル入力で受信されたパケットは、EoMPLS インターフェイスでは untrusted として扱われます。ただし、trust CoS が入力ポートで自動的に設定され、ポリシー マーキングが適用されない VC タイプ 4 は例外です。
- 入力ポートが trusted として設定された場合、EoMPLS インターフェイスで受信されたパケットは元の 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で機能します）。
- 802.1p CoS が 802.1q ヘッダーを介して利用可能な場合、802.1p CoS は入口から出口まで保持されます。
- トンネル出口から先では、1p タグが EoMPLS ヘッダー（VC タイプ 4）でトンネリングされている場合には、キューイングは保持された 802.1p CoS に基づいて行われます。それ以外の場合には、キューイングは QoS 決定から導出された CoS に基づいて行われます。

イーサネットから MPLS

Ethernet to MPLS の入力インターフェイス、PFC モード MPLS QoS、出力インターフェイスの機能は、IP to MPLS の対応する機能と同様です。詳細については、次の各項を参照してください。

- 「IP-to-MPLS 分類」（P.48-9）
- 「IP-to-MPLS の PFC モード MPLS QoS 分類」（P.48-10）
- 「IP-to-MPLS 入力ポートでの分類」（P.48-10）
- 「IP-to-MPLS 出力ポートでの分類」（P.48-10）

MPLS からイーサネット

MPLS to Ethernet については、出力 IP ポリシーが適用できない（パケットが MPLS としてだけ分類できる）EoMPLS カプセル開放の場合を除き、入力インターフェイス、PFC モード MPLS QoS、出力インターフェイスの機能は、MPLS to IP の対応する機能と同様です。詳細については、次の各項を参照してください。

- 「MPLS-to-IP 分類」（P.48-11）
- 「MPLS-to-IP の PFC3BXL または PFC3B モード MPLS QoS 分類」（P.48-11）
- 「MPLS-to-IP 入力ポートでの分類」（P.48-12）
- 「MPLS-to-IP 出力ポートでの分類」（P.48-12）.

IP エッジ（MPLS、MPLS VPN）での LER

ここでは、MPLS および MPLS VPN ネットワークの入力（CE-to-PE）および出力（PE-to-CE）エッジでの LER の QoS 機能について説明します。MPLS と MPLS VPN のどちらも一般 MPLS QoS 機能をサポートします。追加的な MPLS VPN 特定 QoS については「MPLS VPN」（P.48-12）を参照してください。

IP から MPLS

PFC は IP-to-MPLS エッジで次の MPLS QoS 機能を提供します。

- **mls qos trust** または **policy-map** コマンドに基づく EXP 値の割り当て
- ポリシーを利用した EXP 値のマーキング
- ポリシーを利用したトラフィックのポリシング

ここでは PFC3BXL または PFC3B が IP-to-MPLS エッジでサポートする MPLS QoS 分類について説明します。さらに、入力および出力インターフェイス モジュールによって提供される機能についても説明します。

IP-to-MPLS 分類

PFC の IP トラフィック用入力および出力ポリシーでは、IP precedence、IP DSCP、IP ACL の **match** コマンドを使用して元の受信 IP でトラフィックが分類されます。出力ポリシーでは、トラフィックはインポーズされた EXP 値や入力ポリシーによって行われたマーキングに基づいて分類されません。

PFC はポートの信頼および QoS ポリシーを適用したあと、内部 DSCP を割り当てます。次に PFC は、インポーズしたラベルに内部 DSCP-to-EXP グローバル マップに基づいて 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、EXP 値は各ラベルとも同じです。MPLS ラベルがインポーズされたとき、PFC は元の IP ToS を保持します。

PFC は、内部 DSCP-to-CoS グローバル マップに基づいて出力 CoS を割り当てます。デフォルトの内部 DSCP-to-EXP マップおよび内部 DSCP-to-CoS マップが整合している場合、出力 CoS はインポーズされた EXP と同じ値を持ちます。

入力ポートが IP-to-IP および IP-to-MPLS トラフィックの両方を受信した場合、分類を使用してこの 2 つのタイプのトラフィックを分離する必要があります。たとえば、IP-to-IP および IP-to-MPLS トラフィックの宛先アドレス範囲が異なっている場合、宛先アドレスに基づいてトラフィックを分類し、次に IP ToS ポリシーを IP-to-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）ポリシーを IP-to-MPLS トラフィックに適用することができます。次の 2 つの例を参照してください。

- IP ToS をマーキングするポリシーが内部 DSCP を設定：これがすべてのトラフィックに適用された場合、IP-to-IP トラフィックについては出力ポートが（内部 DSCP から導出された）CoS を出力パケットの IP ToS バイトに書き換えます。IP-to-MPLS トラフィックでは、PFC が内部 DSCP をインポーズされた EXP 値にマッピングします。
- MPLS EXP をマーキングするポリシーが内部 DSCP を設定：これがすべてのトラフィックに適用された場合、IP-to-IP トラフィックについては出力ポートが入力 IP ポリシー（または信頼）に従い IP ToS を書き換えます。CoS は ToS からマッピングされます。IP-to-MPLS トラフィックでは、PFC が内部 DSCP をインポーズされた EXP 値にマッピングします。

IP-to-MPLS の PFC モード MPLS QoS 分類

PFC モード MPLS QoS は、PE1 への入力時に次の内容をサポートします。

- IP precedence 値または DSCP 値に基づくマッチング、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

PFC 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-to-MPLS 入力ポートでの分類

IP- to- MPLS の分類は IP-to-IP と同じです。LAN ポートでの分類は、受信レイヤ 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レイヤ 3 IP ヘッダーの情報に基づいて分類を行います。

IP-to-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ます。出力 CoS 値は、その値からマッピングされます。

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 EXP 値のプロキシとして出力 CoS のマッチングを行うときにトラフィックを分類します。**match mpls experimental** コマンドは最上位ラベルの EXP 値のマッチングは行いません。

出力ポートがトランクである場合、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 から IP

PFC モード MPLS QoS は、MPLS-to-IP エッジで次の機能を提供します。

- 出力インターフェイスに従い MPLS ドメインからの送信時に EXP 値を IP DSCP に伝播するオプション
- MPLS-to-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-to-IP MPLS QoS 分類について説明します。さらに、入力および出力モジュールによって提供される機能についても説明します。

MPLS-to-IP 分類

PFC は QoS 結果に基づいて内部 DSCP（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 結果は次の影響を受けます。

- デフォルトの信頼 EXP 値
- ラベル タイプ（プレフィックス単位または集約）
- VPN の数
- 明示的 NULL の使用
- QoS ポリシー

次のような 3 つの異なった分類モードがあります。

- 正規 MPLS 分類：非集約ラベルについては、MPLS の再循環がないため、PFC 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-to-DSCP-to-CoS マッピングから導出された COS に基づいてパケットをキューに入れます。この基になる IP DSCP は、出力カプセル開放後保持されるか、（EXP-to-DSCP マップを介して）EXP から上書きされます。
- VPN CAM 内の集約ラベルの一致による IP 分類：PFC は、次のいずれかを行います。
  - 基礎となる IP ToS を保存
  - EXP-to-DSCP グローバル マップから導出された値によって IP ToS を書き換え
  - IP ToS を、出力 IP ポリシーから導出された値 に変更

  どの場合も、出力キューイングは DSCP-to-CoS マップから導出された最終 IP ToS に基づいています。
- VPN CAM にない集約ラベルでの IP 分類：再循環のあと、PFC は MPLS カプセル開放隣接で指定された入力予約 VLAN に基づき MPLS-to-IP パケットを正規 IP-to-IP パケットと区別します。予約された VLAN は VPN および非 VPN の両方について VRF に従い割り当てられます。再循環後の入力 ToS は元の IP ToS 値でも、元の EXP 値から導出したものでもかまいません。出力 IP ポリシーはこの入力 ToS を任意の値に上書きすることができます。

（注）　再循環の詳細については、「再循環」（P.26-4）を参照してください。

PE-to-CE 入力上の着信 MPLS パケットの場合、PFC では MPLS 分類だけがサポートされます。入力 IP ポリシーはサポートされません。MPLS コアからの PE-to-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-to-IP の PFC3BXL または PFC3B モード MPLS QoS 分類

PFC モード MPLS QoS は、PE2 への入力時に、EXP 値のマッチングおよび **police** コマンドをサポートします。

PFC モード MPLS QoS は、PE2 からの出力時に、IP precedence または DSCP 値のマッチング、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-to-IP 入力ポートでの分類

LAN ポートでの分類は、EXP 値に基づきます。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** コマンドは受信最上位ラベルの EXP 値のマッチングを行います。

MPLS-to-IP 出力ポートでの分類

（注） 出力分類キューイングは LAN および WAN ポートでは異なっています。

MPLS-to-IP の分類は、IP-to-IP と同じです。

LAN インターフェイス分類は出力 CoS に基づきます。OSM および FlexWAN インターフェイスは、送信された 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 PFC の QoS 機能または OSM QoS 機能を使用することができます。ただし、同じ出力ポリシーで両方を使用することはできません。

出力ポートがトランクである場合、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。

（注） MPLS to IP については、出力インターフェイスの MPLS IP（またはタグ IP）がイネーブルの場合は出力 IP ACL または QoS は出力インターフェイスでは有効ではありません。例外は VPN CAM ヒットです。この場合パケットは出力では IP として分類されます。

MPLS VPN

上記の情報のほかに、次の情報が MPLS VPN ネットワークに適用されます。

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介した CE-to-PE IP トラフィックの分類、ポリシング、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）

カスタマー エッジ（CE）-to-PE トラフィック、または CE-to-PE-to-CE トラフィックでは、サブインターフェイス サポートにより IP QoS 入力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することができます。CE 側のある VPN に対応する特定のインターフェイスまたはサブインターフェイスでは VPN 単位のポリシングも提供されます。

同じ VPN に属する複数のインターフェイスがある状況では、同じ PFC3BXL または PFC3B に対応するすべての類似インターフェイスについて、入力または出力サービス ポリシー内の同じ共有ポリサーを使用した VPN 単位のポリシング集約を実行することができます。

集約 VPN ラベルについては、再循環の場合の EXP 伝播はサポートされない可能性があります。これは、最終パケットがどの出力インターフェイスを使用するのかということを、MPLS 隣接が認識していないためです。

（注）　再循環については、「再循環」（P.26-4）を参照してください。

VPN 内のすべてのインターフェイスが EXP 伝播をイネーブルにしている場合、PFC は EXP 値を伝播します。

次の PE MPLS QoS 機能がサポートされています。

- IP パケット用の一般的な MPLS QoS 機能
- VPN サブインターフェイスを介した CE-to-PE IP トラフィックの分類、ポリシング、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 ネットワークのコア（MPLS-to-MPLS）での LSR の MPLS QoS 機能について説明します。Carrier Supporting Carrier（CsC）QoS 機能の入力機能、出力インターフェイス、および PFC の機能は、次の項で説明する MPLS to MPLS のものと同じです。CsC と MPLS to MPLS の相違は、CsC ラベルが MPLS ドメイン内部にインポーズできることです。

MPLS から MPLS

PFC モード MPLS QoS は MPLS コアで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
- 入力最上位 EXP 値を新たにインポーズされた EXP 値へのコピーすること
- MPLS ドメイン間の出力境界での EXP 変換オプション（隣り合った 2 つの MPLS ドメイン間でインターフェイス エッジ上の EXP 値を変更）
- 特定の EXP 値について個々のラベル フローに基づくマルチフロー ポリシング
- 最上位ラベルをマルチラベル スタックからポップする場合に最上位 EXP 値を基礎となる EXP 値へ伝播するオプション

ここでは、MPLS-to-MPLS の PFC モード MPLS QoS 分類について説明します。さらに、入力および出力モジュールによって提供される機能についても説明します。

MPLS-to-MPLS 分類

PFC は、受信 MPLS パケットについてポート信頼状態、入力 CoS、およびあらゆる policy-map **trust** コマンドを無視します。その代わり、PFC 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、PFC モード MPLS QoS の MPLS トラフィック用入力および出力ポリシーは、受信最上位ラベルの EXP 値に基づいてトラフィックを分類します。

PFC モード MPLS QoS は、EXP-to-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。 PFC の次の手順は、ラベルをスワッピングしているのか、新しいラベルをインポーズしているのか、それともラベルをポップしているのかによって異なります。

- ラベルのスワッピング：ラベルをスワッピングする場合、PFC は受信最上位ラベルの EXP 値を保持して、これを送信最上位ラベルの EXP 値にコピーします。PFC は、内部 DSCP-to-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 マップが整合している場合は、出力 CoS は送信最上位ラベルの EXP に基づきます。

PFC は、**police** コマンドの **exceed** および **violate** アクションを使用して、アウトオブプロファイル 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しないため、**conform** アクションは transmitted である必要があり、**set** コマンドを使用することはできません。PFC がマークダウンを実行している場合、内部 DSCP は内部 DSCP マークダウン マップへのインデックスとして使用されます。PFC は、内部 DSCP-to-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。PFC は新しい EXP 値を最上位送信ラベルに書き換え、新しい EXP 値をスタックの他のラベルにはコピーしません。PFC は、内部 DSCP-to-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 マップが整合している場合は、出力 CoS は送信最上位ラベルの EXP 値に基づきます。

- 追加ラベルのインポーズ：新しいラベルを既存のラベル スタックにインポーズする場合、PFC は内部 DSCP-to-EXP マップを使用して内部 DSCP をインポーズされたラベルの EXP 値にマッピングします。そして次にインポーズされたラベルの EXP 値を基礎となるスワップされたラベルにコピーします。PFC は、内部 DSCP-to-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 マップが整合している場合は、出力 CoS はインポーズされたラベルの EXP 値に基づきます。

  PFC は適合するトラフィックをマーキングし、アウトオブプロファイル トラフィックをマークダウンすることができます。PFC は、内部 DSCP をマーキングしたあと、内部 DSCP-to-EXP グローバル マップを使用して内部 DSCP を新しくインポーズされたラベルの EXP 値にマッピングします。そして PFC は、インポーズされたラベルの EXP 値を基礎となるスワップされたラベルにコピーします。PFC は、内部 DSCP-to-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 はインポーズされたラベルの EXP 値に基づきます。
- 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、PFC はエクスポーズされたラベルの EXP 値を保持します。PFC は、内部 DSCP-to-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 マップが整合している場合は、出力 CoS はポップされたラベルの EXP 値に基づきます。
- EXP 伝播が出力インターフェイスで設定されている場合、PFC は DSCP-to-EXP グローバル マップを使用して、エクス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。PFC は、内部 DSCP-to-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 マップが整合している場合は、出力 CoS はエクスポーズされたラベルの EXP 値に基づきます。

MPLS-to-MPLS の PFC モード MPLS QoS 分類

P1 または P2 への入力時に、PFC モード MPLS QoS は次の機能をサポートします。

- **mpls experimental topmost** コマンドによるマッチング
- **set mpls experimental imposition**、**police**、**set imposition** を併用する **police** コマンド

PFC モード MPLS QoS は、P1 または P2 からの出力時に **mpls experimental topmost** コマンドによるマッチングをサポートします。

MPLS-to-MPLS 入力ポートでの分類

LAN ポートでの分類は、PFC からの出力 CoS に基づきます。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** コマンドは受信最上位ラベルの EXP 値のマッチングを行います。

MPLS-to-MPLS 出力ポートでの分類

LAN ポートでの分類は、PFC からの出力 CoS 値に基づきます。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 のマッチングを行いますが、最上位ラベルの EXP 値のマッチングは行いません。

出力ポートがトランクである場合、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。

PFC MPLS QoS のデフォルト設定

ここでは、PFC での MPLS QoS のデフォルト設定について説明します。PFC には、次のグローバル MPLS QoS 設定があります。

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 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** ポートに限る）に、レイヤ 2 CoS を 0、インポーズされた EXP を 0 に設定します。trust CoS では、デフォルトの EXP 値が COS からマッピングされます。trust DSCP では、デフォルトの EXP 値が IP precedence からマッピングされます。OSM WAN ポート（デフォルトは trust DSCP）では、DSCP がインポーズされた EXP にマッピングされます。
PFC QoS 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 から DSCP へのマップ（EXP 値から設定された 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 から DSCP へのマップ（IP precedence 値から設定された 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 から EXP へのマップ （DSCP 値から設定された 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 マップからマークダウンされた DSCP	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	ラベル ＋ EXP 値
MPLS コア QoS	MPLS コア QoS では 4 つの可能性があります。 • スワッピング：着信 EXP フィールドが送信 EXP フィールドにコピーされます。 • スワッピング ＋ インポーズ：着信 EXP フィールドはスワッピングされた 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 フィールドのセット付きサービス ポリシーがある場合、その EXP フィールドはインポーズされたラベルとスワッピングされたラベルに置かれます。 • 最上位ラベルのディスポジション：エクスポーズされた EXP フィールドは保持されます。 • ラベルだけのディスポジション：エクスポーズされた IP DSCP は保持されます。
MPLS から IP エッジの QoS	エクスポーズされた IP DSCP を保持します。

MPLS QoS コマンド

Cisco 7600 PFC 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 コマンドについては、「PFC QoS の設定」（P.45-48）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**

PFC モード MPLS QoS の注意事項および制約事項

PFC の MPLS QoS を設定するときは、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-to-MPLS または EoMPLS のインポジション
  - QoS がディセーブルの場合、EXP 値は受信 IP ToS に基づきます。
  - QoS がキューイングだけの場合、EXP 値は受信 IP ToS に基づきます。
- 受信パケットが非 IP パケットの場合の 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 がキューイングだけの場合、EXP 値は受信 IP ToS に基づきます。
- MPLS-to-MPLS 動作
  - QoS がディセーブルのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
  - QoS がキューイングだけのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
- EXP 値は MPLS-to-IP ディスポジションとは関係がありません。
- **no mls qos rewrite ip dscp** コマンドは、MPLS とは非互換です。デフォルトの **mls qos rewrite ip dscp** コマンドは、PFC がインポーズしたラベルで正しい EXP 値を割り当てられるようイネーブルの状態にしておく必要があります。

PFC の MPLS QoS の設定

ここでは、PFC の MPLS QoS を設定する手順について説明します。

- 「QoS のグローバルなイネーブル化」（P.48-18）

- 「queueing-only モードのイネーブル化」（P.48-19）
- 「MPLS パケットを分類するためのクラス マップの設定」（P.48-20）
- 「入力ポートへの MPLS パケットの信頼状態の設定」（P.48-22）
- 「ポリシー マップの設定」（P.48-23）
- 「ポリシー マップの表示」（P.48-28）
- 「PFC モード MPLS QoS の出力 EXP 変換の設定」（P.48-29）
- 「EXP 値マッピングの設定」（P.48-30）

QoS のグローバルなイネーブル化

PFC で QoS を設定する前に、**mls qos** コマンドで 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。このコマンドはデフォルトのトラフィックの QoS 条件をイネーブルにします。

mls qos コマンドがイネーブルになると、PFC はプライオリティ値を各フレームに割り当てます。この値が内部 DSCP です。内部 DSCP は受信フレームの内容と QoS 設定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`	ルータで PFC QoS をグローバルにイネーブルにします。
	`Router(config)# no mls qos`	ルータで 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`	queueing-only モードをイネーブルにします。
	`Router(config)# no mls qos queueing-only`	PFC QoS をグローバルにディセーブルにします。 （注）　queueing-only モードを個別にディセーブルにすることはできません。
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、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）　ルータ 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

PFC で QoS がディセーブル（**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-to-MPLS または EoMPLS のインポジション
  - QoS がディセーブル（**no mls qos**）の場合、EXP 値は受信 IP ToS に基づきます。
  - QoS がキューイングだけ（**mls qos queueing-only**）の場合、EXP 値は受信 IP ToS に基づきます。
- 受信パケットが非 IP パケットの場合の 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 がキューイングだけの場合、EXP 値は受信 IP ToS に基づきます。
- MPLS-to-MPLS 動作
  - QoS がディセーブルのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。

  - QoS がキューイングだけのときにスワッピングする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がキューイングだけのときに追加ラベルをインポーズする場合、EXP 値は元の EXP 値に基づきます（EXP 変換がない場合）。
  - QoS がディセーブルのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
  - QoS がキューイングだけのときに 1 つのラベルをポップする場合、EXP 値は基礎となる EXP 値に基づきます。
- EXP 値は MPLS-to-IP ディスポジションとは関係がありません。

MPLS パケットを分類するためのクラス マップの設定

match mpls experimental topmost コマンドを使用して、パケット EXP 値による MPLS ドメイン内のトラフィック クラスを定義することができます。これにより、**police** コマンドを使用してインターフェイス ベースで EXP トラフィックをポリシングするためのサービス ポリシーを定義することができます。

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`	パケットがマッチングされるクラス マップを指定します。
ステップ 2	`Router(config-cmap)# match mpls experimental topmost value`	そのクラスにマッチングされ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 を含むすべてのパケットが exp3 という名前のトラフィック クラスによってマッチングされる例を示します。

```
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ときには、次の制約事項および注意事項が適用されます。

- **match mpls experimental** コマンドは、パケットがクラス マップによって指定されるクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用すべき EXP フィールド値の名前を指定します。
- **match mpls experimental** コマンドを使用するには、まず **class-map** コマンドを入力して設定する一致基準のクラスの名前を指定する必要があります。クラスを識別したあとで、**match mpls experimental** コマンドを使用してその一致基準を設定できます。
- クラス マップで複数のコマンドを指定する場合、最後に入力されたコマンドだけが適用されます。最後のコマンドは、それ以前に入力されたコマンドを無効にします。

入力ポートへの MPLS パケットの信頼状態の設定

no mls qos mpls trust exp コマンドを使用して、レイヤ 2 パケットに適用する同じ方法で、ポートまたはポリシーの信頼を MPLS パケットに適用できます。

入力ポートの MPLS パケッ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 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`	すべての信頼状態（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`	着信パケットの EXP 値だけが信頼される、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。

次に、着信 MPLS パケットが着信レイヤ 2 パケットと同じように動作するように、MPLS パケットの信頼状態を untrusted に設定する例を示します。

```
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

次の制約事項および注意事項は、**no mls qos mpls trust exp** コマンドを使用して入力ポートの MPLS パケットの信頼状態を設定する場合に適用されます。

- このコマンドは、レイヤ 2 およびレイヤ 3 パケットの両方に影響します。このコマンドは、レイヤ 2 スイッチド パケットによるインターフェイスでのみ使用してください。
- **no mls qos mpls trust exp** コマンドは、入力マーキングに影響します。分類には影響しません。

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。PFC の MPLS QoS は、一致したトラフィックに複数のポリシー マップ クラスからのコマンドを適用することはありません。

EXP 値をすべてのインポーズされたラベルに設定するためのポリシー マップの設定

MPLS EXP フィールドの値をすべてのインポーズされたラベル エントリに設定するには、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、コマンドの no 形式を入力します。

（注）　**set mpls experimental imposition** コマンドは、**set mpls experimental** コマンドと置き換わったものです。

	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 コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
ステップ 3	`Router(config-pmap-c)# set mpls experimental imposition {mpls-exp-value | from-field [table table-map-name]}`	MPLS 実験（EXP）フィールドの値をすべてのインポーズされたラベル エントリに設定します。
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 で定義される DSCP 値に従い 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、次の注意事項および制約事項に従ってください。

- ラベル インポジション中には **set mpls experimental imposition** コマンドを使用してください。このコマンドは MPLS EXP フィールドをすべてのインポーズされたラベル エントリに設定します。
- **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）上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。その代わり、このコマンドは内部 DSCP-to-EXP グローバル マップを介して EXP にマッピングされる内部 DSCP をマーキングします。
- （元の受信 IP ヘッダーに基づく）分類および（内部 DSCP に行われる）マーキングでは IP-to-IP トラフィックと IP-to-MPLS トラフィックが区別されないことに十分注意してください。IP ToS および EXP のマーキングに使用されるコマンドを使用した場合、内部 DSCP のマーキングと同じ結果となります。
- ラベル インポジション中に、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った値に設定するには、**set mpls experimental imposition** コマンドを使用します。
- また任意で IP precedence、DSCP フィールド、または QoS IP ACL とともに **set mpls experimental imposition** コマンドを利用して、すべてのインポーズされたラベル エントリに MPLS EXP フィールドの値を設定できます。
- ラベルを PFC で受信 IP トラフィックにインポーズする場合は、**set mpls experimental imposition** コマンドで EXP フィールドをマーキングすることができます。

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/12_3/switch/command/reference/swi_n1.html#wp1092877

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 クラスを特定のレートに速度制限する機能を提供する PFC のハードウェアの機能です。PFC 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、送信元、宛先、プロトコル、送信元ポート、宛先ポートが異なっていても関係なくポートに着信するすべてのトラフィックを測定します。マイクロフロー ポリシングは、フロー ベース（送信元、宛先、プロトコル、送信元ポート、宛先ポート ベース）でポートに着信するすべてのトラフィックを測定します。集約ポリシングとマイクロフロー ポリシングの詳細については、「ポリサー」（P.45-17）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 7600 Series Router Cisco IOS Command Reference*』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 コンフィギュレーション モードにアクセスして QoS クラス マップを設定します。
ステップ 3	Router(config-pmap-c)# **police** {**aggregate** *name*}	クラスを共有集約ポリサーに追加します。
ステップ 4	Router(config-pmap-c)# **police** *bps burst_normal burst_max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	per-class-per-interface ポリサーを作成します。
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 マップを設定するときには、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* コマンドおよび **violate-action** *action* コマンドが IP 使用と同様に動作します。パケットはドロップされる場合もあり、EXP 値がマークダウンされる場合もあります。これらのアクションが IP-to-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.45-65）を参照してください。
- MPLS では、**set-dscp transmit** *action* コマンドおよび **set-prec-transmit** *action* コマンドがキューイングに影響を与える CoS ビットにマッピングされる内部 DSCP を設定します。ただし、インポジションを除き EXP 値の変更は行いません。
- 受信 MPLS トラフィックのラベルを PFC でスワッピングするときは、**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、アウトオブプロファイル トラフィックをマークダウンすることができます。PFC では適合するトラフィックはマーキングされません。アウトオブプロファイル トラフィックをマークダウンする場合は、PFC は送信最上位ラベルをマーキングします。PFC はマーク ダウンをラベル スタックに伝播しません。
- 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。それ以外では、フロー キー動作は IP-to-IP と同様です。「ポリシー マップの設定」（P.45-65）を参照してください。
- **police** コマンドを使用すれば、ラベル インポジション中に、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った値に設定できます。

- ラベルを PFC で受信 IP トラフィックにインポーズする場合は、**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することができます。
- IP-to-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。ポリシーを設定して IP ToS をマーキングする場合は、PFC が EXP 値をマーキングします。

ポリシー マップの表示

MPLS QoS クラスのインターフェイス サマリーまたは指定されたインターフェイス上のすべてのサービス ポリシーで設定されたすべてのクラスのコンフィギュレーションでポリシー マップを表示することができます。

PFC モード MPLS QoS ポリシー マップのクラス サマリーの表示

PFC 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*}	PFC 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、PFC 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
```

すべてのクラスのコンフィギュレーションの表示

指定されたインターフェイス上のすべてのサービス ポリシーに設定されたすべてのクラスのコンフィギュレーションを表示するには、次の作業を行います。

コマンド	目的
Router# **show policy interface** *interface_type interface_number*	指定され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コンフィギュレーションを表示します。

次に、ファスト イーサネット インターフェイス 3/27 の全クラスのコンフィギュレーション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
```

PFC モード MPLS QoS の出力 EXP 変換の設定

ここでは、PFC の 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.48-29）
- 「インターフェイスへの出力 EXP 変換マップの付加」（P.48-30）

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、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 EXP 値を入力することができます。
- 複数のコマンドを入力して、追加の EXP 値を変換された EXP 値に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 値を変換するため、15 個の入力 EXP 変換マップを設定できます。入力 EXP 変換マップを、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 値から出力 EXP 値を導出します。入力 EXP 変換を設定する場合、PFC QoS は変換された EXP 値から入力 EXP 値を導出しません。

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手順について説明します。

- 「入力 EXP から内部 DSCP へのマッピングの設定」（P.48-30）
- 「名前付き出力 DSCP から出力 EXP へのマッピングの設定」（P.48-31）

入力 EXP から内部 DSCP へのマッピングの設定

入力 EXP から内部 DSCP 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 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 8 つの DSCP 値を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 から内部 DSCP へのマッピング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 から出力 EXP へのマッピングの設定

名前付き出力 DSCP から出力 EXP 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-exp dscp_values to exp_values`	名前付き出力 DSCP から出力 EXP へのマッピングを設定します。1 つの EXP 値には 1 回に最大 8 つの DSCP 値を入力することができます。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 から出力 EXP へのマッピング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

トンネリングは、QoS にネットワークの 1 つのエッジから、そのネットワークの別のエッジまでをトランスペアレントにする機能を提供します。トンネルは、ラベル インポジションのある場所から開始します。トンネルは、ラベル ディスポジションのある場所、つまり、ラベルがスタックから除去された場所で終了します。そしてパケットは下部に異なった Per-Hop Behavior（PHB）レイヤを持つ MPLS パケットとして、または IP PHB レイヤ付き IP パケットとして送信されます。

PFC では、ネットワーク経由でパケットを転送する方法が 2 つあります。

- ショート パイプ モード：ショート パイプ モードでは、出力 PE ルータは中間プロバイダー（P）ルータによって使用されるマーキングの代わりに元のパケット マーキングを使用します。EXP マーキングはパケット ToS バイトには伝播しません。

  モードの説明については、「ショート パイプ モード」（P.48-32）を参照してください。

  コンフィギュレーションについては、「ショート パイプ モードの設定」（P.48-35）を参照してください。

- 均一モード：均一モードでは、IP パケットのマーキングはサービス プロバイダーの QoS マーキングをコアに反映するよう操作することができます。このモードでは、CE およびコア ルータを含むネットワーク全体で矛盾のない QoS 分類およびマーキングが提供されます。EXP マーキングは基礎となる ToS バイトへ伝播されます。

  説明については、「均一モード」（P.48-33）を参照してください。

  設定手順については、「均一モードの設定」（P.48-40）を参照してください。

どちらのトンネリング モードもラベルがパケットに付与されたりパケットから削除されたりするエッジおよび最後から 2 番めのラベル スイッチング ルータ（LSR）の動作に影響を与えます。これらのモードは、中間ルータのラベル スワッピングには影響を与えません。サービス プロバイダーは、カスタマーごとに異なったタイプのトンネリング モードを選択することができます。

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

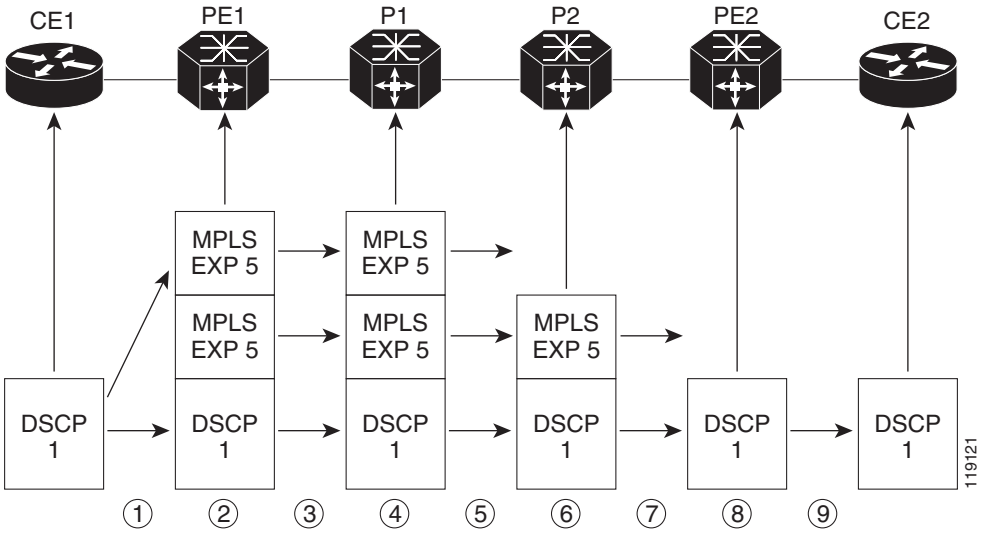
ショート パイプ モード

ショート パイプ モードはカスタマーおよびサービス プロバイダーが異なった DiffServ ドメインにある場合に使用されます。このモードを利用することにより、サービス プロバイダーはカスタマーの DiffServ 情報を保持しながら自身の DiffServ ポリシーを実施することができるため、サービス プロバイダー ネットワークを通して DiffServ の透過性が提供されます。

コアで実施される QoS ポリシーはパケット ToS バイトには伝播しません。MPLS EXP 値に基づく分類は、カスタマー側に向かう出力 PE インターフェイスで終了します。カスタマー側に向かう出力 PE インターフェイスは、元の IP パケット ヘッダーに基づいており、MPLS ヘッダーに基づいてはいません。

（注）　（カスタマーの PHB マーキングに基づいており、プロバイダーの PHB マーキングには基づいていない）出力 IP ポリシーが存在する場合は自動的にショート パイプ モードとなります。

図 48-2　VPN でのショート パイプ モード動作



ショート パイプ 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 で PE1 に送信します。
2. PE1 はインポーズされたラベル エントリで MPLS EXP フィールドを 5 に設定します。
3. PE1 はパケットを P1 に送信します。
4. P1 はスワッピングされたラベル エントリで MPLS EXP フィールド値を 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、QoS は IP DSCP 値に基づきます。

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

ショート パイプ モードの制約事項および注意事項

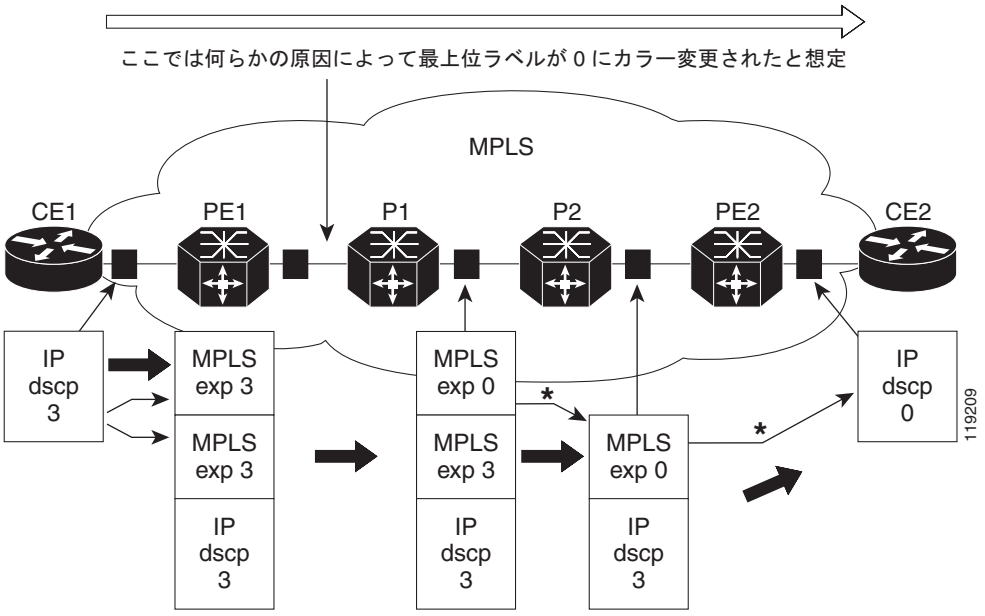
ショート パイプ モードでは次の制約事項が適用されます。

- MPLS-to-IP 出力インターフェイスが EoMPLS（隣接には End of Marker（EoM）ビット セットがある）である場合、ショート パイプ モードはサポートされません。

均一モード

均一モードでは、パケットは IP および MPLS ネットワークで一律に扱われます。つまり、IP precedence 値および MPLS EXP ビットは常に同じ PHB に対応しています。ルータがパケットの PHB の変更またはカラー変更をする場合はいつでも、その変更はすべてのカプセル化マーキングに伝播されなくてはなりません。パケット パス上のルータでのラベル インポジションまたはディスポジションにより PHB が追加またはエクスポーズされる場合、伝播はルータだけによって実行されます。カラーはすべてのレベルのすべての場所で反映される必要があります。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 48-3　　均一モード動作



*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。

この手順は、IP precedence ビット マーキングまたは DSCP マーキングが存在するかどう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発生します。

1. IP パケットがサービス プロバイダー エッジ ルータである PE1 で MPLS ネットワークに着信します。
2. ラベルはパケットにコピーされます。
3. MPLS EXP フィールド値のカラー変更が行われた場合（たとえば、あまりに多くのパケットが送信中であるためパケットがレート外となった場合）、この値は IGP ラベルにコピーされます。BGP ラベルの値は変更されません。
4. 最後から 2 番めのホップでは、IGP は削除されます。この値は次の低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 パケットとして送出されたパケットから削除されたとき、IP precedence または DSCP 値はコアで最後に変更された EXP 値として設定されます。

次に、IP precedence ビット マーキングが存在する例を示します。

1. CE1（カスタマー装置 1）で、IP パケットは IP precedence 値 3 を持っています。
2. パケットが PE1（サービス プロバイダーのエッジ ルータ）で MPLS ネットワークに着信すると、IP precedence 値 3 はパケットのインポーズされたラベル エントリにコピーされます。
3. IGP ラベル ヘッダーの MPLS EXP フィールドはマークダウンにより MPLS コア（たとえば P1）内で変更される可能性があります。

（注）　IP precedence ビットは 3 であるため、BGP ラベルおよび IGP ラベルも 3 を含みます。均一モードではラベルは常に同一であるためです。パケットは IP ネットワークと MPLS ネットワークで一律に扱われます。

均一モードの制約事項および注意事項

均一モードでは次の制約事項が適用されます。

- 出力 IP ACL またはサービス ポリシーが MPLS-to-IP 出口点で設定された場合には、再循環のため均一モードが常に実施されます。

MPLS DiffServ トンネリングの制約事項および使用上のガイドライン

ここでは、MPLS DiffServ トンネリングの制約事項および使用上のガイドラインについて説明します。

- MPLS EXP フィールドは 3 ビット フィールドであるため 1 つのラベルスイッチド パス（LSP）は最大 8 クラスのトラフィック（つまり、8 つの PHB）をサポートすることができます。
- 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 LSP の 1 つであり、ノードはここで MPLS ヘッダーの EXP ビットから排他的に MPLS パケットの QoS 処理を判別します。

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、PHB マーキングの追加レイヤをパケットに提供する機能です）。
- 管理されたカスタマー エッジ（CE）ルータでの制御による MPLS レイヤ管理の拡張性向上。

- MPLS はパケットの QoS をトンネリングすることができます（つまり、QoS はエッジ間でトランスペアレント）。QoS 透過性により、IP パケットの IP マーキングは MPLS ネットワーク全体で保持されます。
- MPLS EXP フィールドには、IP precedence または DSCP フィールドでマーキングされた PHB とは異なった値を別途マーキングすることができます。

ショート パイプ モードの設定

ここでは、ショート パイプ モードを設定する手順について説明します。

- 「入力 PE ルータ：カスタマー側に向かうインターフェイス」（P.48-35）
- 「入力 PE ルータの設定：P 側に向かうインターフェイス」（P.48-36）
- 「P ルータの設定：出力インターフェイス」（P.48-38）
- 「出力 PE ルータの設定：カスタマー側に向かうインターフェイス」（P.48-39）

（注）
- このステップは 1 つの方法を示すものですが、ショート パイプ モードを設定する唯一の方法というわけではありません。
- IP クラスを含む出力サービス ポリシーをインターフェイスに付加した場合、出力 PE（または PHP）でのショート パイプ モードは自動的に設定されます。

入力 PE ルータ：カスタマー側に向かうインターフェイス

この手順は、ポリシー マップを設定して、インポーズされたラベル エントリに MPLS EXP フィールドを設定するものです。

EXP 値を設定するには、入力 LAN または OSM ポートは untrusted である必要があります。FlexWAN ポートには trust の概念がありませんが、従来の Cisco IOS ルータと同様に、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場合）。

MPLS と VPN については、入力 PE はすべての入力 PFC IP ポリシーをサポートします。IP ACL/DSCP/precedence に基づく PFC IP ポリシーの分類については、http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/qos.htm を参照してください。

インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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。

	コマンド	目的
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 set-mpls-exp-transmit exp_value exceed-action drop`	ポリシングを設定します。ここでは、次の内容を設定します。 • サービス レベル契約（SLA）で指定されたレート制限に適合するパケットをとるアクション • SLA で指定されたレート制限を超えるパケットをとるアクション。 *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、インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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 側に向かうインターフェイス

この手順は MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するものです。

（注）　ここで示す QoS 機能は、OSM および FlexWAN および拡張 FlexWAN モジュールに限り使用可能です。

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、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*	どのパケットがマッピング（マッチング）されるのかを示すクラス 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*	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 4	Router(config)# **policy-map** *name*	1 つまたは複数のクラスに一致するパケットの 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 クラスをサービス ポリシーに関連付けます。
ステップ 6	Router(config-p-map-c)# **bandwidth** {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
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**	帯域幅保証を持つトラフィック クラスの WRED ドロップ 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、そのインターフェイスを脱退するパケット上で適用すべき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、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
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 および FlexWAN および拡張 FlexWAN モジュールに限り使用可能です。

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、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`	どのパケットがマッピング（マッチング）されるのかを示すクラス 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`	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 4	`Router(config)# policy-map name`	1 つまたは複数のクラスに一致するパケットの 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 クラスをサービス ポリシーに関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
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`	WRED を IP precedence または MPLS EXP フィールド値に基づく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、そのインターフェイスを脱退するパケット上で適用すべき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、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
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：カスタマー側に向かうインターフェイス

（注）　ここで示す QoS 機能は、OSM および FlexWAN および拡張 FlexWAN モジュールに限り使用可能です。

IP DSCP 値に基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、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`	どのパケットがマッピング（マッチング）されるのかを示すクラス 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`	1 つまたは複数のクラスに一致するパケットの 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 クラスをサービス ポリシーに関連付けます。
ステップ 6	`Router(config-p-map-c)# bandwidth {bandwidth_kbps | percent percent}`	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
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`	帯域幅保証を持つトラフィック クラスの WRED ドロップ 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、そのインターフェイスを脱退するパケット上で適用すべき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、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
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)# service-policy output output-qos
```

均一モードの設定

ここでは、次の設定を行う手順について説明します。

- 「入力 PE ルータの設定：カスタマー側に向かうインターフェイス」（P.48-40）
- 「入力 PE ルータの設定：P 側に向かうインターフェイス」（P.48-41）
- 「出力 PE ルータの設定：カスタマー側に向かうインターフェイス」（P.48-42）

（注）　このステップは 1 つの方法を示すものですが、均一モードを設定する唯一の方法というわけではありません。

入力 PE ルータの設定：カスタマー側に向かうインターフェイス

均一モードでは、信頼状態を IP precedence または IP DSCP に設定すると PFC は IP PHB を MPLS PHB にコピーすることができます。

（注）　この説明は、LAN または OSM ポートの PFC QoS 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

インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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 transmit exceed-action drop**	ポリシングを設定します。ここでは、次の内容を設定します。 • SLA で指定されたレート制限に適合するパケットをとるアクション。 • SLA で指定されたレート制限を超えるパケットをとるアクション。
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、インポーズされたラベル エントリで MPLS EXP フィールドを設定するポリシー 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 ルータの設定：P 側に向かうインターフェイス

MPLS EXP フィールドに基づいてパケットを分類し、適切な廃棄およびスケジューリング処理を提供するには、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*	どのパケットがマッピング（マッチング）されるのかを示すクラス 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*	パケットがそのクラスに属しているかどうかを判別するためにパケットをチェックする一致基準として使用する MPLS EXP フィールド値を指定します。
ステップ 4	Router(config)# **policy-map** *name*	1 つまたは複数のクラスに一致するパケットの 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 クラスをサービス ポリシーに関連付けます。

	コマンド	目的
ステップ 6	Router(config-p-map-c)# **bandwidth** {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。
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**	帯域幅保証を持つトラフィック クラスの WRED ドロップ 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、そのインターフェイスを脱退するパケット上で適用すべき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、適切な廃棄およびスケジューリング処理を提供する例を示します。

```
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：カスタマー側に向かうインターフェイス

カスタマー側に向かう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*	どのパケットがマッピング（マッチング）されるのかを示すクラス 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識別します。
ステップ 4	Router(config)# **policy-map** *name*	1 つまたは複数のクラスに一致するパケットの 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 クラスをサービス ポリシーに関連付けます。
ステップ 6	Router(config-p-map-c)# **bandwidth** {*bandwidth_kbps* | **percent** *percent*}	トラフィック クラスに最小帯域幅保証を指定します。kbps（キロビット/秒）または全体的な帯域幅のパーセント値で最小帯域幅保証を指定することができます。

	コマンド	目的
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`	WRED を IP precedence または MPLS EXP フィールド値に基づく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`	EXP 値が MPLS ドメイン出口 LER 出力ポートで基礎となる IP DSCP へ伝播するの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、そのインターフェイスに着信するパケット上で適用すべき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、カスタマー側に向かう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 49

IEEE 802.1x ポートベースの認証の設定

この章では、認証されていないデバイス（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「IEEE 802.1x ポートベースの認証の概要」（P.49-1）
- 「IEEE 802.1x ポートベースの認証のデフォルト設定」（P.49-6）
- 「IEEE 802.1x ポートベースの認証時の注意事項および制約事項」（P.49-7）
- 「IEEE 802.1x ポートベースの認証の設定」（P.49-7）
- 「IEEE 802.1x ステータスの表示」（P.49-17）

IEEE 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 コントロール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、ルータ ポートに接続する各クライアントを認証したうえで、ルータや 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 コントロールでは、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、802.1x ポートベースの認証について説明します。

- 「デバイスの役割」（P.49-2）
- 「認証の開始およびメッセージ交換」（P.49-3）
- 「許可ステートおよび無許可ステートのポート」（P.49-4）
- 「DHCP スヌーピングでの IEEE 802.1X 認証の使用」（P.49-5）
- 「サポートされるトポロジ」（P.49-5）

デバイスの役割

IEEE 802.1x ポート ベースの認証では、図 49-1 に示すように、ネットワーク上のデバイスにはそれぞれ特定の役割があります。

図 49-1　802.1X デバイスのロール

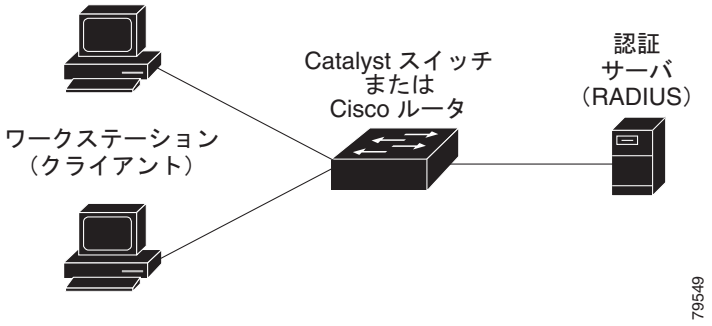


図 49-1 に示す特定の役割は、次のとおりです。

- *クライアント*：LAN およびルータ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションは、Microsoft Windows XP オペレーティング システムで提供されているような 802.1x 準拠のクライアント ソフトウェアを実行する必要があります （クライアントは、802.1x 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 ポートベース認証の問題に関しては、次の URL にある Microsoft Knowledge Base を参照してください。
  http://support.microsoft.com/kb/q303597/

- *認証サーバ*：実際にクライアントの認証を行います。認証サーバは、クライアントのアイデンティティを確認し、そのクライアントの LAN およびルータ サービスへのアクセスが許可されるかどうかをルータに通知します。ルータ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トランスペアレントに行われます。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。

- *ルータ（オーセンティケータおよびバックエンドのオーセンティケータともいう）*：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的アクセスを制御します。ルータ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。ルータには、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。

  ルータが 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。ルータ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

ルータ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、ルータはポートのリンク 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、ルータは 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（ルータは通常、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。

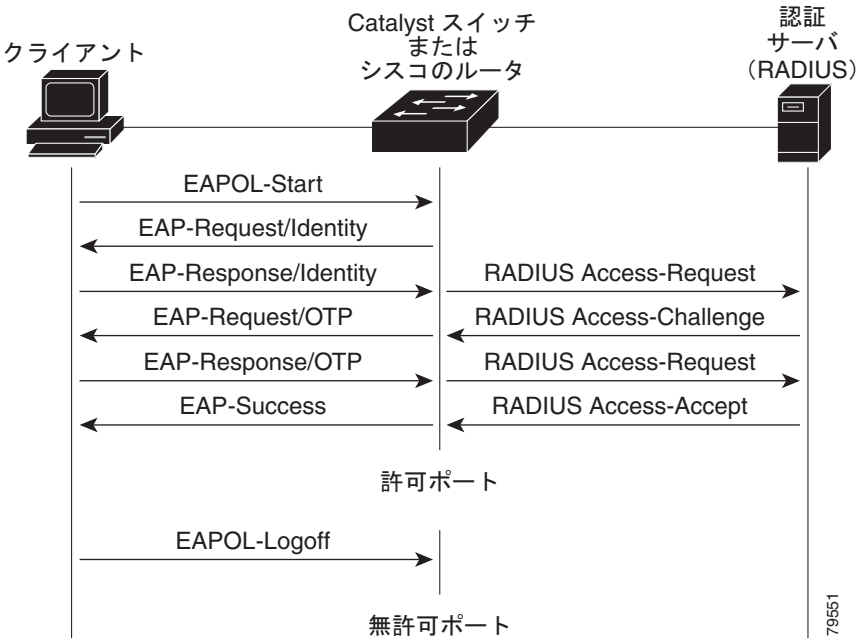
ただし、クライアントが起動時にルータから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始することができます。このフレームはルータに対し、クライアントのアイデンティティを要求するように指示します。

（注）　ネットワーク アクセス デバイスで IEEE 802.1x 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 EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートにあるかのようにフレームの送信を開始します。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.49-4）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、ルータ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、ルータ 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.49-4）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 49-2 に、クライアントが RADIUS サーバとの間でワンタイム パスワード（OTP）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 49-2　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

ルータ ポート ステートによって、クライアントがネットワーク アクセスを許可されているかどうか判別できます。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 IEEE 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、ルータはそのクライアントのアイデンティティを要求します。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のままであり、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。

これに対し、802.1x 対応のクライアントが、802.1x プロトコルプロトコルを実行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。応答が得られないため、クライアントはポートが許可ステートにあるかのようにフレームの送信を開始します。

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て、必要な認証交換を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の 802.1x ベース認証なしで通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized**：ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。ルータは、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て、ポートに無許可ステートを開始させ、EAPOL フレームだけがポートを通じて送受信できるようにします。ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。ルータは、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。ルータはクライアントの MAC 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。

クライアントが正常に認証されると（認証サーバから Accept フレームを受信する）、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のフレームはすべてそのポートを通じて許可されます。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、ルータ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、ルータ 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。

DHCP スヌーピングでの IEEE 802.1X 認証の使用

データ挿入機能を備えたダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングの Option 82 がイネーブルになると、ルータがクライアントの IEEE 802.1X 認証されたユーザ ID 情報を DHCP ディスカバリ プロセスに挿入でき、DHCP サーバが IP アドレスを別の IP アドレス プールから別のエンド ユーザのクラスに割り当てられます。この機能によって、アカウンティングのためにエンド ユーザに与えられた IP アドレスをセキュリティ保護し、レイヤ 3 基準に基づいてサービスを許可できます。

802.1X の認証に成功した後、ポートはフォワーディング ステートとなり、RADIUS サーバから受信した属性を保存します。DHCP スヌーピングを実行している場合、ルータは DHCP リレー エージェントとして機能し、DHCP メッセージを受信し、別のインターフェイスで送信のためにこれらのメッセージを再度生成します。

802.1X 認証後、クライアントが DHCP ディスカバリ メッセージを送信すると、ルータはパケットを受信し、RADIUS 属性サブオプション セクションを、クライアントの保存されている RADIUS 属性を含むパケットに追加します。ルータは、その後、ディスカバリ ブロードキャストを再度送信します。DHCP サーバは変更された DHCP ディスカバリ パケットを受信し、IP アドレスの割り当ての作成時に認証されたユーザ ID 情報を使用できます（設定されている場合）。

ユーザの IP アドレスへのマッピングは、1 対 1、1 対多、多対多で実行できます。1 対多のマッピングでは、同じユーザが複数のポートで 802.1X ホストによって認証を行えます。

801.X 認証とデータ挿入機能を備えた DHCP スヌーピングの Option 82 がイネーブルの場合は、ルータが認証されたユーザ ID 情報を自動的に挿入します。データ挿入機能を備えた DHCP スヌーピングの Option 82 を設定するには、37-3 ページの「DHCP スヌーピングの Option 82 データ挿入」の項を参照してください。

RADIUS 属性サブオプションで挿入されるデータについては、RFC 4014『Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option』を参照してください。

サポートされるトポロジ

IEEE 802.1x ポート ベース認証は、次の 2 つのトポロジーでサポートされます。

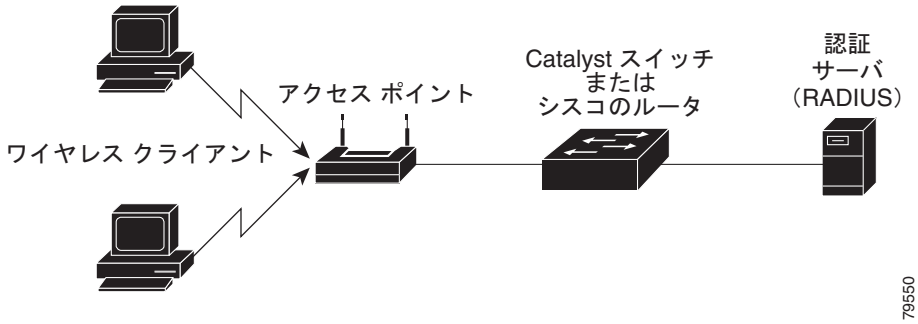
- ポイントツーポイント

- ワイヤレス LAN

ポイントツーポイントの構成（図 49-1（P.49-2）を参照）では、802.1x 対応のルータ ポートに接続できるクライアントは、1 台だけです。ルータは、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替わったときには、ルータはポートのリンク 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 49-3 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）、ルータ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。このトポロジーでは、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、ルータに対するクライアントとしての役割を果たします。

図 49-3　　ワイヤレス LAN の例



IEEE 802.1x ポートベースの認証のデフォルト設定

表 49-1 に、IEEE 802.1x のデフォルト設定を示します。

表 49-1　　802.1X のデフォルト設定

機能	デフォルト設定
認証、許可、アカウンティング（AAA）	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 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）認証ポート	1812
RADIUS サーバ キー	指定なし
インターフェイスごとの 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の 802.1x ベース認証なしで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（ルータがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数）

表 49-1　802.1X のデフォルト設定 （続き）

機能	デフォルト設定
再送信時間	30 秒（ルータが 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（ルータ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、クライアントに要求を再送信するまでにルータが応答を待機する時間）
認証サーバ タイムアウト時間	30 秒（認証サーバからの応答をクライアントにリレーするとき、ルータが応答を待ち、クライアントに要求を再送信するまでの時間）

IEEE 802.1x ポートベースの認証時の注意事項および制約事項

IEEE 802.1x ポートベースの認証を設定する場合、次の注意事項および制約事項に従ってください。

- 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。
  - スイッチド ポート アナライザ（SPAN）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 をイネーブルにすることができます。

IEEE 802.1x ポートベースの認証の設定

ここでは、IEEE 802.1x ポートベースの認証の設定方法を説明します。

- 「IEEE 802.1x ポートベースの認証のイネーブル化」（P.49-8）
- 「ルータと RADIUS サーバ間の通信設定」（P.49-9）
- 「定期的な再認証のイネーブル化」（P.49-11）
- 「手動によるポート接続クライアントの再認証」（P.49-12）
- 「ポート接続クライアント認証の初期化」（P.49-12）
- 「待機時間の変更」（P.49-13）
- 「ルータとクライアント間の EAP 要求フレーム再送信時間の設定」（P.49-14）
- 「ルータと認証サーバ間のレイヤ 4 パケット再送信時間の設定」（P.49-15）
- 「ルータとクライアント間のフレーム再送信回数の設定」（P.49-15）
- 「複数ホストのイネーブル化」（P.49-16）
- 「IEEE 802.1x 設定をデフォルト値にリセットする方法」（P.49-17）

IEEE 802.1x ポートベースの認証のイネーブル化

IEEE 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、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

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、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# configure terminal`	グローバル コ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)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	`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。
ステップ 4	`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。
ステップ 5	`Router(config)# interface type 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。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 6	`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。

	コマンド	目的
ステップ 7	`Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Router# show dot1x all`	入力を確認します。 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。

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が、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 つを入力します。
  - **group radius**：すべての RADIUS サーバのリストを認証に使用します。
  - **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、クライアントはルータ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
```

ルータと 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、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

RADIUS サーバ パラメ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# configure terminal`	グローバル コ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 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。
ステップ 3	`Router(config)# radius-server host` {*hostname* | *ip_address*}	ルータに RADIUS サーバ ホスト名や 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。
ステップ 4	`Router(config)# radius-server key` *string*	ルータと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する、認証キーおよび暗号化キーを設定します。
ステップ 5	`Router(config)# end`	特権 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、ルータと 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キーおよび暗号化キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。このキーは RADIUS デーモンで使用する暗号と一致する必要があります。
- **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、すべての RADIUS サーバに対してタイムアウト、再送信回数、暗号キーの値を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』と『*Cisco IOS Security Command Reference*, Release 12.2』を参照してください。

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

（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、ルータの IP アドレス、およびサーバとルータ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、ルータで 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

IEEE 802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定することができます。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、3600 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.49-12）を参照してください。

インターフェイス コンフィギュレーション モードで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 slot/port*	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
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。
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 3600 秒です。 このコマンドがルータに影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 4	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show dot1x all`	入力を確認します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定して、入力を確認する例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 4000
Router(config-if)# end
Router# show dot1x all
```

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、すでに認証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す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 slot/port*	ポートに接続するクライアントを手動で再認証します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	Router# **show dot1x all**	入力を確認します。

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し、入力を確認する例を示します。

```
Router# dot1x re-authenticate interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
Router# show dot1x all
```

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、既存の認証を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、特権 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# **dot1x initialize interface** *type 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。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	Router# **show dot1x all**	入力を確認します。

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し、入力を確認する例を示します。

```
Router# dot1x initialize interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
Router# show dot1x all
```

待機時間の変更

ルータがクライアントを認証できなかった場合は、ルータ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、インターフェイス 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 slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout quiet-period seconds`	ルータ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 秒です。デフォルトは 60 秒です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータの待機時間を 30 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout quiet-period 30
Router(config-if)# end
Router# show dot1x all
```

ルータとクライアント間の再送信時間の変更

クライアントはルータからの 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。ルータ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。

ルータ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、インターフェイス 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 slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout tx-period seconds`	ルータが 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 秒です。デフォルトは 30 秒です。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータが 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 秒に設定して、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x timeout tx-period 60
Router(config-if)# end
Router# show don1x all
```

ルータ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ルータに通知します。ルータがこの通知を受信できなかった場合、ルータ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。ルータが通知を待機する時間は、1 ～ 65535 秒の範囲に指定できます （デフォルトは 30 秒です）。

ルータ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、インターフェイス 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 slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout supp-timeout seconds`	ルータ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。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータ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 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x timeout supp-timeout 25
Router(config-if)# end
Router# show dot1x all
```

ルータ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ルータに通知します。ルータがパケット送信後、通知を受信できない場合、ルータ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。ルータが通知を待機する時間は、1 ～ 65535 秒の範囲に指定できます （デフォルトは 30 秒です）。

ルータから認証サーバへレイヤ 4 パケットを再送信する時間を設定するには、インターフェイス 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 slot/port*	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x timeout server-timeout` *seconds*	ルータ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。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータ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 秒に設定し、入力を確認する例を示します。

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# dot1x timeout server-timeout 25
Router(config-if)# end
Router# show dot1x all
```

ルータとクライアント間のフレーム再送信回数の設定

ルータ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、（クライアントから応答が得られなかった場合に）ルータが認証プロセスを再起動する前に、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。

ルータ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、インターフェイス 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 slot/port*	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 2	`Router(config-if)# dot1x max-req` *count*	ルータ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。

	コマンド	目的
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

次に、ルータが認証プロセスを再起動する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定し、入力を確認する例を示します。

```
Router(config)# interface fastethernet 4/1
Router(config-if)# dot1x max-req 5
Router(config-if)# end
Router# show dot1x all
```

複数ホストのイネーブル化

図 49-3（P.49-6）に示すように、1 つの IEEE 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、インターフェイス 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 slot/port*	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
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。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

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して入力を確認する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x host-mode multi-host
Router(config-if)# end
Router# show dot1x all
```

IEEE 802.1x 設定をデフォルト値にリセットする方法

IEEE 802.1x 設定をデフォルト値に戻すには、インターフェイス 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 slot/port`	設定するインターフェイスを選択します。 *type*—**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
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`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show dot1x all`	入力を確認します。

IEEE 802.1x ステータスの表示

ルータのグローバルな IEEE 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** 特権 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* 特権 EXEC コマンドを使用します。

これらのコマンドのキーワードと引数の詳細については『*Cisco IOS Security Command Reference, Release 12.2 SR*』を参照してください。

CHAPTER 50

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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.50-1）
- 「デフォルトのポート セキュリティ設定」（P.50-3）
- 「ポートセキュリティに関する注意事項および制約事項」（P.50-3）
- 「ポート セキュリティの設定」（P.50-4）
- 「ポート セキュリティ設定の表示」（P.50-11）

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」（P.50-1）
- 「スティッキ MAC アドレスによるポート セキュリティ」（P.50-2）

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 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、ポートの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のグループ外に送信元アドレスがある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デバイスはそのポートの全帯域を使用できます。

次のいずれかの場合に、セキュリティ違反が発生します。

- ポート セキュリティは、セキュア MAC アドレスがセキュア ポートで最大数に達した場合に、識別されたどのセキュア MAC アドレスとも入力トラフィックの送信元 MAC アドレスが異なると、設定された違反モードを適用します。
- ポート セキュリティは、特定のセキュア 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 VLAN 上の別のセキュア ポートにアクセスしようとすると、シャットダウン違反モードを適用します。

（注）　特定のセキュア 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、同一 VLAN 上の別のポートでポート セキュリティがセキュア MAC アドレスを検出したときに発生する一連のイベントは、MAC 移動の違反と呼ばれます。

違反モードの詳細については、「ポートでのポート セキュリティ違反モードの設定」（P.50-6）を参照してください。

ポートにセキュア MAC アドレスの最大数を設定すると、ポート セキュリティによって、次のいずれかの方法でアドレス テーブルにセキュア アドレスが組み込まれます。

- 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。
- 接続されているデバイスの MAC アドレスで、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することができます。
- アドレス数をいくつかスタティックに設定し、残りのアドレスがダイナミックに設定されるようにすることができます。

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。

起動、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、ポート セキュリティは、ダイナミックに学習された MAC アドレスをアドレス テーブルに読み込みません。

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。

protect、restrict、または shutdown の違反モードのいずれかにポートを設定できます。「ポート セキュリティの設定」（P.50-4）を参照してください。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

スティッキ MAC アドレスによるポート セキュリティ

スティッキ 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、スティッキ MAC アドレスはダイナミックに学習できます。

スティッキ 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。

write memory または **copy running-config startup-config** コマンドを入力すると、スティッキ MAC アドレスによるポート セキュリティは、ダイナミックに学習された MAC アドレスを startup-config ファイルに保存します。したがって、起動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。

デフォルトのポート セキュリティ設定

表 50-1 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 50-1　デフォルトのポート セキュリティ設定

機能	デフォルト設定
ポート セキュリティ	ポートで、ディセーブルに設定されています。
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、SNMP 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、次の注意事項に従ってください。

- errdisable ステートのセキュア ポートを、デフォルトのポート セキュリティ設定によって回復するには、**errdisable recovery cause shutdown** 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、このセキュア ポートを手動で再びイネーブルに戻すこともできます。
- 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 7600 Series Router Cisco IOS Command Reference*』を参照してください
- ポート セキュリティは、許可された MAC アドレスを特定のビット セットとともに学習します。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）。
- スティッキ 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、起動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。
- ポート セキュリティは、Private VLAN（PVLAN; プライベート VLAN）ポートをサポートします。
- ポート セキュリティは、非交渉トランクをサポートします。
  - 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、ポート セキュリティは、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スティッキおよびスタティック セキュア アドレスを、トランクのネイティブ VLAN 上のスティッキまたはスタティック セキュア アドレスに変換します。ポート セキュリティによって、アクセス ポートの音声 VLAN 上のすべてのセキュア 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、ポート セキュリティは、ネイティブ VLAN で学習されたすべてのスティッキおよびスタティック アドレスを、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します。ポート セキュリティによって、ネイティブ VLAN 以外の VLAN で学習されたすべてのアドレスが削除されます。

（注）　ポート セキュリティは、IEEE 802.1Q トランクおよび ISL トランク双方に対し、**switchport trunk native vlan** コマンドで設定した VLAN ID を使用します。

- ポート セキュリティは、トランクをサポートします。
- ポート セキュリティは、IEEE 802.1Q トンネル ポートをサポートします。
- ポート セキュリティは、スイッチド ポート アナライザ（SPAN）宛先ポートをサポートしません。
- ポート セキュリティは、EtherChannel のポートチャネル インターフェイスをサポートしません。
- 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。

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」（P.50-4）
- 「ポートでのポート セキュリティ違反モードの設定」（P.50-6）
- 「ポートでのセキュア MAC アドレスの最大数の設定」（P.50-7）
- 「スティッキ 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.50-8）
- 「ポートでのスタティック セキュア MAC アドレスの設定」（P.50-9）
- 「ポートでのセキュア MAC アドレスのエージング設定」（P.50-10）

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に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」（P.50-5）
- 「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」（P.50-5）

トランクでのポート セキュリティのイネーブル化

ポート セキュリティは、非交渉トランクをサポートします。

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（「ポートでのセキュア MAC アドレスの最大数の設定」（P.50-7）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**	DTP 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）**　ポートは、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。

	コマンド	目的
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、次の点に注意してください。

- **protect**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットを廃棄します。
- **restrict**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットを廃棄し、SecurityViolation カウンタを増分させます。
- **shutdown**：インターフェイスをただちに errordisable ステートにして、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。

次に、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 3/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface fastethernet 5/12 | include Protect
Violation Mode             : Protect
```

次に、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 3/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface fastethernet 5/12 | include Restrict
Violation Mode             : Restrict
```

ポートでのセキュア MAC アドレスの最大数の設定

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、次の点に注意してください。

- *number_of_addresses* の有効範囲は 1 ～ 4,097 です。
- ポート セキュリティは、トランクをサポートします。
  - トランクでは、トランクおよびトランク上のすべての VLAN に対して、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 範囲は、一組の VLAN 番号をダッシュ（-）でつなげて入力します。
  - 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、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 3/12
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
```

スティッキ 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

スティッキ 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`	スティッキ 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`	スティッキ 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**

スティッキ 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、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、スティッキ 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、スティッキ 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、スティッキ 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、スティッキ 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スティッキ 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。
- スティッキ 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、起動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、スティッキ 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
```

ポートでのスタティック セキュア MAC アドレスの設定

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、次の点に注意してください。

- スティッキ 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、スティッキ セキュア MAC アドレスを設定できます（「スティッキ 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.50-8）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。
- トランクでは、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 アドレスおよびスティッキ 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.50-10）
- 「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.50-11）

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 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。

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**

次に、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 5/1
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**]	ルータ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、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** キーワードを入力してセキュア 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表示します。

```
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** 特権 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 51

UDLD の設定

この章では、Cisco 7600 シリーズ ルータに 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「UDLD の機能概要」（P.51-1）
- 「UDLD のデフォルト設定」（P.51-3）
- 「UDLD の設定」（P.51-3）

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」（P.51-1）
- 「UDLD アグレッシブ モード」（P.51-2）

UDLD の概要

シスコ独自の 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デバイスで、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、ネイバーの 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。

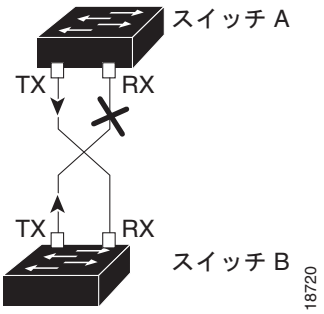
リンク上でローカル デバイスが送信したトラフィックはネイバーで受信されるけれども、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合に、単方向リンクが発生します。対になっているファイバ ケーブルのいずれかの接続が切断された場合、自動ネゴシエーションがアクティブである限り、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方のファイバが正常に動作していれば、レイヤ 2 の UDLD はそれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバー間で双方向に流れているかどうかを判別します。自動ネ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。

Cisco 7600 シリーズ ルータは、UDLD がイネーブルの LAN ポートのネイバー デバイスに、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。プロトコルが単方向リンクを正しく識別してディセーブルにするには、リンクの両端のデバイスで 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 51-1 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 51-1　　単方向リンク



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 デバイス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 ネイバー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 はネイバー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 秒間隔を使用する非アグレッシブな 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。

UDLD のデフォルト設定

表 51-1 に、UDLD のデフォルト設定を示します。

表 51-1　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 を設定する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」（P.51-3）
- 「個別の LAN インターフェイス上での UDLD のイネーブル化」（P.51-4）
- 「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」（P.51-4）
- 「UDLD プローブ メッセージ間隔の設定」（P.51-5）
- 「ディセーブルになった LAN インターフェイスのリセット」（P.51-5）

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 ポートでのみ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 メッセージ間隔の設定

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 52

NetFlow および NDE の設定

この章では、Cisco 7600 シリーズ ルータで NetFlow 統計情報収集および 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、次の URL にある『*Cisco IOS NetFlow Command Reference*』を参照してください。

  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_book.html
- NetFlow バージョン 9 がサポートされます。次の資料を参照してください。

  『*Cisco IOS NetFlow Configuration Guide*』
- NetFlow v9 エクスポート形式による NetFlow マルチキャストがサポートされます。次の資料を参照してください。

  『*Cisco IOS NetFlow Configuration Guide*』

  マルチキャスト高速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）は設定する必要はありません。マルチキャスト CEF スイッチングがサポートされます。

この章の内容は、次のとおりです。

- 「NetFlow および NDE の機能概要」（P.52-1）
- 「インターフェイス単位の NetFlow および NDE」（P.52-11）
- 「IPv6 用 NetFlow バージョン 9」（P.52-14）
- 「VRF インターフェイス上の NDE」（P.52-14）
- 「NetFlow および NDE のデフォルト設定」（P.52-15）
- 「NetFlow および NDE 設定時の注意事項および制約事項」（P.52-15）
- 「NetFlow と NDE の設定」（P.52-17）

NetFlow および NDE の機能概要

ここでは、NetFlow および NDE の機能について説明します。

- 「NetFlow および NDE の概要」（P.52-2）
- 「MSFC 上の NetFlow および NDE」（P.52-2）

- 「PFC 上の NetFlow および NDE」（P.52-2）

NetFlow および NDE の概要

NetFlow は、ルータを通過するトラフィックに関する統計情報を収集します。NetFlow Data Export（NDE; NetFlow データ エクスポート）を使用すると、この統計情報を外部データ コレクタにエクスポートして分析できます。

NetFlow および NDE は、使用しているソフトウェア リリースによって、グローバルにイネーブル化されるか、個々の LAN インターフェイス上でイネーブル化されます。

- Cisco IOS Release 12.2SRA 以前のリリースでは、NetFlow はグローバルにイネーブル化されていました。つまり、ルータのすべてのインターフェイスに対して統計情報が収集されていました。
- Cisco IOS Release 12.2SRB では、レイヤ 3 インターフェイス上の IPv4 トラフィックに対して、個々のインターフェイス上で NetFlow をイネーブル化できます。IPv6 トラフィックに対する NetFlow は、引き続きグローバル モードで動作します。この機能の詳細については、「インターフェイス単位の NetFlow および NDE」（P.52-11）を参照してください。

（注）　Release 12.2SRB 以降、IPv4 トラフィックのグローバル モード NetFlow はデフォルトではありません。これまでと同様のグローバル モード機能を実現するには、IPv4 トラフィック フローの統計情報をキャプチャする各レイヤ 3 インターフェイス上で、手動で NetFlow をイネーブルにする必要があります。

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に対して統計情報を収集できます。ただし、PFC3A では、ルーテッド トラフィックだけの統計情報が収集されます。

2 つの外部データ コレクタ アドレスを設定できます。このように PFC3 による冗長データ ストリームを用意することで、完全な NetFlow データを受信する確率が高くなります。

収集される統計情報の量を減らすには、次の機能を使用します。

- NetFlow サンプリング：収集される統計情報の数を減らします。
- NetFlow アグリゲーション：収集された統計情報を結合します。

MSFC 上の NetFlow および NDE

MSFC の NetFlow キャッシュは、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 では、ソフトウェアでルーティングされるトラフィックに対し、NetFlow アグリゲーションをサポートします。詳細については、『Cisco IOS NetFlow Configuration Guide』を参照してください。

MSFC では、ToS ベースのルータ アグリゲーションをサポートします。詳細については、『Cisco IOS NetFlow Configuration Guide』を参照してください。

PFC 上の NetFlow および NDE

PFC の NetFlow キャッシュは、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、ハードウェアでルーティングされるトラフィックに対し、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 および NDE を詳細に説明します。

- 「フロー マスク」（P.52-3）
- 「NDE のバージョン」（P.52-4）
- 「MLS キャッシュ エントリ」（P.52-7）
- 「NetFlow サンプリング」（P.52-8）
- 「NetFlow アグリゲーション」（P.52-10）

フロー マスク

ここでは、NetFlow エントリを作成するために使用されるフロー マスクについて説明します。Release 12.2SRA 用と Release 12.2SRB 用の 2 種類のフロー マスクが用意されています。NetFlow では、選択したフロー マスクが、ルータ上で収集されるすべての統計情報に適用されます。

Release 12.2SRA

Cisco IOS Release 12.2SRA では、NetFlow エントリを作成するために次のフロー マスクが使用されます。

- 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 アドレスからのすべてのフローは、このエントリを使用します。
- 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 アドレスへ向かうすべてのフローは、このエントリを使用します。
- 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。同じ送信元と宛先 IP アドレス間のすべてのフローは、このエントリを使用します。
- destination-source-interface：より固有性の高いフロー マスク。送信元 VLAN SNMP 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 フローごとにキャッシュ 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 インターフェイスが格納されます。
- full-interface：最も固有性の高いフロー マスクです。送信元 VLAN SNMP ifIndex を full フロー マスク中の情報に追加します。

Release 12.2SRB

Cisco IOS Release 12.2SRB では、次のフロー マスクが使用されます。

- destination-source-interface：より固有性の高いフロー マスク。送信元 VLAN SNMP ifIndex を destination-source フロー マスク中の情報に追加します。
- full-interface：最も固有性の高いフロー マスクです。送信元 VLAN SNMP ifIndex を full フロー マスク中の情報に追加します。

IPv4 トラフィックのインターフェイス単位モードに対応するため、その他のフロー マスクは次のように処理されます。

- source-only、destination、destination-source の各フロー マスクは、destination-source-interface として処理されます。
- full フロー マスクは、full-interface として処理されます。

NDE のバージョン

PFC 上の NDE は、PFC でキャプチャされた統計情報用に NDE バージョン 5、7、および 9 をサポートします。NetFlow バージョン 9 の詳細については、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/ios123/123newft/123_1/nfv9expf.htm

次に、サポートされている NDE フィールドを説明します。

- 表 52-1：バージョン 5 ヘッダー形式
- 表 52-2：バージョン 7 ヘッダー形式
- 表 52-3：バージョン 5 フロー レコード形式
- 表 52-4：バージョン 7 フロー レコード形式

表 52-1　NDE バージョン 5 ヘッダー形式

バイト	コンテンツ	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 52-2　NDE バージョン 7 ヘッダー形式

バイト	コンテンツ	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

（注）　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。

表 52-3　NDE バージョン 5 フロー レコード形式

バイト	コンテンツ	説明	フロー マスク • X = 読み込まれる • A = 追加のフィールド					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
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	—	—	—	—	—	—	—	—
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 プレフィックス マスク ビット	X	0	X	X	X	X
46 ～ 47	dst_mask	宛先アドレス プレフィックス マスク ビット	0	X	X	X	X	X
48	pad2	パッド 2	0	0	0	0	0	0

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. PFC3CXL、PFC3C、PFC3BXL、または PFC3B モードでは、ICMP トラフィックの場合、ICMP コードおよびタイプ値が格納されます。
5. ハードウェア スイッチド フローでは常に 0 です。

表 52-4　NDE バージョン 7 フロー レコード形式

バイト	コンテンツ	説明	フロー マスク • X = 読み込まれる • A = 追加のフィールド					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
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	—	—	—	—	—	—	—	—
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

表 52-4　NDE バージョン 7 フロー レコード形式 （続き）

バイト	コンテンツ	説明	フロー マスク • X = 読み込まれる • A = 追加のフィールド					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
44	src_mask	送信元アドレス プレフィックス マスク ビット	X	0	X	X	X	X
45	dst_mask	宛先アドレス プレフィックス マスク ビット	0	X	X	X	X	X
46 ～ 47	pad2	パッド 2	0	0	0	0	0	0
48 ～ 51	MLS 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. PFC3CXL、PFC3C、PFC3BXL、または PFC3B モードでは、ICMP トラフィックの場合、ICMP コードおよびタイプ値が格納されます。
5. ハードウェア スイッチド フローでは常に 0 です。

MLS キャッシュ エントリ

NetFlow は、PFC の NetFlow キャッシュからトラフィック統計情報をキャプチャします。

NetFlow は、NetFlow キャッシュ内のアクティブ 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。

エクスポートされる 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 キャッシュ中のフロー エントリの統計情報が含まれます。NetFlow キャッシュ中のフロー 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 キャッシュから消去されます。

- エントリの期限切れ。
- ユーザによるエントリの消去。
- インターフェイスの停止。
- ルート フラップの発生。

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 1920 秒（32 分））。

NDE パケットは、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、または所定時間の経過後に外部データ 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だけをエクスポートします。NDE フロー フィルタは NVRAM 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.52-28）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 7600 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 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 7600 シリーズ ルータ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.52-8）
- 「NetFlow フロー サンプリング」（P.52-9）

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 7600 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 によるパケットのサンプリング数を抑制すると、外部コレクタにエクスポートする必要のあるパケットの数も削減されます。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 7600 シリーズ ルータでは、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だけ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 7600 シリーズ ルータ上で使用できます。

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 52-5 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 52-5　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

NetFlow アグリゲーション

PFC および DFC 上での NetFlow アグリゲーション サポートの詳細については、次の URL にあるマニュアルの「NetFlow Aggregation」の項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

（注）

- Release 12.2SRB では、ハードウェア フロー キャッシュにデータが読み込まれるように、個々の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。これにより、NetFlow がイネーブルになっているインターフェイスからのみ、キャッシュにフローが読み込まれます。

- Release 12.2SRA では、アグリゲーション スキームを設定することによってハードウェア フロー キャッシュにデータを読み込むことができます。このキャッシュには、すべてのレイヤ 3 インターフェイスに対する情報がグローバルに読み込まれます。
- MSFC の NetFlow アグリゲーションを設定すると、PFC および DFC の NetFlow アグリゲーションも設定されます（設定方法のリンクについては、「MSFC 上のフローに対する NetFlow アグリゲーションの設定」（P.52-24）を参照してください）。
- NetFlow アグリゲーションは、NDE バージョン 8 を使用します。

インターフェイス単位の NetFlow および NDE

Cisco IOS Release 12.2SRB 以降のリリースでは、インターフェイス単位の NetFlow および NDE 機能により、個々のインターフェイス上で NetFlow をイネーブル化して、それらのインターフェイス上で IPv4 トラフィック フローの統計情報の収集とエクスポートを実行できます。以前は、NetFlow をイネーブルにすると、ルータのすべてのインターフェイスに対して統計情報が収集されていました（グローバル モード）。

以前のリリース（グローバル モード）から Release 12.2SRB（インターフェイス単位モード）にアップグレードする場合、NetFlow をアクティブにするには、個々のインターフェイス上で **ip flow ingress** コマンドを実行する必要があります。アップグレード プロセスでは、既存のグローバル モード フローマスクが対応するインターフェイス単位の種類に自動的に変換されます（source、destination、および destination-source は destination-source-interface になり、full は full-interface になります）。

Release 12.2SRB から以前のリリースにダウングレードすると、（すべてのルータ インターフェイスに対して統計情報を収集する）グローバル モード動作が再開されますが、12.2SRB フローマスクは有効になったままです。

インターフェイス単位 NetFlow 機能により、NetFlow テーブルの使用率とパフォーマンスが次のように向上します。

- 重要なフローに対して、NetFlow テーブルのより多くの領域を提供できる。インターフェイス単位 NetFlow を使用すると、NetFlow がイネーブルになっているインターフェイスに対してだけ、テーブル エントリが作成されます。これにより、テーブル内の不要なエントリの数が減少し、重要なフローに対して、より多くの領域を提供できるようになります。以前は、ルータのすべてのインターフェイスに対してテーブルが作成されていました。

  NetFlow がイネーブルになっているインターフェイスに対してのみ、テーブル エントリを作成すると、次の理由によってパフォーマンスが向上します。

  - フローベースのすべての機能（NetFlow、QoS、マルチキャストなど）で NetFlow テーブルが共有される。
  - NetFlow テーブルがいっぱいになると、NetFlow ショートカットがインストールされず、フロー統計情報（およびアカウンティング情報）が失われる可能性がある。
- NDE レコードを Netflow Data Collector（NFC）に高速にエクスポートすることによって NFC に負荷がかかり、重要なアカウンティング データが失われないようにする。統計情報の収集とエクスポートは、特定のインターフェイスに対してだけ行われるため、NFC に送信される NDE レコードの数を管理しやすくなります。
- NDE とその他の機能の間で発生する意図しない競合が減少する。

ここでは、インターフェイス単位の NetFlow と NDE、および Release 12.2SRB で導入された NetFlow と NDE に関連するその他の機能について説明します。

- 「インターフェイス単位の NetFlow と NDE の使用上の注意事項および制限事項」（P.52-12）

- 「インターフェイス単位の NetFlow および NDE の設定」（P.52-13）
- 「インターフェイス単位の NetFlow および NDE の確認」（P.52-13）
- 「IPv6 用 NetFlow バージョン 9」（P.52-14）
- 「VRF インターフェイス上の NDE」（P.52-14）

インターフェイス単位の NetFlow と NDE の使用上の注意事項および制限事項

Cisco 7600 ルータでインターフェイス単位の NetFlow および NDE を設定する際には、次の使用上の注意事項および制限事項に従ってください。

- Cisco IOS Release 12.2SRB 以降のリリースでサポートされる。
- RSP720、Sup720、および Sup32 でサポートされる。
- レイヤ 3 インターフェイス上の IPv4 ユニキャストおよびマルチキャスト トラフィックに対してサポートされる。
  IPv6 フローに対しては、NetFlow および NDE は、インターフェイス単位モードではなく、グローバル モードで動作する。
- （ブリッジされた）レイヤ 2 フローに対して NetFlow および NDE をイネーブルにすると、インターフェイス上の（ルーティングされた）レイヤ 3 フローに対しても自動的に機能がイネーブルになる。インターフェイスに対して NetFlow および NDE をディセーブルにする場合は、レイヤ 2 フローおよびレイヤ 3 フローの機能もディセーブルにする必要がある。L2 フローをディセーブルにするには、**no ip flow ingress layer2-switched** を使用する。L3 フローをディセーブルにするには、**no ip flow ingress** を使用する。
- インターフェイスでインターフェイス単位の NetFlow および QoS マイクロポリシングを設定できる。ただし、インターフェイス上で異なるフロー マスクのタイプを設定しないようにすること。1 つのフロー マスクのタイプだけを、インターフェイス単位の NetFlow およびマイクロフロー ポリシーに設定する必要がある。
- Release 12.2SRB 以降のルータでは NDE フロー マスクと QoS フロー マスクがサポートされるが、同じインターフェイス上で両方のフロー マスクを設定することはできない。
- NDE とマルチキャスト非 RPF の両方をイネーブルにすると、NDE で統計情報が失われる可能性がある。この潜在的な損失の可能性は、マルチキャスト フローに対して NetFlow と NDE がグローバルにイネーブル化されるために発生する。これは、NetFlow テーブルがオーバーフローする可能性があることを意味する。
- インターフェイスで **platform ip features sequential** コマンドを使用する場合、インターフェイス フル フローマスク機能を設定する必要があります。この機能によって、NDE が正しい統計情報をエクスポートできるようになり、ダブル アカウンティングを回避します。
- 次の制限事項は、インターフェイス単位モードのフロー マスクに適用される。
  - 個々のインターフェイスに異なる種類のフロー マスクを設定できない。インターフェイス単位の NetFlow または NDE に設定されたすべてのインターフェイスに対して、1 種類のフロー マスクだけがサポートされる。
  - NDE の場合は、ルーティングされた（L3）NetFlow エントリとブリッジされた（L2）NetFlow エントリの両方に同じフロー マスクが使用される。
  - 送信元フロー マスクと宛先フロー マスクはすべて destination-source-interface として処理され、フル マスクはどちらも full-interface として処理される。フロー マスクの種類については、「フロー マスク」（P.52-3）を参照。

- 「NetFlow および NDE 設定時の注意事項および制約事項」（P.52-15）に記載されているすべての注意事項および制限事項が適用される。

インターフェイス単位の NetFlow および NDE の設定

次に、Cisco 7600 ルータでインターフェイス単位の NetFlow および NDE を設定するために従う必要があるステップをまとめます。ステップごとの詳細な手順については、この章の後の項を参照してください。

1. NetFlow 統計情報をエクスポートする場合は、次のコマンドを実行することにより、ルータで NDE をグローバルにイネーブル化します。

```
configure terminal
ip flow-export destination
ip flow-export version
mls nde sender version
```

2. 次のコマンドを実行して、個々のインターフェイス上で NetFlow をイネーブル化します。

```
configure terminal
interface
  ip flow ingress
```

3. （任意）NetFlow サンプリングを設定するには、次の手順に従います。
   a. サンプリングされた NetFlow をルータ上でグローバルにイネーブルにします（「NetFlow フロー サンプリングの設定」（P.52-19）を参照）。
   b. 個々のインターフェイスで、サンプリングされた NetFlow をイネーブルにする（**mls netflow sampling**）。
   c. インターフェイスにコンフィギュレーションを適用します（**ip flow ingress**）。
4. NDE の設定が他の機能（QoS やマルチキャストなど）と競合していないことを確認します。設定を確認するには、**show ip interface** コマンドを使用します（「インターフェイス単位の NetFlow および NDE の確認」（P.52-13）を参照）。

インターフェイス単位の NetFlow および NDE の確認

インスタンス単位の NetFlow および NDE が適切に設定されていることを確認するには、**show ip interface** コマンドを次のように使用します。次のコマンド出力では、NetFlow および NDE の設定情報を示すフィールドは太字で示されています。

```
Router# show ip interface gig2/9
GigabitEthernet2/9 is up, line protocol is up
  Internet address is 10.0.0.1/8
  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: 224.0.0.5 224.0.0.2 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  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 Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
  Topology "base", operation state is UP
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
BGP Policy Mapping is disabled
Input features: Ingress-NetFlow
Output features: Post-Ingress-NetFlow, HW Shortcut Installation
Post encapsulation features: HW Shortcut Installation
Sampled Netflow is disabled
IP Routed Flow creation is enabled in netflow table
IP Bridged Flow creation is disabled in netflow table
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
IP multicast multilayer switching is disabled
```

IPv6 用 NetFlow バージョン 9

Cisco IOS Release 12.2SRB では、IPv6 用に NetFlow バージョン 9 のサポートが導入されています。この機能を Cisco 7600 ルータで設定する方法の詳細については、次の URL にある Release 12.2SRB の新しい機能に関するマニュアル（機能ガイド）でフィーチャ モジュールの説明を参照してください。

http://www.cisco.com/en/US/products/ps6922/products_feature_guides_list.html

VRF インターフェイス上の NDE

Cisco IOS Release 12.2SRB には、VRF インターフェイス上の NDE のサポートが導入されています。この新機能により、Cisco 7600 ルータは MPLS バーチャル プライベート ネットワーク（VPN）上で IPv4 パケットの NetFlow 統計情報をキャプチャしてエクスポートできます。この場合、ルータは、MPLS ネットワークのエッジでプロバイダー エッジ（PE）ルータとして動作します。

VRF インターフェイス上の NDE の詳細については、次の URL にある Release 12.2SRB の新しい機能に関するマニュアル（機能ガイド）でフィーチャ モジュールの説明を参照してください。

http://www.cisco.com/en/US/products/ps6922/products_feature_guides_list.html

NetFlow および NDE のデフォルト設定

表 52-6 に、NetFlow および NDE のデフォルト設定を示します。

表 52-6　NetFlow および NDE のデフォルト設定

機能	デフォルト値
NetFlow	ディセーブル 12.2SRB：IPv4 ユニキャストの場合はインターフェイス単位モード（その他はすべてグローバル モード） 12.2SRA：グローバル モード
NDE	ディセーブル
VRF インターフェイス上の NDE	12.2SRB：ディセーブル 12.2SRA：使用不可
入力ブリッジド IP トラフィックの NetFlow および 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。
NetFlow マスク	なし。
NetFlow サンプリング	ディセーブル
NetFlow アグリゲーション	ディセーブル
追加の NDE フィールドの読み込み	イネーブル。

NetFlow および NDE 設定時の注意事項および制約事項

NetFlow および NDE を設定する際には、次の注意事項および制約事項に従ってください。

NetFlow および NDE は、NetFlow バージョン 9 でのみ IP マルチキャスト トラフィックをサポートします。それ以外の NetFlow バージョンでは、**show mls ip multicast** コマンドを使用することで、IP マルチキャスト トラフィック用の NetFlow 統計情報を表示できます。

- Cisco 7600 ルータは、ユニキャスト IP パケットの出力方向の NetFlow をサポートしていません。
- すべての PFC（PFC3A を除く）では、ブリッジド IP トラフィックに対する NetFlow および NDE はサポートされません。
- NDE は、Internetwork Packet Exchange（IPX）トラフィックをサポートしません。
- Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）は、ハードウェアでのレイヤ 3 スイッチングに NetFlow テーブルを使用しません。
- NetFlow テーブルの使用率が、次の表に示す推奨レベルの使用率を超過すると、統計情報を保管するための十分な領域が不足する確率が高くなります。

PFC	推奨される NetFlow テーブルの使用率	NetFlow テーブルの合計容量
PFC3CXL PFC3BXL	235,520（230 K）エントリ	262,144 エントリ
PFC3C PFC3B	117,760（115 K）エントリ	131,072 エントリ
PFC3A	65,536（64 K）エントリ	131,072 エントリ

- 統計情報は、NetFlow テーブルが満杯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。
- Cisco 7600 シリーズ ルータ は、NetFlow テーブルを使用してフローベースの機能に関する情報を保持します。通常、Feature Manager は、フローが着信するラインカード上でのみ、フローベースの機能用に Netflow テーブル エントリを作成します。しかし、TCP インターセプトはグローバルな機能であるため、ルータは、入力 PFC および DFC だけでなく、取り付けられているすべての PFC および DFC で各 TCP インターセプト フローのエントリを作成します。これは、TCP インターセプト フローが着信する PFC または DFC ではゼロでないパケット カウントが表示され、その他の PFC および DFC ではパケットカウントがゼロになることを意味します（CSCek47971）。
- 次の IPv4 NetFlow オプションおよび NDE オプションは、IPv6 フローには使用できません（CSCek55571）。
  - アグリゲーションのサポート（**ip flow-aggregation cache** コマンド）
  - レイヤ 2 でスイッチングされた IPv6 フローのエクスポート
  - Netflow および NDE サンプリング
  - NDE フィルタのサポート

マルチキャスト NDE の設定時の注意事項

Cisco 7600 でマルチキャスト NDE を設定する際には、次の注意事項に従ってください。

- Release 12.2SRB 以降のリリースでは、マルチキャスト NDE と QoS マイクロフロー ポリシングの両方を同じインターフェイス上で設定できません。ただし、異なるインターフェイス上では、これらの機能を設定できます。
- マルチキャスト NDE を設定するには、**ip flow ingress** コマンドと **ip multicast netflow ingress** コマンドの両方を実行します。**ip multicast netflow ingress** コマンドは、デフォルトでイネーブルに設定されています。

Release 12.2SRB 以降のリリース

Release 12.2SRB 以降のルータは、IPv4 トラフィックに対して、インターフェイス単位モードの NetFlow および NDE だけをサポートしています。IPv6 フローに対しては、NetFlow および NDE は引き続きグローバル モードで動作します。

インターフェイス単位の NetFlow と NDE、およびその注意事項と制限事項の詳細については、「インターフェイス単位の NetFlow および NDE」（P.52-11）を参照してください。

NetFlow と NDE の設定

ここでは、NetFlow および NDE の設定手順について説明します。

- 「PFC 上のフローに対する NetFlow および NDE の設定」（P.52-17）
- 「MSFC 上のフローに対する NetFlow および NDE の設定」（P.52-23）
- 「入力ブリッジド IP トラフィックに対する NetFlow および NDE のイネーブル化」（P.52-26）
- 「NDE アドレスおよびポートの設定の表示」（P.52-27）
- 「NDE フロー フィルタの設定」（P.52-28）
- 「NDE の設定の表示」（P.52-30）

（注）
- PFC 上の NDE および MSFC 上の NDE をサポートするには、MSFC レイヤ 3 インターフェイスで 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 上の 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）。

（注）同じインターフェイス上で NDE と NAT を設定することはサポートされません。NDE では、統計情報をエクスポートするためにフローが定期的に期限切れになる必要があります。NAT は、期限切れにならないハードウェア ショートカットをインストールします。したがって、NAT されたフローの NDE は正しく動作しません。

PFC 上のフローに対する NetFlow および NDE の設定

ここでは、PFC 上のフローに対して NetFlow および NDE を設定する手順について説明します。

- 「PFC 上のフローに対する NetFlow の設定」（P.52-17）
- 「NDE のイネーブル化」（P.52-23）

PFC 上のフローに対する NetFlow の設定

ここでは、PFC 上のフローに対して NetFlow 統計情報収集を設定する手順について説明します。

- 「PFC での NetFlow のイネーブル化（Release 12.2SRA）」（P.52-18）
- 「インターフェイス単位の NetFlow のイネーブル化（Release 12.2SRB 以降）」（P.52-18）
- 「NetFlow フロー サンプリングの設定」（P.52-19）
- 「PFC 上のフローに対する NetFlow アグリゲーションの設定」（P.52-20）
- 「最小 IP MLS フロー マスクの設定（Release 12.2SRA のみ）」（P.52-21）
- 「MLS エージング タイムの設定」（P.52-22）

PFC での NetFlow のイネーブル化（Release 12.2SRA）

Release 12.2SRA で PFC 上のフローに対して 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。
Release 12.2SRB 以降のリリースでの NetFlow のイネーブル化の詳細については、次の項を参照してください。

コマンド	目的
`Router(config)# mls netflow`	PFC の NetFlow をイネーブルにします。
`Router(config)# no mls netflow`	PFC の NetFlow をディセーブルにします。

次に、NetFlow 統計情報収集をイネーブルにする例を示します。

```
Router(config)# mls netflow
```

インターフェイス単位の NetFlow のイネーブル化（Release 12.2SRB 以降）

Release 12.2SRA 以降のリリースで PFC 上のフローに対して 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。NetFlow および NDE のインターフェイス単位モードでのルータの動作の詳細については、「インターフェイス単位の NetFlow および NDE」（P.52-11）を参照してください。コマンド構文の詳細については、この章の最初に記載されているコマンド リファレンスを参照してください。

コマンド	目的
`Router(config)# mls flow ip`	NetFlow エントリに使用するフロー マスクを設定します。
`Router(config)# interface` *interface*	NetFlow をイネーブルにするインターフェイスを選択します。
`Router(config-if)# [no] ip flow ingress`	レイヤ 3 インターフェイス上で NetFlow をイネーブルにします。機能をイネーブルにする各インターフェイス上でコマンドを実行します。 インターフェイス上で NetFlow および NDE をディセーブルにするには、コマンドの **no** 形式を使用します。
`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。
`Router(config)# mls nde sender` `Router(config)# ip flow-export destination` {*hostname* | *ip-address*} *udp-port*	（任意）NDE をイネーブルにします。NetFlow 統計情報をエクスポートする場合は、これらのコマンドを実行します。 NetFlow 統計情報の送信先の外部ホスト（名前または IP アドレス）およびポートを指定します。
`Router(config)# mls nde sender`	（任意）NDE をイネーブルにします。NetFlow 統計情報をエクスポートする場合は、このコマンドを使用します。
`Router(config)# ip flow-export destination` {*hostname* | *ip-address*} *udp-port*	（任意）NetFlow 統計情報のエクスポート先の外部ホストのホスト名または IP アドレスと、統計情報の送信先のポートを指定します。
`Router(config)# show ip interface` *interface*	指定したインターフェイスの設定を表示します。設定を調べ、NDE の設定が他の機能（QoS やマルチキャストなど）と競合していないことを確認します（「インターフェイス単位の NetFlow および NDE の確認」を参照）。

NetFlow フロー サンプリングの設定

ここでは、PFC でサンプリングされた NetFlow を設定する手順について説明します。

- 「NetFlow フロー サンプリングのグローバルな設定（Release 12.2SRB および Release 12.2SRA）」（P.52-19）
- 「インターフェイス単位モードの NetFlow フロー サンプリングの設定（Release 12.2SRB）」（P.52-19）
- 「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（Release 12.2SRA）」（P.52-20）

（注）　MSFC 上の NDE は、NetFlow フロー サンプリングをサポートしません。

NetFlow フロー サンプリングのグローバルな設定（Release 12.2SRB および Release 12.2SRA）

Release 12.2SRB および Release 12.2SRA で、サンプリングされた NetFlow フロー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。

グローバルにサンプリングされた NetFlow を設定する場合、次の点に注意してください。

- *rate* 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 *interval* の有効値は 8,000 ～ 16,000 です。
- Release 12.2SRA の任意のデータをエクスポートするには、レイヤ 3 インターフェイス上でサンプリングされた NetFlow を設定する必要もあります。

詳細については、「NetFlow サンプリング」（P.52-8）を参照してください。

インターフェイス単位モードの NetFlow フロー サンプリングの設定（Release 12.2SRB）

Release 12.2SRB 以降のリリースでは、次の例のように、サンプリングされた NetFlow をグローバルにイネーブルにするか、個々のインターフェイス上でイネーブルにする必要があります。

この例では、**mls sampling** は、サンプリングされた NetFlow をグローバルにイネーブルにします。また、**mls netflow sampling** は、サンプリングされた NetFlow をインターフェイス（この例では、ファスト イーサネット ポート 5/12）上でイネーブルにします。

```
Router# configure terminal
Router(config)# mls sampling packet-based 64
Router(config)# interface fastethernet 5/12
Router(config-if)# mls netflow sampling
Router(config)# end
Router#
```

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（Release 12.2SRA）

Release 12.2SRA では、full-interface フロー マスクまたは destination-source-interface フロー マスクを使用して、個々のレイヤ 3 インターフェイスでサンプリングされた NetFlow を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、サンプリングされた NetFlow 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。

Release 12.2SRA で、レイヤ 3 インターフェイス上でサンプリングされた NetFlow を設定するには、サンプリングされた NetFlow がグローバルにイネーブルになっていることを確認してから、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指定します。 （注）　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。
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サンプリングされた NetFlow 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サンプリングされた NetFlow 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 でサンプリングされた NetFlow 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#
```

PFC 上のフローに対する NetFlow アグリゲーションの設定

MSFC に対して NetFlow アグリゲーションを設定すると、PFC および DFC 上のフローに対して NetFlow アグリゲーションが自動的に設定されます（「MSFC 上のフローに対する NetFlow アグリゲーションの設定」（P.52-24）を参照）。

PFC または DFC の NetFlow アグリゲーション キャッシュ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。このコマンドは、Release 12.2SRA でのみ使用できます。Release 12.2SRB では使用できません。

（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（Release 12.2SRA のみ）。

```
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#
```

最小 IP MLS フロー マスクの設定（Release 12.2SRA のみ）

PFC の NetFlow キャッシュに対するフロー マスクの最小特性を設定できます（「フロー マスク」（P.52-3）を参照）。使用する実際のフロー マスクには、**mls flow ip** コマンドで設定された最小の特性が備わっています。

（注）　この作業は、interface-destination-source フロー マスクと interface-full flow フロー マスクだけがサポートされる Release 12.2SRB には適用できません。

最小 IP 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 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 フロー マスクに戻します（ヌル）。

次に、最小 IP フロー マスクを設定する例を示します。

```
Router(config)# mls flow ip destination
```

IP 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 キャッシュ エントリに適用されます。normal エージング タイムは、32 ～ 4092 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使用率（「NetFlow および NDE 設定時の注意事項および制約事項」（P.52-15）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 キャッシュ サイズが推奨使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**：期限切れとなり、fast エージングまたは long エージングの対象外のエントリが削除されるまでの待機時間を設定します。
- **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**：常時使用されているエントリを削除するためのエージング タイムを設定します。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キャッシュ エントリは、ドメイン ネーム サーバ（DNS）または TFTP サーバとやりとりするフローに対するエントリです。このエントリは作成後に再び使用されることはありません。PFC は、これらのエントリを検出し期限切れにする場合、他のデータ用に NetFlow キャッシュのスペースを節約します。

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 キャッシュ サイズが増え続け、推奨使用率を超えた場合は、キャッシュ サイズが推奨使用率未満になるまで設定値を下げます。キャッシュが増え続け、推奨使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 キャッシュ 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
```

NDE のイネーブル化

Release 12.2SRA および Release 12.2 SRB では、次の操作を実行して NDE をグローバルにイネーブル化できます。

コマンド	目的
`Router(config)# mls nde sender [version {5 | 7}]`	PFC 上のフローに対して NDE をイネーブルにし、（任意で）NDE バージョンを設定します。データのエクスポート先の NetFlow コレクタと一致する NDE バージョンを指定します。
`Router(config)# ip flow-export destination {hostname | ip-address} udp-port`	識別します。
`Router(config)# no mls nde sender`	PFC 上のフローに対して NDE をディセーブルにします。
`Router(config)# no mls nde sender version`	デフォルト値に戻します（バージョン 7）。

（注）
- PFC 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.52-25）を参照）。
- NetFlow バージョン 9 がサポートされます。次の資料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 上のフローに対して NDE をグローバルにイネーブルにする例を示します。

```
Router(config)# mls nde sender
```

次に、PFC に対して NDE をグローバルにイネーブルにし、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
```

MSFC 上のフローに対する NetFlow および NDE の設定

ここでは、次の URL に記載されている NetFlow 手順について補足します。

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

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 上のフローに対する NetFlow のイネーブル化」（P.52-24）
- 「MSFC 上のフローに対する NetFlow アグリゲーションの設定」（P.52-24）
- 「MSFC NDE 送信元レイヤ 3 インターフェイスの設定」（P.52-25）
- 「NDE の宛先の設定」（P.52-25）

MSFC 上のフローに対する NetFlow のイネーブル化

Release 12.2SRB 以降のリリースでは、インターフェイス上で NetFlow をイネーブルにすると（**ip flow ingress**）、そのインターフェイス上で NDE が自動的にイネーブルになります。ただし、NDE が動作するためには、NDE をグローバルにイネーブルにして、統計情報のエクスポート先を指定する必要があります（**mls nde sender** および **ip flow-export destination**）。

Release 12.2SRA では、NDE をイネーブルにする各レイヤ 3 インターフェイスに対して次の作業を行うことにより、MSFC 上の NetFlow をイネーブルにします。

	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` `Router(config-if)# ip route-cache flow`	NetFlow をイネーブルにします。

MSFC 上のフローに対する NetFlow アグリゲーションの設定

MSFC 上のフローに対して NetFlow アグリゲーションを設定するには、次の URL の項「Configuring an Aggregation Cache」の手順を実行します。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt2/xcfnfc.htm#wp1001058

（注）
- MSFC の NetFlow アグリゲーションを設定すると、PFC および DFC の NetFlow アグリゲーションが自動的に設定されます
- Release 12.2SRB では、ハードウェア フロー キャッシュにデータが読み込まれるように、個々の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。これにより、NetFlow がイネーブルになっているインターフェイスからのみ、キャッシュにフローが読み込まれます。
- Release 12.2SRA では、アグリゲーション スキームを設定することによってハードウェア フロー キャッシュにデータを読み込むことができます。このキャッシュには、すべての L3 インターフェイスに対する情報がグローバルに読み込まれます。

MSFC に対して NetFlow ToS ベースのルータ アグリゲーションを設定するには、次の URL の手順を実行します。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm

（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。

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 統計情報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 回入力し、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 の複数のエクスポート先機能は、次のハードウェアでサポートされます。

- PFC3

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 に保存され、NDE をディセーブルにして再びイネーブルにした場合、またはルータの電源をオフ / オンした場合にも、削除されずに残ります。データ収集に NetFlow FlowCollector アプリケーションを使用する場合は、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。

入力ブリッジド IP トラフィックに対する NetFlow および NDE のイネーブル化

すべての PFC（PFC3A を除く）では、入力ブリッジド IP トラフィックに対する NetFlow および NDE はサポートされません。ここでは、入力ブリッジド IP トラフィックに対して NetFlow および NDE をイネーブルにする手順について説明します。

- 「VLAN 上の入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化」（P.52-26）
- 「VLAN 上の入力ブリッジド IP トラフィックに対する NDE のイネーブル化」（P.52-27）

（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.52-8）を参照）。
- ブリッジド IP トラフィックに対して NetFlow および NDE をイネーブルにする各 VLAN に対して、対応する VLAN インターフェイスを作成し、IP アドレスを割り当て、**no shutdown** コマンドを実行してそのインターフェイスを起動する必要があります。
- NDE がグローバルにイネーブルになっている限り、VLAN 上でブリッジド IP トラフィックに対して NetFlow をイネーブルにすると、ブリッジド トラフィックのエクスポートがデフォルトでイネーブルに設定されます。

VLAN 上の入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化

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
```

VLAN 上の入力ブリッジド IP トラフィックに対する NDE のイネーブル化

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化されます）。 **（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」（P.52-28）
- 「ポート フロー フィルタの設定」（P.52-29）
- 「ホストおよびポート フロー フィルタの設定」（P.52-29）
- 「ホスト フロー フィルタの設定」（P.52-29）
- 「プロトコル フロー フィルタの設定」（P.52-30）

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削除されません。

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.52-30）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 へのフローだけが含まれて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 172.20.52.37 255.255.255.255
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.52-30）を参照）。

プロトコル フロー フィルタを設定するための使用上のガイドライン

NetFlow データ エクスポート フィルタを設定する場合は、次の制約事項と使用上のガイドラインに従ってください。

- フロー エクスポートを追加または除外するためのフィルタは 1 つしかサポートされません。フロー エクスポート設定は、送信元 IP、宛先 IP、送信元ポート、宛先ポート、およびプロトコルに基づきます。
- 次の例で示すように、フィルタ パラメータを個別に設定すると、最後のフィルタが、設定されたすべてのフィルタ値で構成されます。

```
Router(config)#mls nde flow include src-port 100
Router#sh run | I mls nde flow
mls nde flow include protocol tcp src-port 100
Router(config)#mls nde flow include dest-port 200
Router#sh run | I mls nde flow
mls nde flow include protocol tcp src-port 100 dest-port 200
Router#
```

- 次の例に示すように、フィルタを新しい値で設定し直すと、古い値が上書きされます。

```
Router(config)#mls nde flow include dest-port 200
Router#sh run | I mls nde flow
mls nde flow include dest-port 200
Router(config)#mls nde flow include dest-port 500
Router#sh run | I mls nde flow
mls nde flow include dest-port 500
```

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 53

ローカル SPAN、RSPAN、および ERSPAN の設定

この章では、Cisco 7600 シリーズ ルータ上でローカル スイッチド ポート アナライザ（SPAN）、リモート SPAN（RSPAN）、およびカプセル化 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）は、ERSPAN をサポートしています（「ERSPAN に関する注意事項および制約事項」（P.53-11）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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- Shared Port Adapter（SPA; 共有ポート アダプタ）ポートおよび FlexWAN ポートは、SPAN、RSPAN、または ERSPAN をサポートしていません。

この章の内容は、次のとおりです。

- 「ローカル SPAN、RSPAN、および ERSPAN の機能概要」（P.53-1）
- 「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」（P.53-6）
- 「ローカル SPAN、RSPAN、および ERSPAN の設定」（P.53-12）

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」（P.53-2）
- 「ローカル SPAN、RSPAN、および ERSPAN の送信元」（P.53-5）
- 「ローカル SPAN、RSPAN、および ERSPAN の宛先」（P.53-6）

ローカル SPAN、RSPAN、および ERSPAN の概要

SPAN は 1 つまたは複数のポート、1 つまたは複数の EtherChannel、または 1 つまたは複数の VLAN からトラフィックをコピーし、モニタしたトラフィックを、SwitchProbe デバイスまたは他の Remote Monitoring（RMON; リモート モニタリング）プローブなどの、1 つまたは複数の宛先に送信します。

SPAN は、送信元上のトラフィックのスイッチングには影響しません。その宛先は、SPAN 専用に設定する必要があります。SPAN が生成したトラフィックのコピーは、送信元ルータのユーザ トラフィックと競合します。

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」（P.53-2）
- 「RSPAN の概要」（P.53-3）
- 「ERSPAN の概要」（P.53-4）
- 「SPAN 送信元でモニタされるトラフィックについて」（P.53-4）

ローカル SPAN の概要

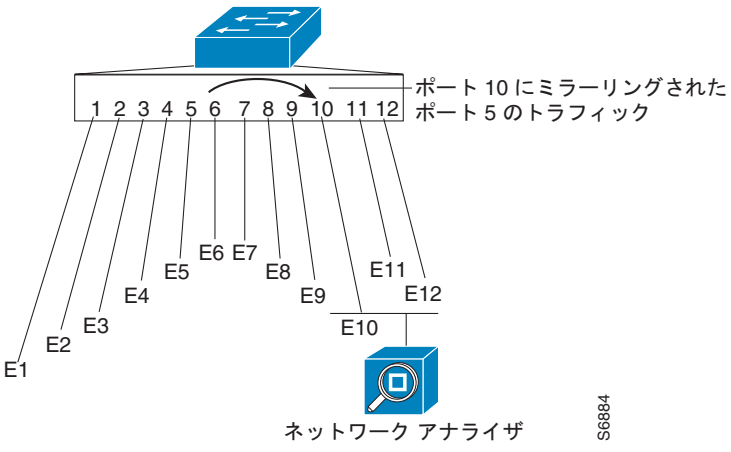
ローカル SPAN セッションは、送信元ポートおよび送信元 VLAN を、1 つまたは複数の宛先に対応付けたものです。ローカル SPAN セッションは、単一のルータ上に設定します。ローカル SPAN には、個別の送信元および宛先のセッションはありません。

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 ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。ローカル SPAN セッションは、送信元 RSPAN Generic Routing Encapsulation（GRE）でカプセル化されたトラフィックを送信元ポートからローカルにコピーしません。

ローカル SPAN セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

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へコピーします（図 53-1 を参照）。たとえば図 53-1 の場合、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できます。

図 53-1　　SPAN の設定例



RSPAN の概要

RSPAN は、異なるルータ上の送信元ポート、送信元 VLAN、および宛先をサポートします。ERSPAN は、ネットワーク上の複数のルータをリモート モニタします（図 53-2 を参照）。RSPAN は、レイヤ 2 VLAN を使用して、ルータ間の SPAN トラフィックを伝送します。

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。異なるルータ上で、RSPAN 送信元セッションと宛先セッションを個別に設定します。1 つのルータ上で RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは VLAN を 1 つの RSPAN VLAN に対応付けます。別のルータ上で RSPAN 宛先セッションを設定するには、宛先を RSPAN VLAN に対応付けます。

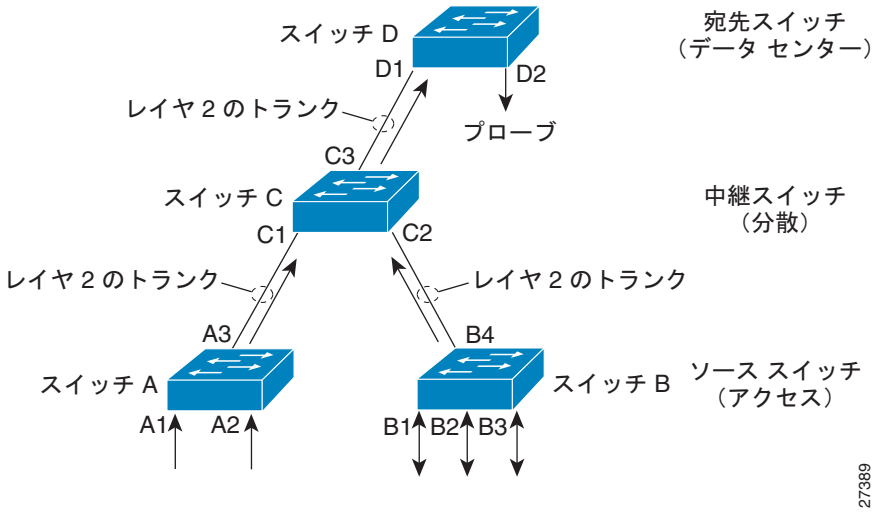
各 RSPAN セッションのトラフィックは、レイヤ 2 非ルーティング トラフィックとして、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのルータの RSPAN セッション専用です。参加しているすべてのルータは、レイヤ 2 によってトランク接続されている必要があります。

RSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。RSPAN 送信元セッションは、送信元 RSPAN GRE でカプセル化されたトラフィックを送信元ポートからローカルにコピーしません。

RSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

RSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からトラフィックをコピーし、RSPAN VLAN 上のトラフィックを RSPAN 宛先セッションへスイッチングします。RSPAN 宛先セッションはトラフィックを宛先ポートへスイッチングします。

図 53-2　　RSPAN の設定



ERSPAN の概要

ERSPAN は、異なるルータ上の送信元ポート、送信元 VLAN、および宛先をサポートします。ERSPAN は、ネットワーク上の複数のルータをリモート モニタします（図 53-3 を参照）。ERSPAN は、GRE トンネルを使用して、ルータ間の SPAN トラフィックを伝送します。

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。異なるルータ上で、ERSPAN 送信元セッションと宛先セッションを個別に設定します。

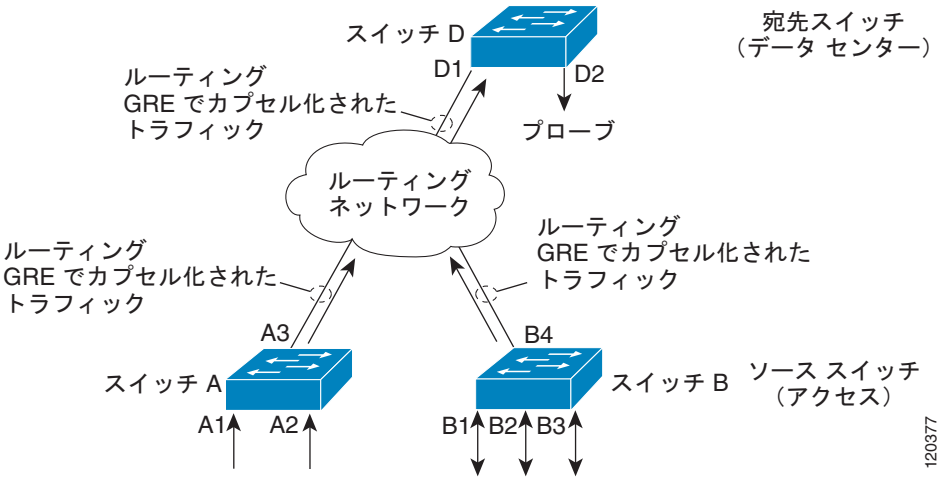
ERSPAN 送信元セッションを 1 つのルータ上で設定するには、送信元ポートまたは VLAN のセットを、宛先 IP アドレス、ERSPAN ID 番号、およびオプションとして VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）名に対応付けます。ERSPAN 宛先セッションを別のルータ上で設定するには、宛先ポートを、送信元 IP アドレス、ERSPAN ID 番号、およびオプションとして VRF 名に対応付けます。

ERSPAN 送信元セッションは、RSPAN VLAN を伝送する送信元トランク ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。ERSPAN 送信元セッションは、送信元 ERSPAN GRE でカプセル化されたトラフィックを送信元ポートからローカルにコピーしません。

ERSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

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、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 宛先セッションはトラフィックを宛先へスイッチングします。

図 53-3　　ERSPAN の設定



SPAN 送信元でモニタされるトラフィックについて

ここでは、ローカル SPAN、RSPAN、および ERSPAN の送信元がモニタできる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.53-5）
- 「モニタ対象トラフィックのタイプ」（P.53-5）
- 「重複トラフィック」（P.53-5）

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 送信元セッションが、入力トラフィック（入力 SPAN）のモニタ、出力トラフィック（出力 SPAN）のモニタ、または両方向でのトラフィック フローのモニタを行う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 は送信元ポートまたは VLAN で受信され、宛先ポートに送信されたトラフィックをコピーします。

モニタ対象トラフィックのタイプ

デフォルトでは、ローカル SPAN および ERSPAN がマルチキャスト フレームおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックをモニタリングします。RSPAN は BPDU モニタリング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、宛先に送信します。たとえば、双方向 SPAN（入力および出力の両方）セッションが、s1 および s2 の 2 つを SPAN 送信元、d1 を SPAN の宛先として設定している場合、パケットが s1 からルータに入って、出力パケットとしてスイッチから s2 に送信されると、s1 の入力 SPAN および s2 の出力 SPAN 両方が、パケットのコピーを SPAN の宛先 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 にスイッチングされたレイヤ 3 だった場合は、レイヤ 3 書き換えによって送信元および宛先レイヤ 2 アドレスが変更され、SPAN パケットは異なるものとなります。

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。

- 「送信元ポートと EtherChannel」（P.53-5）
- 「送信元 VLAN」（P.53-5）

送信元ポートと EtherChannel

送信元ポートまたは EtherChannel は、トラフィック分析のためにモニタされるポートまたは EtherChannel です。レイヤ 2 およびレイヤ 3 のポートの両方を、SPAN 送信元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または EtherChannel を、単一の SPAN セッションでモニタできます。任意の VLAN に、SPAN 送信元としてポートまたは EtherChannel を設定できます。トランク ポートまたは EtherChannel を、送信元として設定したり、非トランク送信元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）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および EtherChannel が、SPAN トラフィックの送信元になります。

（注）　送信元 VLAN にあるレイヤ 3 VLAN インターフェイスが、SPAN トラフィックの送信元ではありません。レイヤ 3 VLAN インターフェイスを介して VLAN に入るトラフィックは、送信元 VLAN にある EtherChannel の出力ポートを介してルータから送信される際に、モニタされます。

ローカル SPAN、RSPAN、および ERSPAN の宛先

SPAN の宛先は、レイヤ 2 またはレイヤ 3 の LAN ポートか、または、Release 12.2(33)SRC およびそれ以降では、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 またはレイヤ 3 LAN ポートです。ポートまたは EtherChannel を SPAN の宛先として設定すると、そのポートは SPAN 機能専用になります。

宛先 EtherChannel では、ポート集約プロトコル（PAgP）またはリンク集約制御プロトコル（LACP）EtherChannel プロトコルはサポートされません。すべての EtherChannel プロトコルでディセーブルがサポートされる場合に、オン モードがサポートされます。

宛先 EtherChannel のメンバー リンクが、EtherChannel がサポートされるデバイスに接続される際の、要件はありません。たとえば、メンバー リンクに接続し、ネットワーク アナライザと分離できます。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。

デフォルトでは、宛先で、任意のトラフィックを受信することはできません。Release 12.2(33)SRC およびそれ以降では、レイヤ 2 の宛先を設定し、接続されている任意のデバイスからトラフィックを受信できます。

デフォルトでは、宛先で、SPAN 以外のトラフィックは送信されません。トラフィックを受信するために設定したレイヤ 2 の宛先は、宛先に接続された任意のデバイスのレイヤ 2 アドレスを認識し、そのデバイスあてに送信されるトラフィックを送信するよう、設定できます。

トランク ポートを宛先として設定できます。これによって、トランクの宛先がカプセル化したトラフィックを送信することができます。許可される VLAN のリストを使用して、宛先トランク VLAN フィルタリングを設定できます。

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 の設定時の注意事項および制約事項について説明します。

- 「機能の非互換性」（P.53-6）
- 「ローカル SPAN、RSPAN、および ERSPAN セッションの制限」（P.53-7）
- 「ローカル SPAN、RSPAN、および ERSPAN の注意事項および制約事項」（P.53-8）
- 「VSPAN に関する注意事項および制約事項」（P.53-9）
- 「RSPAN に関する注意事項および制約事項」（P.53-10）
- 「ERSPAN に関する注意事項および制約事項」（P.53-11）

機能の非互換性

ローカル SPAN、RSPAN、および ERSPAN には、機能の互換性がありません。

- Unknown Unicast Flood Blocking（UUFB）ポートは、RSPAN またはローカル SPAN 出力だけの宛先にはできません (CSCsj27695)。
- EoMPLS ポートを SPAN 送信元として使用することはできません (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ー ポートを SPAN 送信元ポートとして設定することはできません。EtherChannel の非アクティブなメンバー 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状態になりトラフィックを伝送しません。
- EtherChannel のアクティブなメンバー ポートを SPAN の宛先ポートとして設定することはできません。EtherChannel の非アクティブなメンバー ポートは、SPAN の宛先ポートとして設定できますが、これらのポートは中断状態になりトラフィックを伝送しません。
- 次の機能は、SPAN の宛先ポートとは機能的に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
  - スパニングツリー プロトコル（STP）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 トランキング プロトコル（VTP）
  - ダイナミック トランキング プロトコル（DTP）
  - IEEE 802.1Q トンネリング

（注）　SPAN 宛先ポートは、IEEE 802.3Z フロー制御に参加できます。

ローカル SPAN、RSPAN、および ERSPAN セッションの制限

Release 12.2(33)SRC およびそれ以降では、PFC3 のローカル SPAN、RSPAN、および ERSPAN セッションの制限は、表 53-1 のとおりです。PFC3 のローカル SPAN、RSPAN、および ERSPAN 送信元および宛先の制限は、表 53-2 のとおりです。

表 53-1　PFC3 ローカル SPAN、RSPAN、および ERSPAN セッションの制限

	ローカル セッションと送信元セッション		宛先セッション	
総セッション数	ローカル SPAN、RSPAN 送信元、ERSPAN 送信元入力と出力のどちらか、または両方	ローカル SPAN の出力のみ	RSPAN 宛先セッション	ERSPAN 宛先セッション
80	2	14	64	23

表 53-2　PFC3 のローカル SPAN、RSPAN、および ERSPAN 送信元および宛先の制限

	ローカル SPAN セッションごと	RSPAN 送信元セッションごと	ERSPAN 送信元セッションごと	RSPAN 宛先セッションごと	ERSPAN 宛先セッションごと
出力または「両方」の送信元	128	128	128	—	—
入力送信元	128	128	128	—	—
RSPAN および ERSPAN 宛先セッションの送信元	—	—	—	1 RSPAN VLAN	1 つの IP アドレス
セッションごとの宛先	64	1 RSPAN VLAN	1 つの IP アドレス	64	64

ローカル SPAN、RSPAN、および ERSPAN の注意事項および制約事項

次の注意事項および制約事項は、ローカル SPAN、RSPAN、および ERSPAN に適用されます。

- 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 の宛先は、出力トラフィックだけをネットワーク アナライザに送信します。ただし、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 送信元ポートが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 の宛先に送信します。(CSCds22021)
- 再び **monitor session** コマンドを入力しても、前に設定した SPAN パラメータを消去しません。設定済みの SPAN パラメータをクリアするには、**no monitor session** コマンドを入力する必要があります。
- ネットワーク アナライザを SPAN の宛先に接続します。
- SPAN セッション内では、すべての SPAN の宛先は、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。ただし、送信元 VLAN フィルタリングが SPAN の送信元に設定されている場合を除きます。
- SPAN の宛先から送信されるトラフィックを選択するよう、宛先トランク VLAN フィルタリングを設定できます。
- レイヤ 2 LAN ポート（**switchport** コマンドで設定された LAN ポート）とレイヤ 3 LAN ポート（**switchport** コマンドを使用せずに設定された LAN 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。

- セッション内では、VLAN を SPAN 送信元として設定することと、送信元 VLAN フィルタリングを行うことの、両方を設定することはできません。VLAN を SPAN 送信元として設定するか、または、送信元ポートおよび EtherChannel からのトラフィックの送信元 VLAN フィルタリングを行うことはできますが、同じセッションで両方を行うことはできません。
- 内部 VLAN に対し、送信元 VLAN フィルタリングは設定できません。
- イネーブルなローカル SPAN、RSPAN、および ERSPAN は、すでに入力された設定があれば、その設定を使用します。
- 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、送信元トランク ポートの Inter-Switch Link Protocol（ISL; スイッチ間リンク プロトコル）タグまたは 802.1Q タグはコピーしません。宛先をトランクとして設定し、タグ付きトラフィックをトラフィック アナライザにローカルに送信できます。

（注）　トランクとして設定した宛先は、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 としてタグ付けします。

- 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 ポートから送信元 RSPAN VLAN トラフィックをローカルにコピーしません。
- 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。
- ポートまたは EtherChannel は、1 つの SPAN セッションでのみ SPAN の宛先にできます。SPAN セッションは、共有の宛先にはできません。
- SPAN の宛先は、SPAN の送信元にはできません。
- 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。したがってモニタリングの宛先で確認される BPDU は、送信元から送られたものです。RSPAN は BPDU モニタリング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ルータ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、出力ポート経由でルータから送出されないパケットが含まれます。これは、STP が出力ポートをブロッキング ステートに移行するためです。また、出力ポートでは、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ためです。

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。

- VSPAN セッションは、VLAN フィルタリングをサポートしません。

- 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）アナライザへ転送されます。
- VSPAN は、VLAN 内のレイヤ 2 ポートを出入りするトラフィックだけをモニタします。
  - VLAN を入力送信元として設定し、トラフィックがモニタ対象 VLAN にルーティングされる場合、ルーティングされたトラフィックは、VLAN 内のレイヤ 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対象 VLAN からルーティングされる場合、ルーティングされたトラフィックは、VLAN 内のレイヤ 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。

- 参加しているすべてのルータは、レイヤ 2 トランクによって接続されている必要があります。
- RSPAN VLAN をサポートするネットワーク デバイスは、RSPAN 中間デバイス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 デバイスでは、サポートできる RSPAN VLAN の数が制限される場合があります。
- すべての送信元、中間、宛先ネットワーク デバイスにおいて、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 の番号がついた 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 デバイスで、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だけ使用できます。
- 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 VLAN 内の RSPAN トラフィックの伝送用に選択されたトランク ポート以外のポートは設定しないでください。
- MAC アドレス ラーニングは、RSPAN VLAN 上でディセーブルです。
- RSPAN 送信元ルータの RSPAN VLAN 上にある出力アクセス コントロール リスト（ACL）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 モニタリング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。
- すべての関与しているネットワーク デバイスが RSPAN VLAN の設定をサポートし、すべての関与しているネットワーク デバイスで各 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、PFC3B、PFC3BXL、PFC3C、PFC3CXL でサポートされます。
- ERSPAN は、WS-SUP720（PFC3A 搭載の Supervisor Engine 720）のハードウェア バージョン 3.2 以降でサポートされます。ハードウェア バージョンを表示するには、**show module version | include WS-SUP720-BASE** コマンドを入力します。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
```

- 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 バイトの巡回冗長検査（CRC）トレーラーと置き換えます。
- 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 トラフィックが廃棄されます。

（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 サポートの設定」（P.8-9）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）。

- 参加しているすべてのルータはレイヤ 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。ERSPAN パケットの IP ヘッダー内には、do not fragment ビットが設定されます。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 Diffserv コード ポイント（DSCP）の値を設定することで、Quality of Service（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。
- ルータ上のすべての 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** コマンドで設定します（「ERSPAN 送信元セッションの設定」（P.53-26）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.53-28）を参照）。

- ERSPAN 送信元セッションの宛先 IP アドレス（宛先ルータ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。
- ERSPAN の出力は、EVC ポートではサポートされません。

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。

- 「無条件トランクとしての宛先ポートの設定（任意）」（P.53-12）
- 「宛先トランクの VLAN フィルタリングの設定（任意）」（P.53-13）
- 「宛先ポートの許可リストの設定（任意）」（P.53-15）
- 「ローカル SPAN の設定」（P.53-15）
- 「RSPAN の設定」（P.53-20）
- 「ERSPAN の設定」（P.53-26）
- 「ERSPAN の設定」（P.53-26）
- 「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.53-30）
- 「設定の確認」（P.53-31）
- 「設定例」（P.53-31）

無条件トランクとしての宛先ポートの設定（任意）

宛先を脱退するときにモニタ対象トラフィックにタグを付けるには、宛先として設定する前に、宛先をトランクとして設定します。

宛先をトランクとして設定するには、インターフェイス 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# configure terminal`	グローバル コ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 | port-channel number}`	設定するインターフェイスを選択します。 *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 3	`Router(config-if)# switchport`	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 ポートにレイヤ 2 スイッチングがまだ設定されていない場合だけ必須）。
ステップ 4	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	カプセル化を設定して、インターフェイスを ISL または 802.1Q トランクとして設定します。
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。

次に、無条件 IEEE 802.1Q トランクとしてポートを設定する例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
```

（注）　Release 12.2(33)SRC よりも前のリリースでは、宛先ポートを条件なしトランクとして設定する場合、**switchport nonegotiate** コマンドを入力する必要があります。Release 12.2(33)SRC およびそれ以降では、この要件は除外されました。

宛先トランクの VLAN フィルタリングの設定（任意）

（注）　トランク上での VLAN のフィルタリングに加え、許可される VLAN リストも適用してポートにアクセスできます。

宛先トランクの VLAN フィルタリングは、宛先に適用されます。宛先トランク VLAN フィルタリングを使用する場合、SPAN の送信元から SPAN の宛先に送信されるトラフィックの量は削減されません。

宛先がトランクの場合、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 VLAN フィルタリングを使用すると、SPAN セッション内で、すべての宛先がすべての送信元からのトラフィックを全部受信するという制限が解除されます。宛先トランク VLAN フィルタリングを使用すると、各宛先トランクからネットワーク アナライザに送信されるトラフィックを VLAN 単位で選択できます。

宛先トランク VLAN フィルタリングを宛先トランク上に設定するには、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 slot/port*	設定する宛先トランク ポートを選択します。 *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
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。

宛先トランク ポート上で許可される VLAN のリストを設定する場合、次の点に注意してください。

- *vlan* パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）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。
- 許可リストからすべての VLAN を削除するには、**switchport trunk allowed vlan none** コマンドを入力します。

- 許可リストに VLAN を追加するには、**switchport trunk allowed vlan add** コマンドを入力します。
- SPAN 設定を削除しないで、許可 VLAN リストを変更できます。

次に、各宛先トランク ポートが VLAN からトラフィックを送信するように宛先トランク ポート VLAN フィルタリングが SPAN トラフィックをフィルタリングする場合、送信元として複数の VLAN を、宛先として複数のトランク ポートを持ったローカル SPAN セッションの設定例を示します。

```
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
```

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リスト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)# monitor permit-list destination interface` *type slot/port*`[-`*port*`] [, `*type 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の許可リストに追加します。 *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**
ステップ 4	`Router(config)# do show monitor permit-list`	設定を確認します。

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 を含む宛先ポートの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

ここでは、ローカル SPAN セッションの設定手順について説明します。

- 「ローカル SPAN の設定（SPAN コンフィギュレーション モード）」（P.53-15）
- 「ローカル SPAN の設定（グローバル コンフィギュレーション モード）」（P.53-18）

ローカル SPAN の設定（SPAN コンフィギュレーション モード）

（注）　宛先を脱退するときにモニタ対象トラフィックにタグを付けるには、無条件で宛先をトランクに設定してから、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（任意）」（P.53-12）を参照）。

SPAN コンフィギュレーション モードでローカル 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 type [local | local-tx]`	ローカル SPAN セッション番号を設定し、ローカル SPAN 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。 • **local** キーワードを入力し、入力セッション、出力セッション、または両方の SPAN セッションを設定します。 • **local-tx** キーワードを入力し、出力だけの SPAN セッションを設定します。
ステップ 3	`Router(config-mon-local)# description session_description`	（任意）ローカル SPAN セッションの説明を入力します。
ステップ 4	`Router(config-mon-local)# 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 セッション番号を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。 **（注）** **monitor session** コマンドに **local-tx** キーワードを入力する場合、**rx** キーワードと **both** キーワードは使用できず、**tx** キーワードが必要です。 使用可能な SPAN セッションを最大限に活用するには、**tx** 付きで **local** セッションを使用する代わりに、常に **local-tx** セッションを使用することを推奨します。
ステップ 5	`Router(config-mon-local)# filter {single_vlan | vlan_list | vlan_range | mixed_vlan_list}`	（任意）ローカル SPAN 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 6	`Router(config-mon-local)# destination {single_interface | interface_list | interface_range | mixed_interface_list} [ingress [learning]]`	ローカル SPAN セッション番号を宛先と関連付けます。
ステップ 7	`Router(config-mon-local)# no shutdown`	（任意）ローカル SPAN セッションを開始します。 **（注）** **no shutdown** コマンドおよび **shutdown** コマンドは、local-tx 出力だけの SPAN セッションでは、サポートされません。
ステップ 8	`Router(config-mon-local)# 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場合、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が、特殊文字は使用できません。Release 12.2(33)SRC およびそれ以降では、スペースは使用できます。

（注） **description** コマンドのあとに、240 文字を入力できます。

- *local_span_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

  （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.10-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグ付きトラフィックをルータに返信する場合、ISL または 802.1Q のいずれかのトランキングを使用します。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをルータに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、ギガビット イーサネット ポート 1/1 からの入力トラフィックをモニタするようにセッション 1 を設定し、Gigabit Ethernet ポート 1/2 を宛先として設定する例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 type local
Router(config-mon-local)# source interface gigabitethernet 1/1 rx
Router(config-mon-local)# destination interface gigabitethernet 1/2
```

```
Router(config-mon-local)# no shutdown
Router(config-mon-local)# end
```

詳細については、「設定例」（P.53-31）を参照してください。

ローカル SPAN の設定（グローバル コンフィギュレーション モード）

（注）　宛先を脱退するときにモニタ対象トラフィックにタグを付けるには、無条件で宛先をトランクに設定してから、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（任意）」（P.53-12）を参照）。

グローバル コンフィギュレーション モードでは、最大 2 つまでのローカル SPAN セッションを設定できます。

すべての SPAN 設定作業に対して、SPAN コンフィギュレーション モードを使用できます。

サポートされる最大数の SPAN を設定するには、SPAN コンフィギュレーション モードを使用する必要があります。

ローカル SPAN は、個別の送信元および宛先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、ローカル SPAN 送信元および宛先に同じセッション番号を設定します。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を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。
ステップ 3	`Router(config)# monitor session` *local_span_session_number* **destination** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [**ingress** [**learning**]]	ローカル SPAN セッション番号と宛先を関連付けます。

ローカル SPAN セッションを設定する場合、次の点に注意してください。

- *local_span_session_number* の範囲は、1 ～ 66 です。
- *single_interface* は
  - **interface** *type slot*/*port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

（注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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。
- **ingress** キーワードを入力し、接続サービスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、ルータによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。

  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.8-6）の項を参照してください。
  - 宛先がトランクで、接続デバイスがタグ付きトラフィックをルータに返信する場合、ISL または 802.1Q のいずれかのトランキングを使用します。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをルータに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

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
```

詳細については、「設定例」（P.53-31）を参照してください。

RSPAN の設定

RSPAN は、ルータで送信元セッションを、別のルータ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.53-20）
- 「RSPAN セッションの設定（SPAN コンフィギュレーション モード）」（P.53-20）
- 「RSPAN セッションの設定（グローバル コンフィギュレーション モード）」（P.53-23）

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リストで複数のイーサネット VLAN 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`	VLAN を RSPAN VLAN として設定します。
ステップ 4	`Router(config-vlan)# end`	VLAN データベースを更新して、特権 EXEC モードに戻ります。

RSPAN セッションの設定（SPAN コンフィギュレーション モード）

ここでは、SPAN コンフィギュレーション モードで RSPAN セッションを設定する手順について説明します。

- 「SPAN コンフィギュレーション モードでの RSPAN 送信元セッションの設定」（P.53-20）
- 「SPAN コンフィギュレーション モードでの RSPAN 宛先セッションの設定」（P.53-22）

SPAN コンフィギュレーション モードでの RSPAN 送信元セッションの設定

SPAN コンフィギュレーション モードで SPAN 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* `type rspan-source`	RSPAN 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 RSPAN 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。
ステップ 3	`Router(config-mon-rspan-src)# description` *session_description*	（任意）RSPAN 送信元セッションの説明を入力します。

	コマンド	目的
ステップ 4	`Router(config-mon-rspan-src)# source {single_interface | interface_list | interface_range | mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list [rx | tx | both]}`	RSPAN 送信元セッション番号を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。
ステップ 5	`Router(config-mon-rspan-src)# filter {single_vlan | vlan_list | vlan_range | mixed_vlan_list}`	（任意）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。
ステップ 6	`Router(config-mon-rspan-src)# destination remote vlan rspan_vlan_ID`	RSPAN 送信元セッション番号を RSPAN VLAN に関連付けます。
ステップ 7	`Router(config-mon-rspan-src)# no shutdown`	RSPAN 送信元セッションをアクティブにします。
ステップ 8	`Router(config-mon-rspan-src)# end`	コンフィギュレーション モードを終了します。

RSPAN 送信元セッションを設定する場合、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が、特殊文字は使用できません。Release 12.2(33)SRC およびそれ以降では、スペースは使用できます。

（注）　**description** コマンドのあとに、240 文字を入力できます。

- *RSPAN_source_span_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は
  - **interface** *type slot*/*port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port_channel** *number*
- *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。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.53-20）を参照してください。

次に、ギガビット イーサネット ポート 1/1 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 1 を設定する例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 type rspan-source
Router(config-mon-rspan-src)# source interface gigabitethernet 1/1
Router(config-mon-rspan-src)# destination remote vlan 2
Router(config-mon-rspan-src)# no shutdown
Router(config-mon-rspan-src)# end
```

詳細については、「設定例」（P.53-31）を参照してください。

SPAN コンフィギュレーション モードでの RSPAN 宛先セッションの設定

（注）　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（任意）」（P.53-12）を参照）。

RSPAN 送信元セッション ルータに RSPAN 宛先セッションを設定し、RSPAN トラフィックをローカルにモニタするようにできます。

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_source_session_number* `type rspan-destination`	RSPAN 宛先セッション番号を設定し、このセッションに対する RSPAN 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。
ステップ 3	`Router(config-mon-rspan-dst)# description` *session_description*	（任意）RSPAN 宛先セッションの説明を入力します。
ステップ 4	`Router(config-mon-rspan-dst)# source remote vlan rspan_vlan_ID`	RSPAN 宛先セッション番号を RSPAN VLAN に関連付けます。
ステップ 5	`Router(config-mon-rspan-dst)# destination {single_interface | interface_list | interface_range | mixed_interface_list} [ingress [learning]]`	RSPAN 宛先セッション番号を RSPAN VLAN に関連付けます。
ステップ 6	`Router(config-mon-rspan-dst)# end`	コンフィギュレーション モードを終了します。

RSPAN 宛先セッションを設定する場合、次の点に注意してください。

- *RSPAN_destination_session_number* の範囲は、1 ～ 80 です。
- *single_interface* は
  - **interface** *type slot/port* の形式で、type は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

    （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。

- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。

  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.10-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグ付きトラフィックをスイッチに返信する場合、ISL または 802.1Q のいずれかのトランキングを使用します。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

- **no shutdown** コマンドおよび **shutdown** コマンドは、RSPAN 宛先セッションでは、サポートされません。

次に、セッション 1 の送信元として、および、ギガビット イーサネット ポート 1/2 の宛先として、RSPAN VLAN 2 を設定する例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 type rspan-destination
Router(config-rspan-dst)# source remote vlan2
Router(config-rspan-dst)# destination interface gigabitethernet 1/2
Router(config-rspan-dst)# end
```

詳細については、「設定例」（P.53-31）を参照してください。

RSPAN セッションの設定（グローバル コンフィギュレーション モード）

ここでは、グローバル コンフィギュレーション モードで RSPAN セッションを設定する手順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 RSPAN 送信元セッションの設定」（P.53-23）
- 「グローバル コンフィギュレーション モードでの RSPAN 宛先セッションの設定」（P.53-24）

グローバル コンフィギュレーション モードでの RSPAN 送信元セッションの設定

グローバル コンフィギュレーション モードで 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。

	コマンド	目的
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 送信元番号を送信元ポートまたは VLAN に関連付け、モニタするトラフィック方向を選択します。
ステップ 3	`Router(config)# monitor session RSPAN_source_session_number destination remote vlan rspan_vlan_ID`	RSPAN 送信元セッション番号を RSPAN VLAN に関連付けます。

RSPAN 送信元セッションを設定する場合、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.53-20）を参照してください。
- *RSPAN_source_session_number* の範囲は、1 ～ 66 です。
- *single_interface* は
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*
- *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。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.53-20）を参照してください。

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、セッション 2 の宛先として、RSPAN VLAN 200 を設定する例を示します。

```
Router(config)# monitor session 2 destination remote vlan 200
```

詳細については、「設定例」（P.53-31）を参照してください。

グローバル コンフィギュレーション モードでの RSPAN 宛先セッションの設定

（注）　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（任意）」（P.53-12）を参照）。

RSPAN 送信元セッション ルータに RSPAN 宛先セッションを設定し、RSPAN トラフィックをローカルにモニタするようにできます。

グローバル コンフィギュレーション モードで 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を RSPAN VLAN に関連付けます。
ステップ 3	`Router(config)# monitor session` *RSPAN_destination_session_number* `destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [`ingress` {`learning`}]	RSPAN 宛先セッション番号を宛先に関連付けます。

モニタ セッションを設定する場合、次の点に注意してください。

- *RSPAN_source_span_session_number* の範囲は、1 ～ 66 です。
- RSPAN VLAN ID については、「RSPAN VLAN の設定」（P.53-20）を参照してください。
- *single_interface* は
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

  （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。
- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、スイッチによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。
  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.10-6）を参照してください。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、ISL または 802.1Q のいずれかのトランキングを使用します。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをスイッチに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。

- レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
- 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

次に、セッション 3 の送信元として、RSPAN VLAN 200 を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 5/4
```

詳細については、「設定例」（P.53-31）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、異なるルータ上に設定します。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.53-26）
- 「ERSPAN 宛先セッションの設定」（P.53-28）

（注） PFC3 では、ERSPAN がサポートされます（「ERSPAN に関する注意事項および制約事項」（P.53-11）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。
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)# source` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]	ERSPAN 送信元セッション番号を、CPU、送信元ポート、または VLAN に関連付け、モニタするトラフィック方向を選択します。
ステップ 5	`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 6	`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。

	コマンド	目的
ステップ 7	`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、宛先ルータ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.53-28）、ステップ 6 を参照）。
ステップ 8	`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.53-28）、ステップ 7 を参照）。
ステップ 9	`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 10	`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）値を設定します。
ステップ 11	`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 12	`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 13	`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 14	`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。
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場合、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が、特殊文字は使用できません。Release 12.2(33)SRC およびそれ以降では、スペースは使用できます。

  （注）　**description** コマンドのあとに、240 文字を入力できます。

- *ERSPAN_source_session_number* の範囲は、1 ～ 66 です。
- *single_interface* は
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

    （注）　ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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* の範囲は、1 ～ 1023 です。
- 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。ルータ上ですべての 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。

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# configure terminal
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
Router(config-mon-erspan-src-dst)# end
```

詳細については、「設定例」（P.53-31）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することはできません。

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。
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)# destination` {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} [**ingress** [**learning**]]	ERSPAN 宛先セッション番号を宛先ポートに関連付けます。
ステップ 5	`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。

	コマンド	目的
ステップ 6	`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.53-26）のステップ 7 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 7	`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.53-26）のステップ 8 で入力した ID と一致する必要があります。
ステップ 8	`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 9	`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 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場合、次の点に注意してください。

- *ERSPAN_destination_session_number* の範囲は、1 ～ 66 です。
- *single_interface* は
  - **interface** *type slot/port* の形式で、*type* は、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** になります。
  - **interface port-channel** *number*

  （注）　宛先ポート チャネル インターフェイスは、**channel-group** *group_num* **mode on** コマンドおよび **no channel-protocol** コマンドで設定する必要があります。「EtherChannel の設定」（P.12-8）を参照してください。

- *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。ルータ上ですべての 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ことも必要です（「ERSPAN 送信元セッションの設定」（P.53-26）、ステップ 7 を参照）。

- *ERSPAN_flow_id* の範囲は、1 ～ 1023 です。
- **ingress** キーワードを入力し、接続デバイスからトラフィックを受信する宛先を設定します。

- **learning** キーワードを入力して、宛先から MAC アドレス ラーニングをイネーブルにします。これにより、ルータによって、宛先に接続されているデバイスに対してトラフィックを送信できます。

  ingress キーワードと **learning** キーワードで宛先を設定する際は、次の点に注意してください。

  - レイヤ 2 スイッチング用の宛先を設定します。「レイヤ 2 スイッチング用の LAN インターフェイスの設定」（P.10-6）を参照してください。
  - 宛先がトランクで、接続デバイスがトラフィックをルータに返信する場合、ISL または 802.1Q のいずれかのトランキングを使用します。
  - 宛先がトランクで、接続デバイスがタグなしトラフィックをルータに返信する場合、設定されているネイティブ VLAN で 802.1Q トランキングを使用して、接続デバイスからのトラフィックを受信します。
  - レイヤ 3 アドレスに宛先を設定しないでください。VLAN インターフェイスを使用して、宛先に接続されているデバイスとの間でトラフィックを送受信します。
  - 宛先はダウン ステートのままです。接続デバイスとの間でトラフィックを送受信するには、追加のアクティブなレイヤ 2 ポートを VLAN に設定し、VLAN インターフェイスがアップされたままになるようにします。

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# configure terminal
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
```

詳細については、「設定例」（P.53-31）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

送信元がトランク ポートである場合に、送信元 VLAN フィルタリングは特定の 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.53-26）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*	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 フィルタリングを設定する場合、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
```

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 の設定例を示します。

```
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、複数の送信元のある RSPAN 送信元セッションの設定例を示します。

```
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
```

SPAN on EVC の設定

現在、サービス インスタンス単位のトラフィック ミラーリング、合法的傍受、またはスイッチド ポート アナライザ（SPAN）は使用できません。

既存のコマンドライン インターフェイスでサポートされるのは、インターフェイスおよび VLAN をローカル SPAN の送信元として設定することです。同じコマンドライン インターフェイスが、インターフェイスとともにサービス インスタンス ID を受け入れるように拡張されています。EVC はローカル セッション SPAN でのみサポートされるので、SPAN 送信元に対するサービス インスタンス オプションがローカル SPAN コンフィギュレーション サブモードに追加されています。

トラフィックを代行受信するように SPAN を設定する方法には次の 3 つがあります。

- SPAN on Port : ポートまたはポート チャネル上のすべての EVC のトラフィックが、そのポート上のルーティングされたトラフィックとともに SPAN セッションに含まれます。
- SPAN on VLAN : 同じ VLAN を使用するすべての EVC ブリッジ ドメインのトラフィックが、同じ VLAN 上の他のスイッチポートとともに SPAN セッションに含まれます。
- SPAN on EVC : 特定の EFP または一連の EFP のトラフィックが SPAN セッションに含まれます。

制約事項および使用上の注意事項

SPAN on EVC を設定する場合は、次の制約事項および使用上の注意事項に従ってください。

- ローカル SPAN のみがサポートされます。
- EVC SPAN は、EVC が ES+ ラインカード上にある場合にのみ有効です。
- SPAN 宛先としての EVC はサポートされていません。
- 出力 SPAN パケットには QoS 処理は行われません。
- スイッチポートと EVC ブリッジ ドメインの組み合わせが存在する場合、両方のフラッド ケース パケットにスパンされます。VLAN および SPAN は、送信元ポートの送信方向に設定されます。
- 異なる EVC ブリッジ ドメインの組み合わせが存在する場合、すべての EVC のフラッド ケース パケットにスパンされます。VLAN および SPAN は、送信元ポートの送信方向に設定されます。
- EVC SPAN は、複数の宛先ポートでは機能しません。
- 複数の SPAN セッションの一部として設定されている EVC の場合（EVC、VLAN、またはポート）、トラフィックは 1 つのセッションだけでモニタされます。
- EFP と VLAN は、同じモニタ セッションで送信元として設定できません。
- 10G ポートの場合、入力トラフィックと SPAN トラフィックの合計が 10G を超えることはできません。
- ポート シェーパーを持つ 10G ポートの場合、ポート トラフィックと SPAN トラフィックの合計がポート シェーパーを超えることはできません。
- 1G ポートの場合、合計 SPAN トラフィックは 10G まで可能ですが、ネットワーク プロセッサの制限とファブリックのボトルネックにより、ネット トラフィックは減少することがあります。

SPAN on EVC の設定

EVC で SPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *number*
4. [**no**] **ip address**
5. [**no**] **service instance** *id* **Ethernet** [*service-name*]
6. **encapsulation** {**default**|**untagged**|**dot1q** *vlan-id* [**second-dot1q** *vlan-id*]}
7. **rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** ***vlan-id*** | **dot1ad** ***vlan-id*** **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {dot1q *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} **symmetric**
8. **exit**
9. **monitor session** local_span_session_number **type [local | local-tx]**
10. **source** {interface | service instance | vlan}{GigabitEthernet |Port-channel | TenGigabitEthernet} [**rx | tx | both**]
11. **destination interface**{GigabitEthernet |Port-channel | TenGigabitEthernet}
12. [**no**] **shutdown**
13. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface port-channel *number*	ポートチャネル インターフェイスを作成します。
ステップ 4	[no] ip address	イーサネット チャネルにサブネット マスクを割り当てます。
ステップ 5	[**no**] **service instance** *id* **Ethernet** [service-name}	サービス インスタンス（EVC をインスタンス化したもの）をインターフェイスで作成し、デバイスをイーサネット サービス コンフィギュレーション サブモードに設定します。
ステップ 6	**encapsulation** {**default**|**untagged**|**dot1q** *vlan-id* [**second-dot1q** *vlan-id*]}	インターフェイス上の入力 dot1q フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。

	コマンド	目的
ステップ 7	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {dot1q *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} **symmetric**	サービス インスタンスへのフレーム入力で実行されるタグ操作を指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**monitor session** local_span_session_number **type [local | local-tx]**	SPAN セッション番号を使用してモニタ セッションを設定し、SPAN 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。
ステップ 10	**source** {interface | service instance | vlan} {GigabitEthernet |Port-channel | TenGigabitEthernet} [**rx | tx | both**]	SPAN セッション番号を送信元ポート、VLAN、または EVC に関連付け、モニタするトラフィック方向を選択します。
ステップ 11	**destination interface** {GigabitEthernet |Port-channel | TenGigabitEthernet}	SPAN セッション番号を宛先と関連付けます。
ステップ 12	**no shutdown**	SPAN セッションをアクティブにします。
ステップ 13	**end**	コンフィギュレーション モードを終了します。

設定例

これは SPAN on EVC を設定する場合の例です。

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 11
Router(config-if)# no ip address
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 13
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# exit
Router(config)# monitor session 1 type local
Router(config-mon-local)# source service instance 2 - 100 Port-channel 1 both
Router(config-mon-local)# destination interface Port-channel 3
Router(config-mon-local)# no shut
Router(config-mon-local)# end
```

SPAN on EVC の確認

ここでは、SPAN の設定を確認するコマンドを示します。

```
Router# show monitor session 1
    Session 1
    ---------
    Type                   : Local Session
    Status                 : Admin Enabled
    Source EFPs            :
        Both               : Po1:   2-100
    Destination Ports      : Po3

Router# show run | section monitor
```

```
monitor session 1 type local
 source service instance 2 - 100 Port-channel1
 destination interface Po3
```

トラブルシューティング

個別のトラブルシューティング情報については、次の URL にある Cisco Technical Assistance Center（TAC）にお問い合わせください。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

分散型出力 SPAN

集中型出力 SPAN では、レプリケーションが必要な各パケットはスーパーバイザ エンジンを通過する必要があります。これにより、ルータのパフォーマンスが低下します。分散型出力 SPAN（DES）では、送信（Tx）SPAN は、スーパーバイザ エンジンを使用する代わりに、ラインカードでローカルに複製されます。

リリース 15.2(2)S 以降では、DES は Cisco 7600 ルータでサポートされます。

DES 機能の制約事項

DES には、次の制約事項が適用されます。

- Hyperion ASIC リビジョン レベル 5.0 以上および Metropolis ASIC のすべてのバージョンは、ERSPAN 送信元に対する DES モードをサポートします。
- Hyperion ASIC リビジョン レベル 5.0 未満のスイッチング モジュールは、ERSPAN 送信元に対する DES モードをサポートしません。
- ローカル SPAN および RSPAN セッションの場合は、DES を使用できないカードが原因で集中型出力モードに戻されます。
- DES を使用できないカードは、非 DFC ラインカード、Titan がないラインカード、Hyperion、または Metropolis です。
- DES は、レガシーのグローバル コンフィギュレーション コマンドではなく、サブモード コマンドを使用して設定する必要があります。

分散型出力 SPAN の設定

ここでは、出力レプリケーション モードを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session egress replication-mode centralized**
4. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no monitor session egress replication-mode centralized**	分散型出力 SPAN モードをイネーブルにします。デフォルトでは、SPAN モードは集中型です。 （注）　集中型出力 SPAN モードをイネーブルにするには、**monitor session egress replication-mode centralized** コマンドを入力します。
ステップ 4	**end**	コンフィギュレーション モードを終了します。

設定例

次に、出力レプリケーション モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# no monitor session egress replication-mode centralized
Router(config)# end
```

次に、出力レプリケーション モードをディセーブルにする例を示します。

```
Router# configure terminal
Router(config)# monitor session egress replication-mode centralized
Router(config)# end
```

設定の確認

次に、出力レプリケーション モードを表示する例を示します。

```
Router# show monitor session egress replication-mode
Egress SPAN Replication Mode Session State:
-------------------------------------------
Session          : 1
Session Type     : Local Session
Operational mode : Distributed
Configured mode  : Distributed/Default

Session          : 2
Session Type     : Local Session
Operational mode : Distributed
Configured mode  : Distributed/Default

-----------------------------------------------------
Global Egress SPAN Replication Mode Capability:

Slot          Egress Replication Capability
 No       LSPAN           RSPAN             ERSPAN
-----------------------------------------------------
```

```
 2     Centralized      Centralized        Centralized
 7     Distributed      Distributed        Distributed
 8     Distributed      Distributed        Distributed
 12     Distributed      Distributed         Distributed

Router# show monitor session 1
Session 1
---------
Type                   : Local Session
Status                 : Admin Enabled
Source Ports           :
    Both               : Fa2/3
Destination Ports      : Fa2/1
    Ingress & Learn    : Fa2/1

Egress SPAN Replication State:
Operational mode       : Distributed
Configured mode        : Distributed

Router# show monitor session 1 detail
Session 1
---------
Type                   : Local Session
Status                 : Admin Enabled
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa2/3
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source EFPs            :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : Fa2/1
    Ingress & Learn    : Fa2/1
Filter VLANs           : None
Dest RSPAN VLAN             : None
Source IP Address      : None
Source IP VRF          : None
Source ERSPAN ID       : None
Destination IP Address : None
Destination IP VRF     : None
Destination ERSPAN ID  : None
Origin IP Address      : None
IP QOS PREC            : 0
IP TTL                 : 255

Egress SPAN Replication State:
Operational mode       : Distributed
Configured mode        : Distributed
```

トラブルシューティング

個別のトラブルシューティング情報については、次の URL にある Cisco Technical Assistance Center（TAC）にお問い合わせください。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

CHAPTER 54

SNMP ifIndex パーシステンスの設定

この章では、Cisco 7600 シリーズ ルータに SNMP 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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章で説明する内容は、次のとおりです。

- 「SNMP ifIndex パーシステンス」（P.54-1）
- 「SNMP ifIndex パーシステンスの設定」（P.54-2）

SNMP ifIndex パーシステンス

SNMP ifIndex パーシステンス機能は、ルータ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、ルータ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、デバイス インベントリ、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ルータ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 パーシステンス機能は、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。

次の定義は、RFC 2233『The Interfaces Group MIB using SMIv2』に基づいています。次の用語は、Interfaces MIB（IF-MIB）に含まれる値です。

- **ifIndex**：一意の番号（ゼロより大きい）で、各インターフェイスをそのインターフェイスの SNMP 識別に関して識別します。
- **ifName**：テキストベースのインターフェイス名（例：ethernet 3/1）。
- **ifDescr**：インターフェイスの記述。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 パーシステンスの設定

ここでは、SNMP ifIndex パーシステンスの設定手順について説明します。

- 「SNMP ifIndex パーシステンスのグローバルなイネーブル化」（P.54-2）（任意）
- 「特定のインターフェイス上における SNMP ifIndex パーシステンスのイネーブル化およびディセーブル化」（P.54-2）（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 パーシステンスのグローバルなイネーブル化

SNMP ifIndex パーシステンスは、デフォルトでディセーブルになります。SNMP ifIndex パーシステンス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 パーシステンスをグローバルにイネーブルにします。

次の例では、SNMP ifIndex パーシステンスがすべてのインターフェイスでイネーブルにされます。

```
router(config)# snmp-server ifindex persist
```

SNMP ifIndex パーシステンスのグローバルなディセーブル化

SNMP ifIndex パーシステンス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 パーシステンスをグローバルにディセーブルにします。

次の例では、SNMP ifIndex パーシステンス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 パーシステンス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だけ、SNMP ifIndex パーシステン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)# 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 パーシステンス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は使用できません。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 パーシステンスが、イーサネット インターフェイス 3/1 でだけ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 でだけ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 パーシステンス設定の消去

インターフェイス固有の SNMP ifIndex パーシステンス設定を消去し、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 パーシステンス設定を消去し、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、インターフェイス Ethernet 3/1 における SNMP ifIndex パーシステンス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 パーシステンスがグローバルにイネーブルに設定されている場合、SNMP ifIndex パーシステンスはイーサネット インターフェイス 3/1 でイネーブルになります。SNMP ifIndex パーシステンス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 パーシステンスは、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 55

電源管理および環境モニタリング

この章では、Cisco 7600 シリーズ ルータの電源管理および環境モニタリング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 7600 Series Routers Command References』を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「電源管理の機能概要」（P.55-1）
- 「環境モニタリングの機能概要」（P.55-10）

電源管理の機能概要

ここでは、Cisco 7600 シリーズ ルータの電源管理について説明します。

- 「電源の冗長構成のイネーブル化およびディセーブル化」（P.55-2）
- 「モジュールの電源切断および電源投入」（P.55-3）
- 「システムの電力ステータスの確認」（P.55-4）
- 「モジュールの電源オフ / オン」（P.55-4）
- 「電源のオフ / オン」（P.55-5）
- 「システムの所要電力の判別」（P.55-5）
- 「システムのハードウェア容量の判別」（P.55-5）
- 「センサーの温度しきい値の判別」（P.55-9）

（注） システムにインストールされる電源装置は、ワット数定格が異なる場合があります。インストールされる電源装置は、両方とも AC 入力か、両方とも DC 入力か、または一方が AC 入力で一方が DC 入力の場合があります。電源装置は、冗長モードまたは非冗長モードのいずれかで構成されます。サポートされる電源構成についての詳細については、『*Cisco 7600 Series Router 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.55-5）を参照してください。

電源の冗長構成のイネーブル化およびディセーブル化

冗長構成をディセーブルまたはイネーブルにするには、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** コマンドを入力します（「システムの電力ステータスの確認」（P.55-4）を参照）。

表 55-1 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 55-1　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 メッセージが表示されます。 • 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 メッセージが表示されます。 • 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 メッセージが表示されます。 • 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 メッセージが表示されます。 • 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 55-1　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 メッセージが表示されます。 • 両方の電源装置に電源が入ります。使用可能な合計ワット数は、より高いワット数の電源の出力ワット数です。システムの電源の使用が、より低いワット数の電源装置の最大共有限度を超えると、システムでは、過電流から保護するため、容量がより低い電源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 メッセージが表示されます。 • 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 メッセージが表示されます。 • 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 メッセージが表示されます。 • 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。
ワット数が異なり冗長構成がイネーブルの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 メッセージが表示されます。 • 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。
ワット数が等しいかまたは異なり、冗長構成がディセーブルの電源装置を取り付け、システムを起動した場合	• システム ログと、Syslog メッセージが表示されます。 • 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 CLI 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`	モジュールの電源を投入します。
	`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#
```

特定の電源に対する現在の電力ステータスを表示するには、次のように **show power** コマンドを入力します。

```
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#
```

コマンドに電源番号を指定して、電源の入力フィールドを表示できます。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* コマンドを入力します。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。

電源のオフ/オン

冗長電源がある場合にどちらかの電源をオフ/オンすると、この電源だけがオフ/オンされます。両方の電源をオフ/オンすると、システムはいったん停止し、10 秒以内に復帰します。

電源が 1 つしかない場合にこの電源をオフ/オンすると、システムはいったん停止し、10 秒以内に復帰します。

次に、電源をオフ/オンする例を示します。

```
Router# hw-module power-supply 2 power-cycle
Power-cycling the power supply may interrupt service.
Proceed with power-cycling? [confirm]
Power-cycling power-supply 1
22:10:23: %C6KPWR-SP-2-PSFAIL: power supply 1 output failed.
22:10:25: %C6KENV-SP-4-PSFANFAILED: the fan in power supply 1 has failed
22:10:33: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
22:10:33: %C6KENV-SP-4-PSFANOK: the fan in power supply 1 is OK
Router#
```

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

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使用率
- スイッチ ファブリックの使用率
- CPU（1 つまたは複数）の使用率
- メモリ デバイス（フラッシュ、DRAM、NVRAM）の使用率

次に、Cisco 7600 シリーズ ルータのルート 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 容量とその使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、Cisco 7600 シリーズ ルータのルート 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使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、および割合（%）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 の容量および使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、SPAN 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の容量および使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使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、Cisco 7600 シリーズ ルータ内の各 EARL に対する QoS ポリサー リソースの容量および使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、VLAN 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#
```

センサーの温度しきい値の判別

システム センサーは、さまざまな温度しきい値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、各センサーに対して許可される温度を判別できます。

次に、センサーの温度しきい値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
```

環境モニタリングの機能概要

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することができます。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リング

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**：アラームしきい値を表示します。
- **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、およびスロット単位の冷却容量を表示します。
- **status**：現場交換可能ユニット（FRU）の動作ステータスおよび電源と温度の情報を表示します。
- **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、**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、メジャーとマイナーの 2 種類のアラームを示します。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 分間アラームは取り消されず、いかなる（モジュールのリセットまたはシャットダウンなどの）措置も行われません。この間に温度がアラームしきい値より 5° C（41° F）下がると、アラームは取り消されます。

表 55-2 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、『*Cisco 7600 Series Router Module Installation Guide*』を参照してください。

表 55-2　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リング

コンポーネント	アラーム タイプ	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ーがメジャーしきい値を超過[1]	メジャー	STATUS[2] LED レッド[3]	Syslog メッセージおよび SNMP 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ーが、マイナーしきい値を超過	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ーがメジャーまたはマイナーしきい値を超過	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 アラームが発生し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。

表 55-2　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リング （続き）

コンポーネント	アラーム タイプ	LED 表示	アクション
スイッチング モジュールの温度センサーがメジャーしきい値を超過	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ーがマイナーしきい値を超過	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. 温度センサーは、主要なスーパーバイザ エンジン コンポーネント（ドーター 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.55-1）を参照してください。

CHAPTER 56

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; Web キャッシュ通信プロトコル）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 Cisco 7600 シリーズ ルータを設定する方法、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 7600 Series Routers Command References』を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- PFC は、WCCP をサポートしています。
- 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 Cisco 7600 シリーズ ルータで 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
- 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。

- 「WCCP の概要」（P.56-2）
- 「WCCPv2 の制約事項」（P.56-7）
- 「WCCP の設定」（P.56-8）
- 「WCCP 設定の確認およびモニタリング」（P.56-12）
- 「WCCP の設定例」（P.56-12）
- 「WCCP での VRF サポート」（P.56-16）

（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 に関連付けられたハードウェアとネットワークの計画に関する情報については、Cisco.com Web Scaling サイトで製品パンフレットと製品マニュアルのリンクを参照してください。

WCCP の概要

ここでは WCCP について説明します。

- 「WCCP の概要」（P.56-2）
- 「ハードウェア アクセラレーション」（P.56-3）
- 「WCCPv1 設定の概要」（P.56-4）
- 「WCCPv2 設定の概要」（P.56-5）
- 「WCCPv2 の機能」（P.56-6）

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、これを使用してキャッシュ 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）　シスコは 2001 年 7 月に、Cache Engine 500 シリーズ プラットフォームの後継として一連の Content Engine プラットフォームを発表しました。Cache Engine 製品としては、Cache Engine 505、550、570、および 550-DS3 がありました。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が削減され、ダウンロード時間が短縮されます。

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。トランスペアレント 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「トランスペアレント」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、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、クラスタリング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、各キャッシュ メンバーが並行して動作できるので、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、およびアベイラビリティが向上します。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 アクセラレーション

Cisco 7600 シリーズ ルータを Cisco Cache Engine に直接接続すると、WCCP レイヤ 2 PFC リダイレクション ハードウェアが加速されます。これは、Generic Route Encapsulation（GRE）を備えた MSFC ソフトウェアでのレイヤ 3 リダイレクションよりも効率的です。

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。直接接続されたキャッシュ エンジンを設定すると、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ションできます。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、それぞれのキャッシュで使用されるリダイレクション方法が表示されます。

WCCP レイヤ 2 PFC リダイレクションについては、次の注意事項が適用されます。

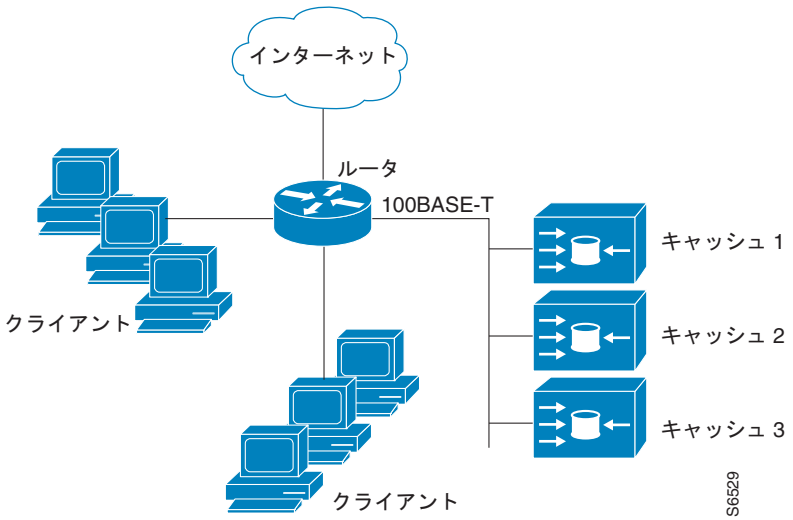
- WCCP レイヤ 2 PFC リダイレクション機能では、IP フロー マスクが full-flow モードに設定されます。
- Cisco Cache Engine ソフトウェア リリース 2.2 以降のリリースを設定すると、WCCP レイヤ 2 PFC リダイレクション機能を使用できます。
- レイヤ 2 リダイレクションは PFC で実行され、MSFC にはわかりません。MSFC で **show ip wccp web-cache detail** コマンドを実行すると、レイヤ 2 リダイレクションが行われたフローの 1 番めのパケットだけの統計情報が表示されます。これにより、パケットではなく、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）
- PFC は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）用にハードウェアを加速します。Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）で WCCP レイヤ 3 リダイレクションを使用すると、ハードウェアによってカプセル化が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。
- 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。この場合、このルータがすべての IP パケット リダイレクションを実行します。図 56-1 に、構成例を示します。

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。

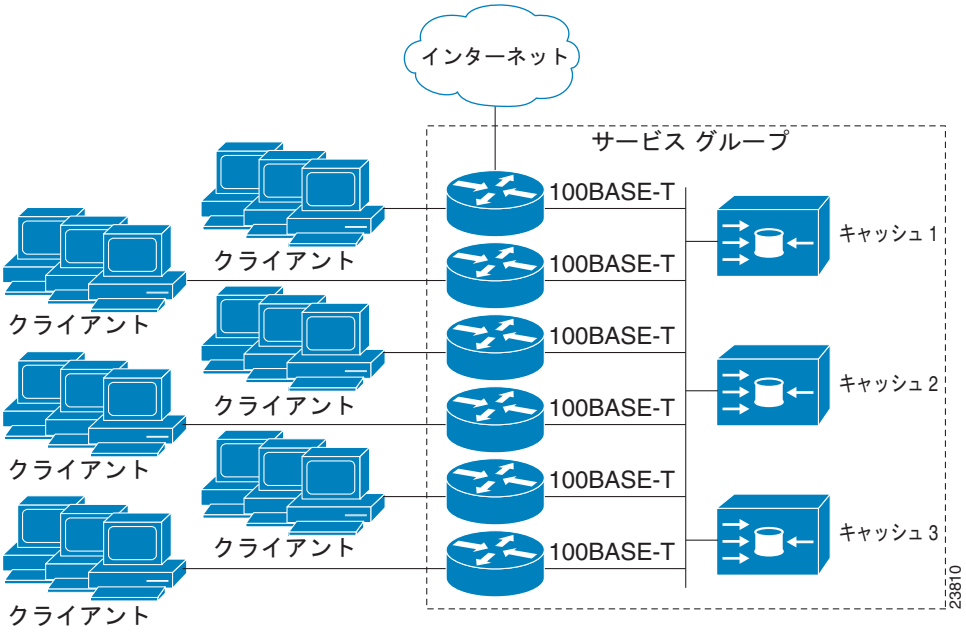
WCCPv1 設定の機能の詳細を次の一連のイベントで示します。

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、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。クラスタのメンバーシップが一定時間同じままになった後で、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 台のルータだけしかコンテンツ要求をクラスタにリダイレクトできない WCCPv1 とは対照的です。図 56-2 に、複数のルータを使用した構成例を示します。

図 56-2　WCCPv2 を使用する Cisco Cache Engine のネットワーク設定



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 およびユーザ データグラム プロトコル（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している必要があります。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 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をす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 エンジンに設定するアドレスが 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。

次の一連のイベントで、WCCPv2 設定の動作の詳細について説明します。

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 エンジンにより、キャッシュ エンジン自体の存在と、各キャッシュ エンジンと通信が確立されているすべてのルータのリストが通知されます。ルータは、ルータが保有しているグループ内のキャッシュ エンジンのビュー（リスト）を返します。
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
- 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）トラフィックだけのリダイレクションをサポートしています。WCCPv2 では、他のポート宛てのパケットをリダイレクトできます。たとえば、プロキシ Web キャッシュ処理、ファイル転送プロトコル（FTP）キャッシング、FTP プロキシの処理、80 以外のポートの Web キャッシング、リアル オーディオ、ビデオ アプリケーション、およびテレフォニー アプリケーションに使用されるポートなどです。

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 コンフィギュレーション 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 メンバー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 グループ内のキャッシュ エンジンは、プロトコル（TCP または UDP）によってリダイレクトされ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 グループと照合されます。

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。

MD5 セキュリティ

WCCPv2 には、パスワードと HMAC MD5 標準を使用して、どのルータとキャッシュ エンジンをサービス グループに含めるかを制御できる、オプションの認証機能があります。共有秘密キー 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、メッセージを代行受信、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、エラーまたは過負荷のためにキャッシュ内の要求されたオブジェクトを提供できない場合、その要求をルータに返送し、最初に指定された宛先サーバへ転送されるようにします。WCCPv2 はパケットをチェックし、処理されずにキャッシュ エンジンから返送された要求を特定します。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行いません）。これにより、エラー処理はクライアントに意識されません。

キャッシュ エンジンがパケットを拒否し、パケット リターン機能を実行する一般的な状況は次のとおりです。

- キャッシュ エンジンが過負荷状態で、パケットを処理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が逆効果を招く特定の状況（IP 認証をオンにしたときなど）をフィルタリングしている場合

負荷分散

WCCPv2 を使用して各キャッシュ エンジンにかかる負荷を調整すると、利用可能なリソースを効率的に使用するとともに、高い Quality of Service（QoS）をクライアントに提供できます。WCCPv2 では、指定キャッシュが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 エンジンだけに送信できました。
- ロード バランシング：キャッシュ エンジンに割り当てられたハッシュ バケット セットを調整することにより、過負荷状態にあるキャッシュ エンジンから、容量に空きのある他のメンバーに負荷を移動できます。
- 負荷制限：キャッシュ エンジンの容量を超えないよう、ルータが負荷を選択的にリダイレクトできます。

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、輻輳の可能性を低減できます。

WCCPv2 の制約事項

WCCPv2 には次の制約事項があります。

- WCCP が動作するのは IP ネットワークだけです。
- マルチキャスト クラスタにサービスを提供するルータには、存続可能時間（TTL）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、メンバー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。

WCCP の設定

次の設定作業は、ネットワークに導入するキャッシュ 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手順については、『*Cisco Cache Engine Configuration 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。ルータの設定作業の例は、この項で説明します。コマンド構文の詳細については、リリース 12.2 の『*CiscoIOS Configuration Fundamentals Command Reference*』を参照してください。

次の項では、WCCP の設定方法について説明します。

- 「WCCP のバージョンの指定」（P.56-8）（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.56-10）（任意）
- 「マルチキャスト アドレスへのルータの登録」（P.56-10）（任意）
- 「WCCP サービス グループのアクセス リストの使用」（P.56-11）（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 サービスを設定しない限り、ルータ上で 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 がサービスに使用されますが、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 のバージョンをバージョン 2 からバージョン 1 に変更する、または最初にバージョン変更した後で WCCPv2 に戻すには、特権 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、ルータ上で WCCPv1 が動作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、ルータ上で現在動作している WCCP プロトコルのバージョン番号が表示されます。

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、それをキャッシュ 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 以外の広く知られているサービスの記述は不要です（この場合はコマンドライン インターフェイス（CLI）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 デバイスを複数のサービス 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、逆プロキシ サービスを指定します。ただし、他のキャッシュ デバイスは、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、Cisco 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 デバイス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。

Cisco 7600 シリーズ ルータ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）　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; シスコ エクスプレス フォワーディング）、distributed Cisco Express Forwarding（dCEF; 分散 CEF）、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調べ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、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インバウンド パケットのリダイレクションからの除外を許可します。

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す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 コマンドを使用する必要があります）。

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リング

WCCP の設定を確認およびモニタリングするには、EXEC モードで次の作業を実行します。

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」などと表示されます。
`Router# show ip wccp {web-cache | service-number} view`	特定のサービス グループのどのデバイスが検出され、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どこかを表示します。**view** キーワードは、サービス グループのアドレス一覧を示します。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。詳細なトラブルシューティング情報を表示するには、**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、次の設定例を示します。

- 「ルータでの WCCP のバージョン変更例」（P.56-13）
- 「一般的な WCCPv2 設定の実行例」（P.56-13）
- 「Web キャッシュ サービスの実行例」（P.56-13）
- 「逆プロキシ サービスの実行例」（P.56-14）
- 「マルチキャスト アドレスへのルータの登録例」（P.56-14）
- 「アクセス リストの使用例」（P.56-14）
- 「ルータおよびキャッシュ エンジンのパスワード設定例」（P.56-15）
- 「WCCP 設定の確認例」（P.56-15）

ルータでの WCCP のバージョン変更例

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 に着信する 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の例を示します。

```
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
```

逆プロキシ サービスの実行例

次の例は、逆プロキシ 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 を使用して逆プロキシ 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。インターフェイス VLAN 60 から発信されるパケットにリダイレクションを適用します。

```
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 から 12.1.1.1 へ送信される要求がキャッシュをバイパスし、その他すべての要求は通常どおりに処理される例を示します。

```
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、インターフェイス VLAN 70 経由で受信し、209.165.196.51 以外の任意のホストを宛先とする Web 関連パケットを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、WCCPv2 パスワード設定セッションでパスワードに alaska1 を設定する例を示します。

```
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
```

WCCP での VRF サポート

Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）は、同じルータ上で同時に複数のインスタンスのルーティング テーブルを共存させるための IP テクノロジーです。Cisco IOS 15.1(3)S よりも前のリリースでは、VRF は Web Cache Communication Protocol（WCCP）のサポートに含まれていませんでした。リダイレクトするトラフィックの特性を定義するサービス グループは、グローバルに設定されていました。WCCP での VRF サポートでは、VRF 向けサポートの実装を可能にすることで既存の WCCP プロトコルが強化され、各 VRF ごとにサービス グループを設定することができます。サービス識別子と WCCP プロトコル パケットの VRF 識別子の両方を使用して、キャッシュ エンジンと設定済みサービス グループが関連付けられます。

WCCP での VRF サポートの設定

WCCP で VRF サポートを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **ip wccp [vrf** *vrf-name***] {web-cache |** *service-number* **| source-interface** *source-interface***} [group-address** *group-address***] [redirect-list** *access-list***] [group-list** *access-list*] [password *password*]
7. **interface** *type number*
8. **ip vrf forwarding** *vrf-name*
9. **ip address** *ip-address subnet-mask*
10. **ip wccp [vrf** *vrf-name***] {web-cache | service-number} redirect {out | in}**
11. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router(config)# terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* **例：** `Router(config)# ip vrf vrf1`	VRF コンフィギュレーション サブモードを開始し、VRF に関連する変数を設定します。
ステップ 4	**rd** *route-distinguisher* **例：** `Router(config-vrf)# rd 100:1`	8 バイトの Route Distinguisher（RD; ルート識別子）を指定します。 **route-distinguisher**：このルート識別子（RD）は、プロバイダーのネットワーク内で VPN を識別するための数値です。Autonomous System（AS; 自律システム）番号と任意の数値（xxx:y）、または IP アドレスと任意の数値（A.B.C.D:y）のいずれかを入力します。

	コマンド	目的
ステップ 5	**exit** **例：** `Router(config-vrf)# exit`	VRF 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	**ip wccp vrf** *vrf-name* **{web-cache |** *service-number* **| source-interface** *source-interface***}** **[accelerated] [group-address** *group-address***]** **[redirect-list** *redirect-list***] [group-list** *group-list***] [password** *password***]** **例：** `Router(config)# ip wccp vrf vrf1 web-cache`	WCCP サービスをイネーブルにします。 • **vrf-name**：サービス グループと関連付ける VRF 名を指定します。 • **service-number**：ダイナミック サービス番号を指定します。0 ～ 255 の数字を指定できます。 • **source-interface**：WCCP が優先ルータ ID として使用するインターフェイスを指定します。 • **group-address**：サービス グループで使用される IP マルチキャスト アドレスを指定します。 • **redirect-list**：トラフィックをリダイレクトするためのアクセス リストを指定します。 • **group-list**：データ トラフィックをフィルタリングするためのアクセス リストを指定します。 • **password**：認証パスワードを指定します。
ステップ 7	**interface gigabitethernet** *slot/port* or **interface tengigabitethernet** *slot/port* **例：** `Router(config)# interface gigabit ethernet 1/1`	WCCP での VRF サポートを設定するためのインターフェイスを指定します。 ***slot/port***：インターフェイスの場所を指定します。
ステップ 8	**ip vrf forwarding** *vrf-name* **例：** `Router(config)# ip vrf forwarding vrf1`	指定された VRF をインターフェイスに適用します。
ステップ 9	**ip address** ***ip-address subnet-mask*** **例：** `Router(config)# ip address 10.1.1.0 255.255.255.0`	インターフェイスに IP アドレスを指定します。

	コマンド	目的
ステップ 10	**ip wccp vrf** *vrf-name* {**web-cache** | *service-number*} **redirect** {**out** | **in**} **例：** `Router(config-if)# ip wccp vrf vrf1 web-cache redirect in`	WCCP を使用するインバウンドまたはアウトバウンド インターフェイスでリダイレクションをイネーブルにします。
ステップ 11	**end** `Router(config-if)# end`	コンフィギュレーション セッションを終了します。

例

次に、VRF が設定されたインターフェイスに Web キャッシュ サービスを設定する例を示します。

```
Router# enable
Router# configure terminal
Router(config)# ip vrf vrf1
Router(config-vrf1)# rd 100:1
Router(config)# ip wccp vrf vrf1 web-cache
Router(config)# interface gigabitethernet 1/1
Router(config-if)# ip vrf forwarding vrf1
Router(config-if) ip address 100.1.1.1 255.255.0.0
Router(config-if)# ip wccp vrf vrf1 web-cache redirect in
Router(config-if)# end
```

次に、VRF と ACL が設定されたインターフェイスに Web キャッシュ サービスを設定する例を示します。

```
Router# enable
Router# configure terminal
Router(config)# ip vrf vrf2
Router(config-vrf1)# rd 200:1
Router(config)# ip wccp vrf vrf2 web-cache
Router(config)# ip access-list extended wccp_acl
Router(config-ext-nacl)# 10 deny tcp any eq www any eq www
Router(config-ext-nacl)# 20 permit ip any any
Router(config)# ip wccp vrf vrf2 web-cache redirct-list wccp_acl
Router(config)# interface gigabitethernet 1/2
Router(config-if)# ip vrf forwarding vrf2
Router(config-if)# ip address 200.1.1.1 255.255.0.0
Router(config-if)# ip wccp vrf vrf2 web-cache redirect in
Router(config-if)# end
```

検証

show ip wccp summary コマンドを使用して、VRF 固有の WCCP 設定も含め、すべての WCCP サービスの概要を表示します。

```
Router# show ip wccp summary
WCCP version 2 enabled, 2 services

Service     Clients   Routers   Assign      Redirect   Bypass
-------     -------   -------   ------      --------   ------
Default routing table (Router Id: 15.0.0.2):
web-cache   1         1         MASK        L2         L2
```

```
VRF vrf1 (Router Id: 6.6.6.5):
web-cache   1         1         MASK        L2          L2
```

show ip wccp vrf *vrf-id* コマンドを使用して、VRF 固有の WCCP 設定を表示します。

```
Router# show ip wccp vrf vrf1
VRF RED WCCP information:
    Router information:
        Router Identifier:                   80.20.1.3
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Service Group Clients:     1
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        Total Packets Dropped Closed:        0
        Redirect access-list:                -none-
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
```

トラブルシューティングのヒント

コマンド	目的
debug ip wccp vrf *vrf-id*	重要な WCCP イベントまたはルータによって送受信された各 WCCP パケットに関する情報を表示します。

CHAPTER 57

Top N ユーティリティの使用

この章では、Cisco 7600 シリーズ ルータで Top N ユーティリティを使用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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章で説明する内容は、次のとおりです。

- 「Top N ユーティリティの概要」（P.57-1）
- 「Top N ユーティリティの使用」（P.57-2）

Top N ユーティリティの概要

ここでは、Top N ユーティリティについて説明します。

- 「Top N ユーティリティの概要」（P.57-1）
- 「Top N ユーティリティ操作の概要」（P.57-2）

Top N ユーティリティの概要

Top N ユーティリティを使用すると、ルータ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、Top 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 Top 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

表 57-1　有効な Top N の統計タイプ （続き）

統計タイプ	定義
multicast	入力および出力マルチキャスト パケット数
overflow	バッファ オーバーフローの数
packets	入力および出力パケット数
utilization	使用率

（注）　Top N ユーティリティはポート使用率を計算する際、Tx および Rx 回線を同一カウンタにまとめます。また、使用率の割合（%）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。

Top 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。Top 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** コマンドを入力します。Top 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、Top N ユーティリティは Top N 処理についての簡単な概要情報を表示します。

Top N の処理を終了するには、**clear top counters interface report** コマンドを入力します。Ctrl+C を押しても、Top 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。

Top N ユーティリティの使用

ここでは、Top N ユーティリティを使用する手順について説明します。

- 「Top 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.57-2）
- 「Top N ユーティリティ レポートの表示」（P.57-3）
- 「Top N ユーティリティ レポートの消去」（P.57-4）

Top N ユーティリティによるレポート作成のイネーブル化

Top 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]`	Top 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**

Top 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、次の点に注意してください。

- レポート作成の対象として、最もビジーなポート数を指定できます（デフォルトは 20）。
- ポートが最もビジー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、使用率が最も高い 4 つのポートに対し、Top 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.
```

Top N ユーティリティ レポートの表示

Top 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]`	Top 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。

Top 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 回め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 Top 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 Top 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
```

Top N ユーティリティ レポートの消去

Top 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 Top 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 Top 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

スイッチ仮想インターフェイス上の双方向フォワーディングおよび検出の設定

この章では、Cisco 7600 シリーズ ルータ にスイッチ仮想インターフェイス（SVI）上の双方向フォワーディングおよび検出（BFD）を設定する手順について説明します。

（注） この章で使用され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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

この章の内容は、次のとおりです。

- 「BFD over SVI の概要」（P.58-1）
- 「制約事項および使用上の注意事項」（P.58-1）
- 「BFD over SVI を使用したサンプル ネットワーク」（P.58-2）
- 「BFD over SVI の設定」（P.58-4）

BFD over SVI の概要

スイッチ仮想インターフェイス（SVI）は、特定の仮想ローカル エリア ネットワーク（VLAN）に属する、レイヤ 2 スイッチ ポート用の基本的なレイヤ 3 機能を提供するよう設計されたインターフェイスのタイプです。SVI は、VLAN インターフェイスで設定された IP アドレスを使用して、レイヤ 2 ドメインをレイヤ 3 ルーティング ドメインに接続します。

レイヤ 2 ネットワークの SVI を使用してレイヤ 3 ルーティング ドメインへのアクセスを提供する場合は、Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）を使用して、ネットワークのデータ トラフィック障害を検出できます。

（注） BFD over SVI 機能を設定する場合、ソフトウェア バージョンを 15.1(1)S から 15.0(1)S にダウングレードする前に、ソフトウェアで **platform bfd allow-svi** コマンドを実行する必要があります。

制約事項および使用上の注意事項

BFD over SVI 機能を設定する場合は、次の制約事項および注意事項に従ってください。

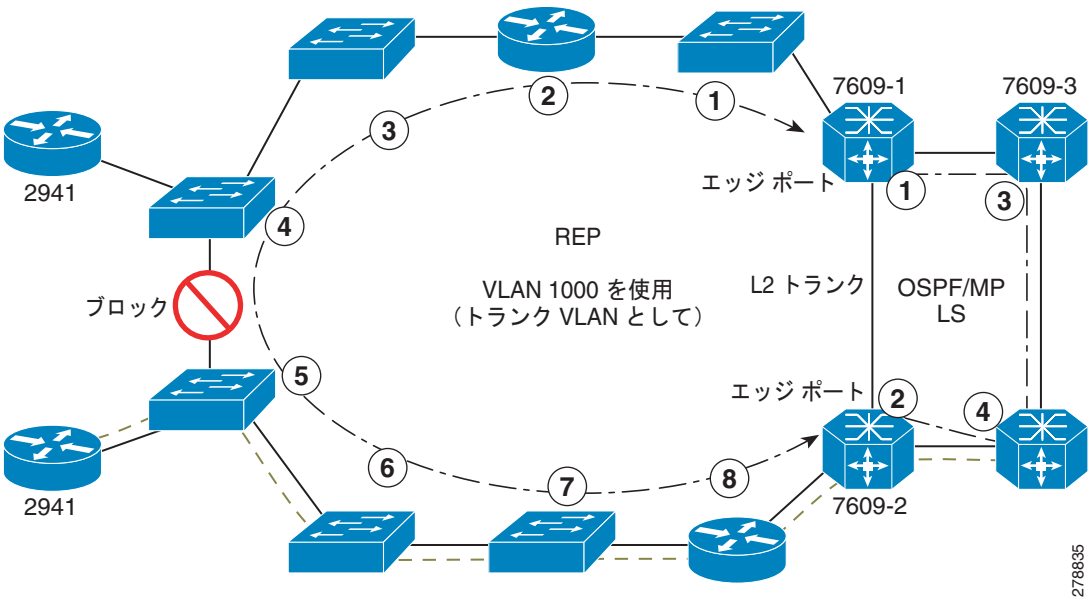
- BFD over SVI は、BFD がサポートされているすべてのハードウェア プラットフォームでサポートされています。
- BFD over SVI に対するタイマー サポートは、メインおよびサブ インターフェイスでサポートされる BFD タイマー値と同様です。
- BFD がポート チャネルで実行されている場合は、BFD over SVI には、750 * 3 ミリ秒のタイマー値制限があります。
- **no ip redirect** コマンドをすべての BFD インターフェイスで実行して、C7600 シリーズ ルータでのデータ パスを最適化します。

BFD over SVI を使用したサンプル ネットワーク

図 58-1 に、REP がイネーブルなリング トポロジで BFD over SVI を使用したネットワークの例を示します。ネットワークの左側のセル サイト ルータ（CSR）は、レイヤ 2 ネットワーク上で C7600 ルータに集約されます。C7600 に設定された SVI は CSR にレイヤ 3 サービスを提供します。

CSR から 7600 ルータへのアップストリーム トラフィックのルーティングは、CSR でのスタティック ルートによって実現されます。そのスタティック ルートでは、C7600 ルータ（7609-1）の 1 台をプライマリ ルートとして指定し、バックアップ ノードとして動作する代替 C7600 ルータ（7609-2）をまたセカンダリ ルートとして指定します。スタティック ルート プリファレンスはスタティック ルート設定のメトリック値を使用して設定されます。

図 58-1　　BFD over SVI ネットワーク



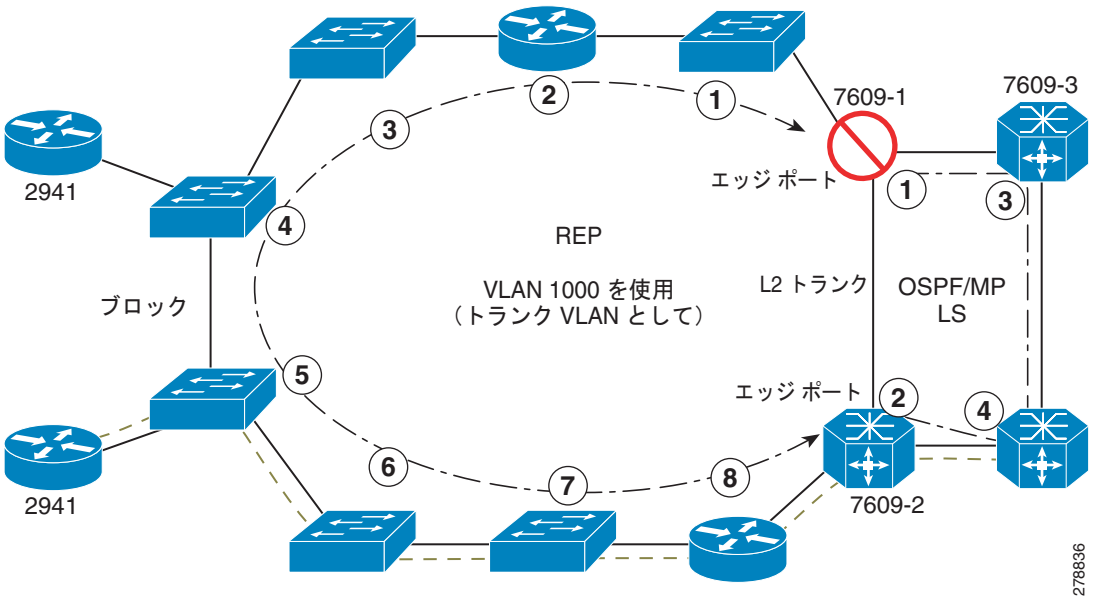
このようなトポロジでは、ネットワークのデータ トラフィック障害を処理するためにノード障害保護とリンク障害保護を展開できます。

ノード障害

ノード障害が BFD によって保護されるスタティック ルートを介して処理されます。プライマリ ノードで障害が発生した場合、BFD は障害を検出し、バックアップ ノードを介してネットワークの再コンバージェンスを開始します。スタティック ルートは CSR で使用されるため、再コンバージェンスに必要なのは、セカンダリまたはバックアップ ルートの初期化だけです。

図 58-2 では、リング トポロジがイネーブルな REP で BFD over SVI を使用したネットワークのノード障害を説明します。ネットワーク内のルータ 7609-1、7609-2 および 2 台の 2941 ルータは、保護されたノードです。プライマリ ノード（7609-1）に障害がある場合、トラフィックはセカンダリ ノード（7609-2）にリダイレクトされます。1 ～ 8 の番号が付けられているレイヤ 2 ノードは、保護されていません。

図 58-2　　ノード障害



プライマリ ノードに障害が発生した場合、次のイベントが実行されます。

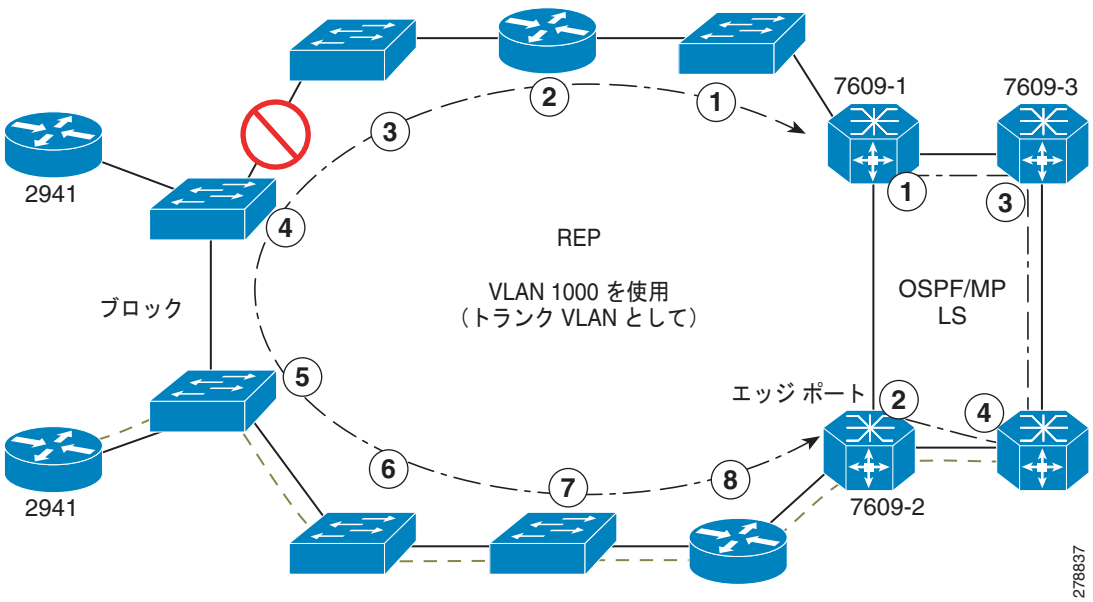
1. レイヤ 2 レベルで、REP はプライマリ パスが不良になり、セカンダリ パスを開くことを検知します。
2. レイヤ 3 レベルで、BFD はプライマリ ノード障害を検出し、セカンダリ ノードへのネットワーク コンバージェンスを開始します。

リンク障害

レイヤ 2 ネットワークのリンク障害は、REP によって処理されます。通常、REP は 100 ミリ秒未満でリング内のリンク障害を検出します。プライマリ レイヤ 2 パスで障害が発生した場合、REP はレイヤ 3 トラフィック用のセカンダリ レイヤ 2 パスを開きます。

図 58-3 では、BFD over SVI を使用したネットワークのリンク障害を説明します。レイヤ 2 リングでプライマリ リンク障害がある場合、REP はレイヤ 2 レベルでプライマリ パスが不良になり、セカンダリ パスを開くことを検出します。ノード障害がないため、BFD は検出せず、どのようなネットワーク変更も開始されません。

図 58-3　リンク障害



REP は、BFD よりも前にネットワークの障害をすべて検出して動作する必要があります。そうでなければ、BFD がノード障害を誤検出する可能性があります。プライマリ レイヤ 2 パスでリンク障害があり、REP がセカンダリ パスを非ブロック化するのに BFD よりも長い時間がかかる場合、BFD はノード障害を誤検出する可能性があります。その場合、REP によるセカンダリ パスの非ブロック化後、トラフィックはセカンダリ ノードを通過します。

REP の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/rep.html

BFD over SVI の設定

BFD over SVI を設定するには、次の手順を実行してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan** *number*
4. **ip address** *ip-address mask*
5. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
6. **ip route static bfd vlan** *number gateway*
7. **ip route** [**vrf** *vrf-name*] **mask** {*ip-address* | **vlan** *vlan-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
8. **end**
9. **show ip static route**

手順の詳細

	コマンド	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします。
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 vlan number`
	
	Example:
	`Router(config)# interface vlan 100`
		インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	`Router(config-if)# ip address ip-address mask`
	Example:
	`Router(config-if)# ip address 10.0.0.1 255.255.255.0`
		インターフェイスに IP アドレスを設定します。

ステップ 5	`Router(config-if)# bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier`
	Example:
	`Router(config-if)# bfd interval 500 min_rx 500 multiplier 5`
		インターフェイスで BFD をイネーブルにして、BFD セッション パラメータを設定します。

ステップ 6	`Router(config-if)# ip route static bfd vlan vlan-number gateway`
	Example:
	`Router(config-if)# ip route static bfd vlan 100 10.0.10.2`
		BFD ネイバーのスタティック ルートを指定します。

ステップ 7	`Router(config-if)# ip route [vrf vrf-name] prefix mask {ip-address | vlan vlan-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]`
	Example:
	`Router(config-if)# ip route vrf red 10.0.0.0 255.0.0.0 vlan 100 10.0.10.2`
		スタティック ルートを指定します。

ステップ 8	`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、特権 EXEC モードに戻ります。
ステップ 9	`Router# show ip static route`	（任意）ローカル スタティック Routing Information Base（RIB; ルーティング情報ベース）の情報を表示します。

（注）　ソフトウェア バージョンを 15.1(1)S から 15.0(1)S にダウングレードして、BFD over SVI を設定する場合、まず **platform bfd allow-svi** コマンドを 15.1(1)S ソフトウェアで実行してから、ソフトウェアのダウングレードを開始する必要があります。

次の例では、同じ VLAN にあるルータ A および B での BFD over SVI 設定を表示し、設定を確認します。**show bfd neighbors details** コマンドを使用して、BFD セッションが作成されていることを確認します。

```
RouterA# show run
Building configuration...
Current configuration : 119 bytes
interface Vlan100
 ip address 51.1.1.2 255.255.255.0
 no ip redirects
 bfd interval 500 min_rx 500 multiplier 3
end
ip route static bfd Vlan100 51.1.1.1
```

```
ip route 60.1.0.0 255.255.0.0 Vlan100 51.1.1.1

RouterB# show run
Building configuration...
Current configuration : 119 bytes
interface Vlan100
 ip address 51.1.1.1 255.255.255.0
 no ip redirects
 bfd interval 500 min_rx 500 multiplier 3
end
ip route static bfd Vlan100 51.1.1.2
ip route 10.1.0.0 255.255.0.0 Vlan100 51.1.1.2

RouterA# show bfd neighbors details
NeighAddr                         LD/RD    RH/RS     State     Int
51.1.1.1                           1/2     Up        Up        Vl100
Session state is UP and using echo function with 500 ms interval.
OurAddr: 51.1.1.2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3 Received MinRxInt: 1000000, Received
Multiplier: 3 Holddown (hits): 0(0), Hello (hits): 1000(447) Rx Count: 335, Rx Interval
(ms) min/max/avg: 1/533592/2465 last: 24 ms ago Tx Count: 451, Tx Interval (ms)
min/max/avg: 1/26236/4077 last: 628 ms ago Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF IPv4 Static
Uptime: 00:04:43
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 2              - Your Discr.: 1
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 500000

RouterB# show bfd neighbors details
NeighAddr                         LD/RD    RH/RS     State     Int
51.1.1.2                           2/1     Up        Up        Vl100
Session state is UP and using echo function with 500 ms interval.
OurAddr: 51.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3 Received MinRxInt: 1000000, Received
Multiplier: 3 Holddown (hits): 0(0), Hello (hits): 1000(1904) Rx Count: 395, Rx Interval
(ms) min/max/avg: 1/534840/2230 last: 228 ms ago Tx Count: 1908, Tx Interval (ms)
min/max/avg: 1/28616/1210 last: 268 ms ago Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF IPv4 Static
Uptime: 00:05:39
Last packet: Version: 1                - Diagnostic: 0
             State bit: Up             - Demand bit: 0
             Poll bit: 0               - Final bit: 0
             Multiplier: 3             - Length: 24
             My Discr.: 1              - Your Discr.: 2
             Min tx interval: 1000000  - Min rx interval: 1000000
             Min Echo interval: 500000
```

CHAPTER 59

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。

（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 7600 Series Routers Command References』を参照してください。

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.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」（P.59-1）
- 「使用上のガイドライン」（P.59-1）
- 「レイヤ 2 Traceroute ユーティリティの使用」（P.59-2）

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、送信元デバイスから宛先デバイスまでのパケットの経路を表すレイヤ 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 アドレスだけをサポートします。このユーティリティは、パス上の各ルータが持つ MAC 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 をサポートしないデバイス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、送信元デバイスから宛先デバイスまでのパスだけです。パケットが送信元ホストから送信元デバイスに到達するパスや、宛先デバイスから宛先ホストへのパスは識別できません。

使用上のガイドライン

レイヤ 2 Traceroute ユーティリティを使用する場合、次の注意事項に従ってください。

- Cisco Discovery Protocol（CDP）がネットワーク上のすべてのデバイスでイネーブルでなければなりません。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デバイスが CDP に対してトランスペアレントであると、レイヤ 2 Traceroute ユーティリティはパス上でこのデバイスを識別できません。

- **ping** 特権 EXEC コマンドを使用して接続をテストできれば、このルータは別のルータから到達可能であると定義できます。レイヤ 2 パス内のすべてのデバイスは、互いに到達可能である必要があります。
- パス内で識別される最大ホップ カウントは 10 です。
- 送信元デバイスから宛先デバイスまでのレイヤ 2 パス上にないルータでは、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを入力できます。パス内のすべてのデバイスは、このルータから到達可能である必要があります。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。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。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定すると、レイヤ 2 Traceroute ユーティリティはアドレス解決プロトコル（ARP）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。
- 複数のデバイスがハブを介して 1 つのポートに接続されている場合は（1 つのポート上で複数の CDP ネイバー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デバイスから宛先デバイスまでのレイヤ 2 パスを表示するには、特権 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。

次の例は、**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#
```

CHAPTER 60

Call Home の設定

この章では、Cisco IOS ソフトウェア リリース 12.2SX で Call Home 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 7600 Series Router Cisco IOS Command Reference*』を参照してください。
http://www.cisco.com/en/US/products/ps6922/prod_command_reference_list.html

この章は、次の内容で構成されています。

- 「Call Home の概要」（P.60-1）
- 「Call Home の設定」（P.60-2）
- 「Call Home 設定情報の表示」（P.60-14）
- 「デフォルト設定値」（P.60-18）
- 「アラート グループの起動イベントとコマンド」（P.60-18）
- 「メッセージの内容」（P.60-24）

Call Home の概要

Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な使用方法には、ネットワーク サポート技術者の直接ページング、ネットワーク オペレーション センターへの E メール通知、サポート Web サイトへの XML の送信、シスコのテクニカル サポート（TAC）での直接の事例生成のための Cisco Smart Call Home サービスの使用などがあります。

Call Home 機能では、設定、診断、環境条件、コンポーネント、システム イベントについての情報を含むアラート メッセージを送信できます。

Call Home 機能では、*Call Home 宛先プロファイル*に従って複数の受信者にアラートを送信できます。宛先プロファイルには、メッセージ形式とコンテンツのカテゴリを設定できます。定義済みの宛先プロファイルは、シスコ TAC にアラートを送信するためのもので、独自の宛先プロファイルを定義することもできます。

柔軟なメッセージ送信オプションと形式オプションにより、特定のサポート要件に簡単に統合できます。

Call Home 機能には、次の利点があります。

- 複数のメッセージ形式オプション
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - プレーン テキスト：人間による読み取りに適したように完全に形式化されたメッセージ情報。
  - XML：Extensible Markup Language（XML）および Adaptive Markup Language（AML）文書型定義（DTD）を使用した読み取り可能なマッチング形式。XML 形式では、シスコ TAC と通信できます。
- 複数のメッセージ宛先への同時配信が可能。
- 設定、診断、環境条件、コンポーネント、Syslog イベントを含む複数のメッセージ カテゴリ。
- 重大度とパターン マッチングによるメッセージのフィルタリング。
- 定期的なメッセージ送信のスケジューリング。

Smart Call Home の取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービス用にデバイスを登録できます。Smart Call Home では、お使いのデバイスから送信された Call Home メッセージを分析し、背景説明と推奨事項を提供することによって、システムの問題をすばやく解決できます。既知と特定できる問題、特に GOLD 診断エラーについては、シスコ TAC によって自動サービス リクエストが生成されます。

Smart Call Home には、次の機能があります。

- 連続的なデバイスのヘルス モニタリングとリアルタイム診断アラート。
- 問題解決を迅速に行うための詳細な診断情報を含む、適切な TAC チームに転送された、お使いのデバイスからの Call Home メッセージの分析および自動サービス リクエストの生成（該当する場合）。
- お使いのデバイスから直接、またはダウンロード可能な転送ゲートウェイ（TG）集約ポイントを介して転送されたメッセージのセキュリティ保護。複数のデバイスをサポートする必要のある場合や、セキュリティ要件によってデバイスがインターネットに直接接続されないことが必要とされる場合は、TG 集約ポイントを使用できます。
- Call Home メッセージと推奨事項､すべての Call Home デバイスのコンポーネントと設定情報への Web アクセス。関連付けられたフィールド通告、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

次の項目を登録する必要があります。

- ルータの SMARTnet 契約番号。
- 電子メール アドレス
- Cisco.com ID

Smart Call Home の詳細については、次の URL の Smart Call Home ページを参照してください。

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

Call Home の設定

Call Home の設定方法は、機能の使用目的によって異なります。Call Home を設定する前に、以下を含むいくつかの情報を考慮する必要があります。

- 少なくとも 1 つの宛先プロファイル（定義済みまたはユーザ定義）を設定する必要があります。使用する宛先プロファイルは、受信エンティティがポケットベル、電子メール、Cisco Smart Call Home のような自動サービスのいずれであるかによって異なります。
  - 宛先プロファイルが E メール メッセージ送信を使用している場合、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サーバを指定する必要があります。
  - 宛先プロファイルが Secure HTTP（HTTPS; セキュア HTTP）メッセージ転送を使用している場合は、トラストポイント Certificate Authority（CA; 認証局）を設定する必要があります。
- 受信者が受信したメッセージの発信源を特定できるように、連絡用 E メール、電話番号、住所の情報を設定する必要があります。
- ルータには、E メール サーバまたは宛先 HTTP サーバへの IP 接続が必要です。
- Cisco Smart Call Home を使用している場合、アクティブなサービス契約が設定するデバイスを対象としている必要があります。

Call Home を設定する手順は、次のとおりです。

ステップ 1　設定場所の連絡先情報を設定します。

ステップ 2　各受信者の宛先プロファイルを設定します。

ステップ 3　各宛先プロファイルを 1 つまたは複数のアラート グループに登録し、アラート オプションを設定します。

ステップ 4　転送方法に応じて（CA 証明書を含め）E メール設定または HTTPS 設定を行います。

ステップ 5　Call Home 機能をイネーブルにします。

ステップ 6　Call Home メッセージをテストします。

ヒント　Smart Call Home Web アプリケーションから、基本的な設定スクリプトをダウンロードして、Smart Call Home およびシスコ TAC とともに使用するよう Call Home 機能を設定するために利用できます。このスクリプトは、Smart Call Home サービスとセキュアな通信を行うために、トラストポイント CA を設定する際にも有用です。スクリプトは、そのままの形で提供され、次の URL からダウンロードできます。http://www.cisco.com/go/smartcall/

連絡先情報の設定

ルータには必ず連絡用の E メール アドレスが必要です。任意で、電話番号、住所、契約 ID、カスタマー ID、サイト ID を割り当てることができます。

連絡先情報を割り当てるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コ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)# call-home`	Call Home コンフィギュレーション サブモードに入ります。
ステップ 3	`Router(cfg-call-home)# contact-email-addr` *email-address*	カスタマーの 電子メール アドレスを割り当てます。E メール アドレス フォーマットにはスペースなしで最大 200 文字まで入力できます。

	コマンド	目的
ステップ 4	`Router(cfg-call-home)# phone-number +phone-number`	（任意）顧客の電話番号を割り当てます。 **（注）** 番号はプラス（+）記号で始まり、ダッシュ（-）と数字だけが含まれるようにしてください。最大 16 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
ステップ 5	`Router(cfg-call-home)# street-address street-address`	（任意）RMA 機器の配送先である顧客の住所を割り当てます。最大 200 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
ステップ 6	`Router(cfg-call-home)# customer-id text`	（任意）カスタマー ID を指定します。最大 64 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
ステップ 7	`Router(cfg-call-home)# site-id text`	（任意）カスタマーのサイト ID を指定します。最大 200 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
ステップ 8	`Router(cfg-call-home)# contract-id text`	（任意）ルータの顧客の契約 ID を指定します。最大 64 文字まで入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。

次に、連絡先情報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)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
Router(config)#
```

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な送信情報が含まれています。少なくとも 1 つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。

定義済みの宛先プロファイルを使用することも、目的のプロファイルを定義することもできます。新しい宛先プロファイルを定義する場合は、プロファイル名を割り当てる必要があります。

（注） Cisco Smart Call Home サービスを使用する場合、宛先プロファイルは XML メッセージ形式を使用する必要があります。

宛先プロファイルには、次の属性を設定できます。

- プロファイル名：ユーザ定義宛先プロファイルを一意に識別する文字列。プロファイル名は 31 文字までで大文字と小文字は区別されません。プロファイル名として **all** は使用できません。
- 転送方法：アラートを送信するための転送メカニズム（E メールまたは HTTP（HTTPS を含む））。
  - ユーザ定義の宛先プロファイルの場合、E メールがデフォルトで、どちらかまたは両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、E メールがイネーブルになります。
  - 定義済みのシスコ TAC プロファイルの場合、どちらかの転送方法をイネーブルにできますが、両方をイネーブルにはできません。
- 宛先アドレス：アラートを送信する転送方法に関連した実際のアドレス。
- メッセージ形式：アラートの送信に使用するメッセージ形式。
  - ユーザ定義宛先プロファイルの形式オプションは、ロング テキスト、ショート テキスト、または XML です。デフォルトは XML です。
  - 定義済みのシスコ TAC プロファイルの場合、XML しか使用できません。
- メッセージ サイズ：宛先メッセージの最大サイズ。有効な範囲は、50 ～ 3,145,728 バイトで、デフォルトは 3,145,728 バイトです。

宛先プロファイルを作成して設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コ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)# call-home`	Call Home コンフィギュレーション サブモードに入ります。
ステップ 3	`Router(cfg-call-home)# profile name`	指定された宛先プロファイルに対する Call Home 宛先プロファイル コンフィギュレーション サブモードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
	`Router(cfg-call-home)# no profile name`	指名ユーザ定義宛先プロファイルを削除します。
	`Router(cfg-call-home)# no profile all`	すべてのユーザ定義宛先プロファイルを削除します。
ステップ 4	`Router(cfg-call-home-profile)# [no] destination transport-method {email | http}`	（任意）メッセージ転送方法をイネーブルにします。**no** オプションを選択すると、方法がディセーブルになります。
ステップ 5	`Router(cfg-call-home-profile)# destination address {email email-address | http url}`	Call Home メッセージが送信される宛先 E メール アドレスまたは URL を設定します。 **（注）** 宛先 URL を入力する場合は、サーバがセキュア サーバであるかどうかに応じて **http://** または **https://** を指定します。宛先がセキュア サーバである場合、トラストポイント CA も設定する必要があります。
ステップ 6	`Router(cfg-call-home-profile)# destination preferred-msg-format {long-text | short-text | xml}`	（任意）使用するメッセージ形式を設定します。デフォルトは XML です。
ステップ 7	`Router(cfg-call-home-profile)# destination message-size bytes`	（任意）宛先プロファイルの宛先メッセージの最大サイズを設定します。

	コマンド	目的
ステップ 8	`Router(cfg-call-home-profile)#` **`active`**	宛先プロファイルをイネーブルにします。デフォルトでは、プロファイルは作成時にイネーブルになります。
	`Router(cfg-call-home-profile)#` **`no active`**	宛先プロファイルをディセーブルにします。
ステップ 9	`Router(cfg-call-home-profile)#` **`exit`**	Call Home 宛先プロファイル コンフィギュレーション サブモードを終了して、Call Home コンフィギュレーション サブモードに戻ります。
ステップ 10	`Router(cfg-call-home)#` **`end`**	特権 EXEC モードに戻ります。
ステップ 11	`Router#` **`show call-home profile`** {*name* | **`all`**}	指定されたプロファイルまたはすべての設定されたプロファイルに対する宛先プロファイル設定を表示します。

宛先プロファイルのコピー

既存のプロファイルをコピーして新しい宛先プロファイルを作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router#` **`configure terminal`**	コ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)#` **`call-home`**	Call Home コンフィギュレーション サブモードに入ります。
ステップ 3	`Router(cfg-call-home)#` **`copy profile`** *`source-profile target-profile`*	既存の宛先プロファイルと同じ設定で新しい宛先プロファイルを作成します。

アラート グループへの登録

アラート グループは、すべてのルータでサポートされる Call Home アラートの定義済みのサブセットです。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。次のアラート グループが使用できます。

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog

各アラート グループの起動イベントは「アラート グループの起動イベントとコマンド」（P.60-18）に示しています。アラート グループ メッセージの内容は「メッセージの内容」（P.60-24）に示しています。

宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

（注）　Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。さらに、アラート グループをイネーブルにする必要があります。

宛先プロファイルをアラート グループに登録するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コ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)# call-home`	Call Home 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 3	`Router(cfg-call-home)# alert-group {all|configuration|diagnostic|environment|inventory|syslog}`	指定されたアラート グループをイネーブルにします。すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。
	`Router(cfg-call-home)# no alert-group {all|configuration|diagnostic|environment|inventory|syslog}`	指定されたアラート グループをディセーブルにします。すべてのアラート グループをディセーブルにするには、**all** キーワードを使用します。
ステップ 4	`Router(cfg-call-home)# profile name`	指定された宛先プロファイルに対する Call Home 宛先プロファイル 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 5	`Router(cfg-call-home-profile)# subscribe-to-alert-group configuration [periodic {daily hh:mm | monthly date hh:mm | weekly day hh:mm}]`	この宛先プロファイルを Configuration アラート グループに登録します。Configuration アラート グループは、「定期的な通知の設定」（P.60-8）で説明しているように、定期的な通知用に設定できます。
	`Router(cfg-call-home-profile)# subscribe-to-alert-group all`	使用可能なすべてのアラート グループに登録します。
	`Router(cfg-call-home-profile)# no subscribe-to-alert-group {all|configuration|diagnostic|environment|inventory|syslog}`	指定されたアラート グループへの登録を解除します。すべてのアラート グループへの登録を解除するには、**all** キーワードを使用します。
ステップ 6	`Router(cfg-call-home-profile)# subscribe-to-alert-group diagnostic [severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging]`	この宛先プロファイルを Diagnostic アラート グループに登録します。Diagnostic アラート グループは、「メッセージ重大度しきい値の設定」（P.60-8）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。
ステップ 7	`Router(cfg-call-home-profile)# subscribe-to-alert-group environment [severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging]`	この宛先プロファイルを Environment アラート グループに登録します。Environment アラート グループは、「メッセージ重大度しきい値の設定」（P.60-8）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。
ステップ 8	`Router(cfg-call-home-profile)# subscribe-to-alert-group inventory [periodic {daily hh:mm | monthly date hh:mm | weekly day hh:mm}]`	この宛先プロファイルを Inventory アラート グループに登録します。Inventory アラート グループは、「定期的な通知の設定」（P.60-8）で説明しているように、定期的な通知用に設定できます。

	コマンド	目的
ステップ 9	`Router(cfg-call-home-profile)#` **`subscribe-to-alert-group syslog [severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging] [pattern`** *`string`*`]`	この宛先プロファイルを Syslog アラート グループに登録します。Syslog アラート グループは、「メッセージ重大度しきい値の設定」（P.60-8）で説明しているように、重大度に応じてメッセージをフィルタするよう設定できます。syslog メッセージで一致するパターンを指定できます。パターンにスペースが含まれている場合は、引用符（""）で囲む必要があります。
ステップ 10	`Router(cfg-call-home-profile)#` **`exit`**	Call Home 宛先プロファイル コンフィギュレーション サブモードを終了します。

定期的な通知の設定

Configuration または Inventory アラート グループに宛先プロファイルを登録すると、指定した期間に定期的にまたは非同期にアラート グループ メッセージを受信するよう選択できます。送信期間は、次のいずれかにできます。

- 毎日：24 時間の時間:分形式 *hh:mm*（例：14:30）で送信する時刻を指定します。
- 毎週：*day hh:mm* という形式で曜日と時刻を指定します。ここで、day は曜日をスペルアウトします（例：monday）。
- 毎月：*date hh:mm* という形式で 1 ～ 31 の日と時刻を指定します。

メッセージ重大度しきい値の設定

宛先プロファイルを Diagnostic、Environment、または Syslog アラート グループに登録すると、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

重大度しきい値は、表 60-1 のキーワードと、catastrophic（レベル 9、最高レベルの緊急性）から debugging（レベル 0、最低レベルの緊急性）までの範囲を使用して設定します。重大度しきい値が設定されていない場合、デフォルトは normal（レベル 1）です。

（注） Call Home の重大度は、システム メッセージ ロギングの重大度とは異なります。

表 60-1　重大度と Syslog レベルのマッピング

レベル	キーワード	Syslog レベル	説明
9	**catastrophic**	該当なし	ネットワーク全体に及ぶ深刻な障害。
8	**disaster**	該当なし	ネットワークへの重大な影響。
7	**fatal**	緊急（Emergency）（0）	システムは使用不能。
6	**critical**	アラート（Alert）（1）	クリティカルな状態、ただちに注意が必要です。
5	**major**	クリティカル（Critical）（2）	メジャー状態です。

表 60-1　重大度と Syslog レベルのマッピング （続き）

レベル	キーワード	Syslog レベル	説明
4	**minor**	エラー（Error）（3）	マイナーな状態。
3	**warning**	警告（Warning）（4）	警告状態。
2	**notification**	通知（Notice）（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	**normal**	情報（Information）（6）	標準状態に戻ることを示す標準イベントです。
0	**debugging**	デバッグ（Debug）（7）	デバッグ メッセージ。

Syslog パターンマッチの設定

宛先プロファイルを Syslog アラート グループに登録すると、各 syslog メッセージ内で一致するテキスト パターンを任意で指定できます。パターンを設定すると、指定されたパターンが含まれ、重大度しきい値に一致する場合にだけ Syslog アラート グループ メッセージが送信されます。パターンにスペースが入っている場合、設定時にそのパターンを引用符（""）で囲む必要があります。宛先プロファイルごとにパターンを 5 つまで指定できます。

一般的な E メール オプションの設定

電子メール メッセージ転送サービスを使用するには、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）の電子メール サーバ アドレスを少なくとも 1 つ設定する必要があります。次のオプションを設定可能です。

- 送信元および返信先の電子メール アドレスと、最大 4 つのバックアップ電子メール サーバ。
- 電子メール メッセージまたは HTTP メッセージにレート制限を設定し、VPN Routing or Forwarding（VRF; VPN ルーティング/転送）インスタンス名を指定して Call Home 電子メール メッセージを送信できます。
- 電子メール メッセージを送信する **vrf** または **source-interface**（または **source-ip-address**）。上記のオプションを設定して http（s）メッセージを送信するには、グローバル コンフィギュレーション モードで **http client source-interface** *interface-name* コマンドを使用します。このとき、設定対象の VRF に **source-interface** を関連付けることができます。

一般的な電子メール オプションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コ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)# call-home`	Call Home コンフィギュレーション サブモードを開始します。

	コマンド	目的
ステップ 3	`Router(cfg-call-home)# mail-server {ipv4-address | name} priority number`	E メール サーバ アドレスを割り当て、設定済みの E メール サーバ内の相対的なプライオリティを割り当てます。 次のどちらかを指定します。 • 電子メール サーバの IP アドレスまたは • 電子メール サーバの 64 文字以下の完全修飾ドメイン名（FQDN） 1（最高のプライオリティ）から 100（最低のプライオリティ）のプライオリティ番号を割り当てます。
	`Router(cfg-call-home)# no mail-server {ipv4-address | name | all}`	1 つまたはすべての E メール サーバを設定から削除します。
ステップ 4	`Router(cfg-call-home)# sender from email-address`	（任意）Call Home E メール メッセージの [from] フィールドに表示される E メール アドレスを割り当てます。アドレスが指定されていない場合は、連絡用の E メール アドレスが使用されます。
ステップ 5	`Router(cfg-call-home)# sender reply-to email-address`	（任意）Call Home E メール メッセージの [reply-to] フィールドに表示される E メール アドレスを割り当てます。
ステップ 6	`Router(cfg-call-home)# rate-limit number`	（任意）1 分間に送信するメッセージ数の上限を指定します（1 ～ 60）。デフォルトは 20 です。
ステップ 7	`Router(cfg-call-home)# vrf name`	（任意）Call Home 電子メール メッセージを送信する VRF インスタンスを指定します。VRF を指定しなければ、グローバル ルーティング テーブルが使用されます。
ステップ 8	`Router(cfg-call-home)# source-interface interface-name`	（任意）Call Home 電子メール メッセージの宛先となる送信元インターフェイスを指定します。送信元インターフェイスまたは IP アドレスを指定しなければ、ルーティング テーブルのインターフェイスが使用されます。
ステップ 9	`Router(cfg-call-home)# sourcee-ip-address ip-address`	（任意）Call Home 電子メール メッセージの宛先となる送信元 IP アドレスを指定します。 **（注）** 送信元インターフェイスと IP アドレスを同時に指定しないでください。送信元インターフェイス名または IP アドレスのいずれかを指定します。

一般的な E メール オプションの設定時には、次の注意が適用されます。

- バックアップ E メール サーバは、異なるプライオリティ番号を使用して、**mail-server** コマンドを繰り返すと定義できます。
- **mail-server priority** *number* パラメータは 1 ～ 100 に設定できます。プライオリティの最も高い（プライオリティ番号が最小の）サーバが最初に試行されます。

次に、プライマリ E メール サーバとセカンダリ E メール サーバを含む、一般的な E メール パラメータの設定例を示します。

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.168.0.1 priority 2
Router(cfg-call-home)# sender from username@example.com
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# exit
Router(config)#
```

Call Home のイネーブル化

Call Home 機能をイネーブルまたは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# configure terminal`	コ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)# service call-home`	Call Home 機能をイネーブルにします。
	`Router(config)# no service call-home`	Call Home 機能をディセーブルにします。

Call Home の通信のテスト

2 種類のコマンドを使用して、手動でメッセージを送信することで Call Home の通信をテストできます。ユーザ定義の Call Home テスト メッセージを送信するには、**call-home test** コマンドを使用します。特定のアラート グループ メッセージを送信するには、**call-home send** コマンドを使用します。

Call Home テスト メッセージの手動送信

Call Home テスト メッセージを手動で送信するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# call-home test [“test-message”] profile name`	指定された宛先プロファイルにテスト メッセージを送信します。ユーザ定義のテスト メッセージ テキストは任意ですが、スペースが含まれる場合は、引用符 ("") で囲む必要があります。ユーザ定義のメッセージが設定されていない場合、デフォルト メッセージが送信されます。

Call Home アラート グループ メッセージの手動送信

Call Home アラート グループ メッセージを手動で起動するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# call-home send alert-group configuration [profile name]`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Configuration アラート グループ メッセージを送信します。
	`Router# call-home send alert-group diagnostic {module number | slot/subslot | slot/bay_number} [profile name]`	設定された宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Diagnostic アラート グループ メッセージを送信します。診断情報が送信されるモジュールまたはポートを指定する必要があります。
	`Router# call-home send alert-group inventory [profile name]`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Inventory アラート グループ メッセージを送信します。

Call Home アラート グループ メッセージを手動で送信する場合は、次の点に注意してください。

- 手動で送信できるのは、Configuration、Diagnostic、または Inventory アラート グループだけです。
- Configuration、Diagnostic、または Inventory アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定すると、プロファイルのアクティブ ステータス、登録ステータス、または重大度設定に関係なくメッセージが宛先プロファイルに送信されます。
- Configuration または Inventory アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定しないと、normal または指定されたアラート グループへの定期的な登録に指定されたアクティブなプロファイルすべてにメッセージが送信されます。
- Diagnostic アラート グループ メッセージを手動で起動し、宛先プロファイル名を指定しないと、コマンドによって次の動作が行われます。
  - 重大度が minor より下の診断イベントに登録されたアクティブなプロファイルの場合、モジュールまたはインターフェイスが診断イベントを遵守しているかどうかに関係なくメッセージが送信されます。
  - 重大度が minor 以上の診断イベントに登録されたアクティブなプロファイルの場合、指定されたモジュールまたはインターフェイスが、少なくとも登録された重大度の診断イベントを遵守している場合にだけメッセージが送信されます。遵守していない場合、診断メッセージは宛先プロファイルに送信されません。

分析およびレポート要求の送信

call-home request コマンドを使用して、システム情報を送信し、セキュリティ アラート、既知のバグ、ベスト プラクティス、コマンド リファレンスなどの情報を受信することができます。

Cisco Output Interpreter（COI）ツールからレポートおよび分析情報を要求するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router# call-home request output-analysis "show-command" [profile name] [ccoid user-id]`	分析用として指定した show コマンドの出力を送信します。show コマンドは、引用符（""）で囲む必要があります。
ステップ 1	`Router# call-home request {config-sanity | bugs-list | command-reference | product-advisory} [profile name] [ccoid user-id]`	分析のため、**show running-config all**、**show version**、および **show module**（**standalone**）コマンドなど所定のコマンド セットの出力を送信します。要求するレポート タイプを指定します。

Call Home レポートおよび分析要求を手動で送信する場合は、次の注意事項に従ってください。

- **profile** *name* を指定すると、要求はプロファイルに送信され、それ以外の場合は Cisco TAC プロファイルに送信されます。**call-home request** の受信者プロファイルを有効にする必要はありません。受信者プロファイルは、転送ゲートウェイが設定されている電子メール アドレスを指定するようにプログラムされているので、要求メッセージは Cisco TAC へ転送され、ユーザは Smart Call Home サービスからの返信を受け取ることができます。
- **ccoid** *user-id* は、Smart Call Home ユーザの登録 ID です。ユーザ ID を指定すると、応答は登録ユーザの電子メール アドレスに送信され、それ以外の場合はデバイスの連絡先電子メール アドレスに送信されます。
- 要求するレポート タイプを指定するキーワードに基づいて、以下の情報が返送されます。
  - **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティスの情報。
  - **bugs-list**：実行中のバージョンおよび現在設定されている機能の既知のバグ。
  - **command-reference**：実行コンフィギュレーションに含まれるすべてのコマンドへの参照リンク。
  - **product-advisory**：ネットワークのデバイスに影響する可能性のある Product Security Incident Response Team（PSIRT）通知、End of Life（EOL）または End of Sales（EOS）通知、あるいは Field Notice（FN）。

次に、ユーザが指定した show コマンドの分析を要求する例を示します。

```
Router# call-home request output-analysis "show diagnostic result module all" profile TG
```

Smart Call Home の設定とイネーブル化

Cisco Smart Call Home サービスの適用と設定の情報については、次の URL の『*Smart Call Home User Guide*』の「FastStart」の項を参照してください。

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

ユーザ ガイドには、デバイスから直接、または転送ゲートウェイ（TG）集約ポイントを介して Smart Call Home メッセージを送信するための設定例が記載されています。複数のデバイスをサポートする必要のある場合や、セキュリティ要件によってデバイスがインターネットに直接接続されないことが必要とされる場合は、TG 集約ポイントを使用できます。

Smart Call Home サービスは転送方法として HTTPS を使用するため、『*Smart Call Home User Guide*』で説明されているように CA をトラストポイントとして設定する必要もあります。

Call Home 設定情報の表示

設定済みの Call Home 情報を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **show call-home**	Call Home 設定の概要を表示します。
	Router# **show call-home detail**	Call Home 設定の詳細を表示します。
	Router# **show call-home alert-group**	使用可能なアラート グループとそれらのステータスを表示します。
	Router# **show call-home mail-server status**	設定済みの E メール サーバのアベイラビリティをチェックして表示します。
	Router# **show call-home profile** {**all** | *name*}	指定された宛先プロファイルの設定を表示します。**all** キーワードを使用してすべての宛先プロファイルの設定を表示します。
	Router# **show call-home statistics**	Call Home イベントの統計情報を表示します。

例 60-2 から 60-8 は、**show call-home** コマンドの異なるオプションを使用した場合の結果を示しています。

例 60-1　　設定済みの Call Home 情報

```
Router# show call-home
Current call home settings:
    call home feature : disable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara
    source ip address: Not yet set up
    source interface: Not yet set up
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 message(s) per minute

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Disable configuration info
    diagnostic               Disable diagnostic info
    environment              Disable environmental info
    inventory                Enable  inventory info
    syslog                   Disable syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
```

```
Router#
```

例 60-2　設定済みの Call Home 情報の詳細

```
Router# show call-home detail
Current call home settings:
    call home feature : disable
    call home message's from address: switch@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara
    source ip address: Not yet set up
    source interface: Not yet set up
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 message(s) per minute

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Disable configuration info
    diagnostic               Disable diagnostic info
    environment              Disable environmental info
    inventory                Enable  inventory info
    syslog                   Disable syslog info

Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group              Severity
    ------------------------ ------------
    inventory                normal

    Syslog-Pattern           Severity
    ------------------------ ------------
    N/A                      N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 1 day of the month at
 09:27
```

```
    Periodic inventory info message is scheduled every 1 day of the month at 09:
12

    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Router#
```

例 60-3　使用可能な Call Home アラート グループ

```
Router# show call-home alert-group
Available alert groups:
    Keyword                   State   Description
    ------------------------ ------- --------------------------------
    configuration             Disable configuration info
    diagnostic                Disable diagnostic info
    environment               Disable environmental info
    inventory                 Enable  inventory info
    syslog                    Disable syslog info

Router#
```

例 60-4　E メール サーバのステータス情報

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...

Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]

Router#
```

例 60-5　すべての宛先プロファイルの情報（定義済みおよびユーザ定義）

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
```

```
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 1 day of the month at 09:27

    Periodic inventory info message is scheduled every 1 day of the month at 09:12

    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Router#
```

例 60-6　ユーザ定義宛先プロファイルの情報

```
Router# show call-home profile campus-noc

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Router#
```

例 60-7　Call Home の統計情報

```
Router# show call-home statistics
Message Types Total Email HTTP
------------- -------------------- -------------------- ------------------
Total Success 13 13 0
Config 1 1 0
Diagnostic 0 0 0
Environment 0 0 0
Inventory 10 10 0
SysLog 1 1 0
Test 0 0 0
Request 0 0 0
Send-CLI 1 1 0

Total In-Queue 0 0 0
Config 0 0 0
Diagnostic 0 0 0
Environment 0 0 0
Inventory 0 0 0
```

```
SysLog 0 0 0
Test 0 0 0
Request 0 0 0
Send-CLI 0 0 0

Total Failed 0 0 0
Config 0 0 0
Diagnostic 0 0 0
Environment 0 0 0
Inventory 0 0 0
SysLog 0 0 0
Test 0 0 0
Request 0 0 0
Send-CLI 0 0 0

Total Ratelimit
-dropped 0 0 0
Config 0 0 0
Diagnostic 0 0 0
Environment 0 0 0
Inventory 0 0 0
SysLog 0 0 0
Test 0 0 0
Request 0 0 0
Send-CLI 0 0 0
```

デフォルト設定値

表 60-2 は Call Home のデフォルト設定を示しています。

表 60-2　Call Home のデフォルト設定

パラメータ	デフォルト
Call Home 機能のステータス	ディセーブル
ユーザ定義プロファイルのステータス	アクティブ
定義済みのシスコ TAC プロファイルのステータス	非アクティブ
転送方法	電子メール
メッセージのフォーマット タイプ	XML
ロング テキスト、ショート テキスト、または XML 形式で送信されるメッセージの宛先メッセージのサイズ	3,145,728
アラート グループのステータス	イネーブル
Call Home メッセージの重大度しきい値	1（normal）
1 分間に送信するメッセージのレート制限	20

アラート グループの起動イベントとコマンド

Call Home 起動イベントはアラート グループにグループ化され、各アラート グループにはイベントの発生時に実行するよう CLI コマンドが割り当てられます。CLI コマンド出力は転送されるメッセージに含まれます。表 60-3 に、各アラート グループに含まれる起動イベントを示します。これには、各イベントの重大度と実行されるアラート グループの CLI コマンドも含まれます。

表 60-3　Call Home アラート グループ、イベント、および動作

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
Syslog				syslog にログ記録されるイベント （syslog レベル 0、1、または 2 の場合だけ、TAC に送信）。 実行される CLI コマンド **show logging**
	SYSLOG	LOG_EMERG	0	システムは使用不能。
	SYSLOG	LOG_ALERT	1	即時対処が必要。
	SYSLOG	LOG_CRIT	2	クリティカルな状態。
	SYSLOG	LOG_ERR	3	エラー状態。
	SYSLOG	LOG_WARNING	4	警告状態。
	SYSLOG	LOG_NOTICE	5	正常だが重大な状態。
	SYSLOG	LOG_INFO	6	情報。
	SYSLOG	LOG_DEBUG	7	デバッグレベル メッセージ。
	SYSLOG	C2PLUSWITHNODB	2	スロット %d のモジュールにはフォワーディング ドーター ボードがない。電力が供給できない。
	SYSLOG	DFCMISMATCH	2	モジュール %d DFC はスーパーバイザ エンジン DFC と互換性がない。電力が供給できない。
	SYSLOG	BADFLOWCTRL	2	モジュール %d は DFC をサポートするのに適切なハードウェア リビジョン レベルではない。電力が供給できない。
	SYSLOG	BADFLOWCTRL_WARN	2	警告：モジュール %d は DFC3 をサポートするのに適切なハードウェア リビジョン レベルではない。
	SYSLOG	BADPINN1	2	モジュール %d は PFC3 システムと共存するのに適切なハードウェア リビジョン レベルではない。電力が供給できない。
	SYSLOG	FANUPGREQ	2	ファンをアップグレードしなければ、モジュール %d はサポートされない。
	SYSLOG	INSUFFCOO	4	モジュール %d は適切に冷却できない。
	SYSLOG	PROVISION	6	モジュール %d はプロビジョニング要件を満たしていない。電力が供給できない。
	SYSLOG	PWRFAILURE	6	電源コンバータの障害により、モジュール %d はディセーブルになる。
	SYSLOG	LC_FAILURE	3	モジュール %d には重大なオンライン診断障害、%s がある。
	SYSLOG	HARD_RESET	3	スイッチオーバー エラー回復の一環としてモジュール %d はハード リセットされる。
	SYSLOG	SOFT_RESET	3	スイッチオーバー エラー回復の一環としてモジュール %d はソフト リセットされる。
		DOWNGRADE	6	ファブリック対応モジュール %d は適切なハードウェア リビジョン レベルではなく、フロー スルー モードでしか実行できない。

表 60-3　Call Home アラート グループ、イベント、および動作 （続き）

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
環境				電源、ファン、温度アラームのような環境感知要素に関連するイベント （TAC に送信）。 実行される CLI コマンド **show environment** **show logging** **show module** **show power**
	FAN_FAILURE	FANPSINCOMPAT	4	ファン トレイと電源モジュール %d に互換性がない。
		ALARMCLR	4	指定されたアラーム条件がクリアされ、シャットダウンがキャンセルされた。
	FAN_FAILURE	FANHIOUTPUT	4	バージョン %d 高出力ファン トレイが有効である。
	FAN_FAILURE	FANLOOUTPUT	4	バージョン %d 低出力ファン トレイが有効である。
	FAN_FAILURE	FANVERCHK	4	挿入されている電源モジュール %d はバージョン %d ファン トレイとだけ互換性がある。
	FAN_FAILURE	FANTRAYFAILED	4	ファン トレイに障害が発生した。
	FAN_FAILURE	FANTRAYOK	4	ファン トレイは正常である。
	FAN_FAILURE	FANCOUNTFAILED	4	必要な数のファン トレイがない。
	FAN_FAILURE	FANCOUNTOK	4	必要な数のファン トレイがある。
	FAN_FAILURE	PSFANFAIL	4	電源モジュールのファンに障害が発生した。
	FAN_FAILURE	PSFANOK	4	電源モジュールのファンは正常である。
	TEMPERATURE_ALARM	MAJORTEMPALARM	2	可能な動作温度範囲を超えている。
		MAJORTEMPALARM RECOVER	4	可能な動作温度範囲に戻った。
	TEMPERATURE_ALARM	MINORTEMPALARM	4	正常な動作温度範囲を超えている。
		MINORTEMPALARM RECOVER	4	正常な動作温度範囲に戻った。
	VTT_FAILED	VTTFAILED	4	VTT %d に障害が発生した。
		VTTOK	4	VTT %d は動作可能である。
	VTT_FAILED	VTTMAJFAILED	0	システムの動作を続行するには VTT の障害が多すぎる。

表 60-3　Call Home アラート グループ、イベント、および動作 （続き）

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
		VTTMAJ RECOVERED	2	システムの動作を続行するために十分な VTT が動作している。
	CLOCK_FAILED	CLOCKFAILED	4	クロックに障害が発生した。
		CLOCKOK	4	クロックは動作可能である。
	CLOCK_FAILED	CLOCKMAJFAILED	0	システムの動作を続行するにはクロックの障害が多すぎる。
		CLOCKMAJRECOVERED	2	システムの動作を続行するために十分なクロックが動作している。
		SHUTDOWN-SCHEDULED	2	%d 秒以内に %s のシャットダウンがスケジュールされている。
		SHUTDOWN_NOT_SCHEDULED	2	%s の重大なセンサー アラームは無視され、%s はシャット ダウンされない。
		SHUTDOWN-CANCELLED	2	シャットダウンはキャンセルされた。
		SHUTDOWN	2	%s により %s をただちにシャットダウンする。
		SHUTDOWN-DISABLED	1	%s をシャット ダウンする必要があるが、シャットダウン処理がディセーブルになっている。
		RESET_SCHEDULED	2	数秒内にシステムのリセットがスケジュールされている。
		CLOCK_SWITCHOVER	2	システム スイッチング クロックの変更。
		CLOCK_A_MISSING	4	システム内でクロック A が検出できない。
		CLOCK_B_MISSING	4	システム内でクロック B が検出できない。
		USE_RED_CLOCK	4	システムは冗長クロック（クロック B）を使用している。
		ENABLED	4	スロット %d のモジュールへの電源がオンに設定されている。
		DISABLED	4	スロット %d のモジュールへの電源が %s に設定されている。
		PSOK	4	電源モジュール %d がオンになった。
	POWER_SUPPLY_FAILURE	PSFAIL	4	電源モジュール %d の出力に障害が発生した。
		PSREDUNDANTMODE	4	電源モジュールは冗長モードに設定されている。
		PSCOMBINEDMODE	4	電源モジュールはコンバインド モードに設定されている。
		PSREDUNDANTMISMATCH	4	電源モジュールのレート出力が一致しない。
		PSMISMATCH	4	電源モジュールのレート出力が一致しない。

表 60-3　Call Home アラート グループ、イベント、および動作 （続き）

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
		PSNOREDUNDANCY	4	電源モジュールの冗長性が完全ではない。電源の使用量が供給容量の下限を超えた。
	POWER_SUPPLY_FAILURE	PSOCPSHUTDOWN	2	電源の使用量が電源モジュール %d の許容量を超えた。
		PSREDUNDANTONESUPPLY	4	電源冗長モードで、システムは 1 つの電源モジュールで動作している。
		PSREDUNDANTBOTHSUPPLY	4	電源冗長モードで、システムは両方の電源モジュールで動作している。
	POWER_SUPPLY_FAILURE	UNDERPOWERED	4	システム内のすべての FRU を動作させるには電力が不十分である。
	POWER_SUPPLY_FAILURE	COULDNOTREPOWER	4	FRU（スロット %d）に電力を再供給したかったが、できなかった。
	POWER_SUPPLY_FAILURE	POWERDENIED	4	電力が不十分。スロット %d のモジュールに電力が供給できない。
		UNSUPPORTED	4	スロット %d のモジュールはサポートされておらず、電力が供給できない：%s。
	POWER_SUPPLY_FAILURE	INSUFFICIENT POWER	2	重要なすべてのカードを動作させるのに十分な電力がないため、ラインカード すべての電源を切断する。
		INPUTCHANGE	4	電源モジュール %d の入力が変更された。電力容量が %sW に調整された。
		PSINPUTDROP	4	電源モジュール %d の入力が低下した。
Inventory				Inventory ステータスは、ユニットがコールド ブートされた場合や、FRU が挿入または取り外された場合に指定される。これは、重大ではないイベントと見なされ、情報はステータスと資格設定に使用される（TAC に送信）。 実行される CLI コマンド **remote command switch show version** **show diagbus** **show idprom all** **show install running（ION のみ）** **show inventory** **show module** **show version**
	HARDWARE_INSERTION	INSPS	6	電源モジュールがスロット %d に挿入された。
	HARDWARE_REMOVAL	REMPS	6	電源モジュールがスロット %d から取り外された。

表 60-3　Call Home アラート グループ、イベント、および動作 （続き）

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
	HARDWARE_REMOVAL	REMCARD	6	カードがスロット %d から取り外され、インターフェイスがディセーブルになった。
		STDBY_REMCARD	6	スタンバイ スーパーバイザ エンジン上の OIR 機能が、アクティブなスーパーバイザ エンジンによって、スロット [n] からプロセッサが取り外されたと通知された。
	HARDWARE_INSERTION	INSCAR	6	カードがスロット %d に挿入され、インターフェイスがオンラインになった。
		STDBY_INSCARD	6	スタンバイ スーパーバイザ エンジンが通知された。スロット %d のカードがオンラインになっている。
		SEQ_MISMATCH	6	スロット %d のカードの Switch-Module Configuration Protocol（SCP）シーケンスが一致しない：%s。
	HARDWARE_REMOVAL	UNKNOWN	3	スロット %d のカードが不明。カードはディセーブルになる。
		STDBY_UNKNOWN	3	スタンバイ スーパーバイザ エンジンが通知された。スロット %d のカードが不明。
	HARDWARE_REMOVAL	UNSUPPORTED	3	スロット %d のカードはサポートされていない。%s。
		PWRCYCLE	3	モジュール %d のカードは電源サイクル中 %s。
		STDBY_PWRCYCLE	3	スタンバイ スーパーバイザ エンジンが通知された。モジュール %d のカードは電源サイクル中 %s。
		CONSOLE	6	%s プロセッサへのコンソール所有権の変更。
		RUNNING_CONFIG	6	スイッチオーバー中に OIR 機能は running-config プロセッサをクリーン アップできない。
		DISALLOW	6	EHSA モードでセカンダリとしてアップさせようとしたスーパーバイザ エンジンは許可されない。
	HARDWARE_REMOVAL	REMFAN	6	ファン %d が取り外された。
	HARDWARE_INSERTION	INSFAN	6	ファン %d が挿入された。
	HARDWARE_INSERTION	PSINSERTED	4	電源モジュールがスロット %d に挿入された。

表 60-3　Call Home アラート グループ、イベント、および動作 （続き）

アラート グループ	Call Home 起動イベント	Syslog イベント	Severity	説明と実行される CLI コマンド
Diagnostic				標準またはインテリジェント ラインカードに関連するイベント （TAC に送信）。 実行される CLI コマンド **remote command switch show version** **show buffers** **show diagnostic result module <slot#> detail** **show diagnostic result module all** **show install running（ION のみ）** **show inventory** **show logging** **show logging system last 100** **show module** **show version**
		DIAG_OK		
		DIAG_BYPASS		
	DIAGNOSTICS_FAILURE	DIAG_ERROR		
	DIAGNOSTICS_FAILURE	DIAG_MINOR_ERROR		
	DIAGNOSTICS_FAILURE	DIAG_MAJOR_ERROR		
Configuration				ユーザが作成した設定要求 （TAC に送信）。 実行される CLI コマンド **remote command switch show version** **show install running（ION のみ）** **show module** **show running-config all** **show startup-config** **show version**
Test		TEST		ユーザが作成したテスト メッセージ （TAC に送信）。 実行される CLI コマンド **show install running（ION のみ）** **show module** **show version**

メッセージの内容

次の表に、アラート グループ メッセージの内容の形式を示します。

- 表 60-4 では、ショート テキスト メッセージの内容フィールドについて説明しています。
- 表 60-5 では、ロング テキスト メッセージと XML メッセージすべてに共通の内容フィールドについて説明しています。特定のアラート グループ メッセージに固有のフィールドは、共通フィールドの間に挿入されます。挿入ポイントは表に示しています。

- 表 60-6 では、リアクティブ メッセージ（TAC を必要とするシステム障害）とプロアクティブ メッセージ（システム パフォーマンスが低下する可能性のある問題）に挿入される内容フィールドについて説明しています。
- 表 60-7 では、コンポーネント メッセージに挿入される内容フィールドについて説明しています。

表 60-4　ショート テキスト メッセージの形式

データ項目	説明
Device identification	設定されたデバイス名
Date/time stamp	起動イベントのタイム スタンプ
Error isolation message	起動イベントの簡単な説明（英語）
Alarm urgency level	システム メッセージに適用されるようなエラー レベル

表 60-5　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Time stamp	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DDTHH:MM:SS*	CallHome/EventTime
Message name	メッセージの名前。特定のイベント名は「アラート グループの起動イベントとコマンド」（P.60-18）に記載。	（ショート テキスト メッセージのみ）
Message type	具体的に Call Home。	CallHome/Event/Type
Message subtype	特定のタイプのメッセージ、full、delta、または test。	CallHome/Event/SubType
Message group	具体的に reactive または proactive。	（ロング テキスト メッセージのみ）
Severity level	メッセージの重大度（表 60-1（P.60-8）を参照）。	Body/Block/Severity
Source ID	ルーティングのための製品タイプ。具体的に Catalyst 6500。	（ロング テキスト メッセージのみ）
Device ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。 メッセージがファブリック スイッチに固有でない場合、このフィールドは空白。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • *@* は区切り文字。 • *Sid* は、シャーシのシリアル番号としてシリアル ID を特定する C。 • *serial* は、[Sid] フィールドによって特定される数字。 例：WS-C6509@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/CustomerId
Contract ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/ContractId
Site ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/SiteId

表 60-5　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド （続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Server ID	メッセージがファブリック スイッチから生成されている場合、これはスイッチの固有のデバイス ID（UDI）。 形式は、*type*@*Sid*@*serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字。 • *Sid* は、シャーシのシリアル番号としてシリアル ID を特定する C。 • *serial* は、[Sid] フィールドによって特定される数字。 例：WS-C6509@C@12345678	（ロング テキスト メッセージのみ）
Message description	エラーを説明する短い文章。	CallHome/MessageDescription
Device name	イベントが発生するノード。これは、デバイスのホスト名。	CallHome/CustomerData/SystemInfo/Name
Contact name	イベントの発生するノードに関連する問題を連絡する人物の名前。	CallHome/CustomerData/SystemInfo/Contact
Contact e-mail	このユニットの連絡先である人物の E メール アドレス。	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
Street address	このユニットに関連付けられた RMA 部品出荷の住所を含むオプションのフィールド。	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	スイッチのモデル名。これは、製品ファミリ名の一部として固有のモデル。	CallHome/Device/Cisco_Chassis/Model
Serial number	ユニットのシャーシのシリアル番号。	CallHome/Device/Cisco_Chassis/SerialNumber
Chassis part number	シャーシの最上アセンブリ番号。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="PartNumber"/
System Object ID	システムを一意に識別するシステム オブジェクト ID。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="sysObjectID"
SysDesc	管理対象デバイスのシステム説明。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="sysDescr"
このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
Command output name	発行される CLI コマンドの正確な名前。	/aml/Attachments/Attachment/Name
Attachment type	タイプ（通常はインライン）。	/aml/Attachemtents/Attachment@type

表 60-5　ロング テキスト メッセージと XML メッセージすべてに共通のフィールド （続き）

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
MIME type	通常はテキスト/プレーンまたは符号化タイプ。	/aml/attachments/attachment/Data@encoding
Command output text	自動的に実行されるコマンドの出力（表 60-3（P.60-19）を参照）。	/aml/attachments/attachment/atdata

表 60-6　リアクティブまたはプロアクティブ イベント メッセージのフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Chassis hardware version	シャーシのハードウェア バージョン。	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="SoftwareVersion"
Affected FRU name	イベント メッセージを生成する、影響のある FRU の名前。	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
Affected FRU serial number	問題を起こした FRU のシリアル番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
Affected FRU part number	問題を起こした FRU の部品番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	イベント メッセージを生成している FRU のスロット番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	問題を起こした FRU のハードウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	問題を起こした FRU で動作するソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString
Process name	プロセスの名前。	/aml/body/process/name
Process ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

表 60-7　Inventory イベント メッセージのフィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Chassis hardware version	シャーシのハードウェア バージョン。	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="SoftwareVersion"
FRU name	イベント メッセージを生成する、影響のある FRU の名前。	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	FRU のシリアル番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU part number	FRU の部品番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	FRU のスロット番号。	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	FRU のハードウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	FRU で動作するソフトウェア バージョン。	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

表 60-8　ユーザが作成したテスト メッセージの挿入フィールド

データ項目（プレーン テキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
Process ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

ロング テキスト形式での Syslog アラート通知の例

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
```

```
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:User Name
Contact Email:admin@yourcompany.com
Contact Phone:+1 408 555-1212
Street Address:#1234 Picaboo Street, Any city, Any state, 12345
Event Description:2006 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$
Interface fc2/5, vsan 1 is up

syslog_facility:PORT
start chassis information:
Affected Chassis:WS-C6509
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式での Syslog アラート通知の例

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00

<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.example.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2007-04-25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
```

```
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007-04-25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>user@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1 408 555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>270 E. Tasman Drive, San Jose, CA</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="12.2(20070421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 53 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged

Log Buffer (8192 bytes):

00:00:54: curr is 0x20000

00:00:54: RP: Currently running ROMMON from F2 region
```

```
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:01:01: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch

00:01:01: %SYS-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure console
debugging output.

00:03:00: SP: SP: Currently running ROMMON from F1 region
00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK_ENABLED: The default factory setting for config
register is 0x2102.It is advisable to retain 1 in 0x2102 as it prevents returning to
ROMMON when break is issued.

00:03:18: %SYS-SP-5-RESTART: System restarted --
Cisco IOS Software, s72033_sp Software (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 2
00:01:09: %SSH-5-ENABLED: SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy, power
usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6 became
active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]


00:00:22: %SYS-DFC4-5-RESTART: System restarted --
```

```
Cisco IOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 16:40 by username1
00:00:26: DFC2: Currently running ROMMON from F2 region
00:04:56: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimal Diagnostics...
00:00:09: DaughterBoard (Distributed Forwarding Card 3)

Firmware compiled 11-Apr-07 03:34 by integ Build [100]

slot_id is 8

00:00:31: %FLASHFS_HES-DFC8-3-BADCARD: /bootflash:: The flash card seems to be corrupted
00:00:31: %SYS-DFC8-5-RESTART: System restarted --
Cisco IOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 17:20 by username1
00:00:31: DFC8: Currently running ROMMON from S (Gold) region
00:04:59: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal Diagnostics...
00:05:12: %DIAG-SP-6-RUN_MINIMUM: Module 8: Running Minimal Diagnostics...
00:05:13: %DIAG-SP-6-RUN_MINIMUM: Module 1: Running Minimal Diagnostics...
00:00:24: %SYS-DFC1-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version
12.2(20070421:012711)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
00:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW Replication Mode
Change Detected. Current replication mode for unused asic session 1 is Centralized
00:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
00:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
00:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
00:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
00:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC error
timeout. Disabling linecard. (Expected during linecard OIR)
00:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to system PFC
and will perform at current system operating mode.
00:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online

Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

CHAPTER 61

IPv6 ポリシーベース ルーティングの設定

この章では、Cisco IOS Software Release 15.2(1)S の IPv6 ポリシーベース ルーティング（PBR）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 の『Cisco 7600 Series Router Command Reference』を参照してください。
http://www.cisco.com/en/US/products/ps6922/prod_command_reference_list.html

この章の内容は次のとおりです。

- 「IPv6 ポリシーベース ルーティングの概要」（P.61-1）
- 「IPv6 PBR の設定」（P.61-4）

IPv6 ポリシーベース ルーティングの概要

IPv6 PBR はパケットをルーティングするための柔軟なメカニズムを提供し、トラフィック フローのポリシーを定義します。ルーティング プロトコルで提供される既存のメカニズムを拡張し、補完します。PBR では、基本的なパケット マーキング機能も提供します。

PBR は次の処理を実行します。

- 拡張アクセス リスト基準に基づいてトラフィックを分類します。リストへのアクセスを提供し、一致基準を設定します。
- IPv6 precedence ビットを設定し、ネットワークでサービス クラスを区別できるようにします。
- 特定のトラフィック処理が行われたパスにパケットをルーティングします。ネットワークを介して特定の Quality of Service（QoS）を許可するためにパケットをルーティングできます。

Cisco 7600 シリーズ ルータは Earl7 フォワーディング エンジンの機能を使用して、アクセス コントロール リスト（ACL）Ternary Content Addressable Memory（TCAM）ルックアップによってトラフィックを分類するために、この機能を実装します。ACL TCAM ルックアップは、さまざまなレイヤ 3 およびレイヤ 4 トラフィック パラメータの組み合わせに基づいてトラフィックを分類します。分類後、ACL TCAM によりフローのマッチングが行われます。Feature Manager（FM）コンポーネントは、インターフェイスで設定されたルート マップ ポリシーを一連の値、マスク、および結果（VMR）に変換し、これらを ACL TCAM でプログラムします。

ポリシー ベース ルーティング

PBR がイネーブルなインターフェイスで受信されたすべてのパケットは、ルート マップと呼ばれる拡張パケット フィルタを通過します。ルート マップは *permit* または *deny* とマークされたステートメントで構成され、次のように解釈されます。

- パケットが、*permit* とマークされているルート マップのすべての match ステートメントに一致する場合、ルータは set ステートメントを使用して PBR をパケットに適用します。
- パケットが、*deny* とマークされているルート マップのいずれかの match ステートメントに一致する場合、ルータはそのパケットに PBR を適用せず、通常どおり転送します。
- ステートメントが permit とマークされ、パケットがいずれのルート マップ ステートメントにも一致しない場合、ルータはそのパケットを通常の転送チャネルを介して返送し、宛先ベースのルーティングを実行します。

パケット マッチング

シーケンスの IPv6 PBR の一致基準は IPv6 アクセス リストおよびパケット長操作の組み合わせによって指定します。match ステートメントは、**match ipv6 address** コマンドで指定した基準に基づいて最初に評価され、次に、**match length** コマンドで指定した基準に基づいて評価されます。したがって、ACL と length ステートメントの両方が使用されている場合、最初に ACL によるマッチングがパケットに対して行われます。ACL マッチングに合格したパケットだけが、パケット長による次のマッチングの対象となります。最後に、ACL と length ステートメントの両方に合格したパケットだけに対してポリシー ルーティングが行われます。

set ステートメントを使用したパケット転送

IPv6 パケット転送に対する PBR は、PBR ルート マップの複数の set ステートメントを使用して制御されます。転送アクション（優先順位の降順）、およびこれらのオプションが ACL TCAM でプログラムされた VMR の結果に反映される方法を次に列挙します。複数のパケット転送アクションを 1 つのシーケンスで指定した場合、優先順位の最も高いアクションが選択されます。

表 61-1　パケット転送の set ステートメント

set ステートメント	注記
set vrf *vrf name*	パケット属性に基づいてパケットが送信される必要がある VPN ルーティングおよび転送（VRF）インスタンスを指定します。デフォルトでは、パケットが転送される VRF はパケットを受信する VRF と同じです。
set ipv6 next-hop *next-hop ipv6 address*	パケットのネクスト ホップを指定します。このネクスト ホップは、ルーティング情報ベース（RIB）に存在し、直接接続され、グローバル IPv6 アドレスである必要があります。このネクスト ホップが無効である場合、set 文は無視されます。
set interface *next-hop interface*	パケットに対してネクスト ホップ インターフェイスを指定します。パケットは、指定されたインターフェイスの外に転送されます。パケットの宛先アドレスのエントリは、IPv6 RIB に存在する必要があります。指定された出力インターフェイスは、パス セットに存在する必要があります。このインターフェイスが無効な場合、set ステートメントは無視されます。

set ステートメント	注記
set ipv6 default next-hop *default next-hop ipv6 address*	通常の転送方法でデフォルトの結果が得られない場合に、パケットの接続されるネクスト ホップを指定します。グローバル IPv6 アドレスである必要があります。この set 文は、IPv6 RIB のパケット宛先に明示的なエントリがない場合にだけ使用されます。
set default interface *default next-hop interface*	通常の転送方法で結果が得られない場合に、一致パケットの転送元のデフォルト ネクスト ホップ インターフェイスを指定します。この set 文は、IPv6 RIB のパケット宛先に明示的なエントリがない場合にだけ使用されます。

IPv6 PBR の制限

次の制限は、IPv6 PBR に適用されます。

- match length はハードウェアでサポートされず、PBR はソフトウェアに適用されます。
- パケットのマーキング アクションはハードウェアでサポートされず、PBR によるマーキングが必要なパケットは、ソフトウェアにパントされます。
- set interface はシリアル インターフェイスのハードウェアでのみサポートされます。他のインターフェイスはソフトウェアでサポートされます。
- IPv6 ホップバイホップ ヘッダーが含まれるパケットは、ルータによって検査する必要があり、ソフトウェアにパントされます。このようなパケットには、ソフトウェアで PBR が適用されます。
- IPv6 フロー ラベル、DSCP 値、および拡張ヘッダー（ルーティング、モビリティ、宛先ヘッダーなど）でアクセス リスト マッチングを使用する PBR ポリシーは、ハードウェアで完全には分類できず、部分分類後にソフトウェアでパントされます。
- 非圧縮性アドレス上でアクセス リスト マッチングが使用された場合は、ハードウェアでトラフィックを完全に分類できません。この場合、PBR はソフトウェアに適用されます。
- Tycho ベースのシステムでは、レイヤ 4 プロトコルでのマッチングが必要なフラグメント パケットは、システム ソフトウェアにパントされます。
- SVI インターフェイスの IPv6 PBR はソフトウェアに適用され、ハードウェアは部分分類のみ提供します。
- ハードウェアに適用された IPv6 PBR は、ルータ アドレス宛てのパケットに適用されます。
- ネクスト ホップがトンネルの反対側にある set next-hop アクションはハードウェアでサポートされません。
- set interface および set default interface では、インターフェイスはポイントツーポイントである必要があります。
- PBR は、マルチキャスト トラフィックとリンク ローカル アドレス宛てのトラフィックには適用されません。
- トラフィック フローがない場合は、TCAM エントリはパントからポリシー ルートに変更されません。

IPv6 PBR の設定

IPv6 PBR を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router# enable`	特権 EXEC モードをイネーブルにします。
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)# route-map map-tag [permit | deny] [sequence-number]`	あるルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。 • **route-map** コマンドを使用して、ルート マップ 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-route-map)# match length minimum-length maximum-length`
	or
	`Router(config-route-map)# match ipv6 address {prefix-list prefix-list-name | access-list-name}`
		一致基準を指定します。
		• レベル 3 のパケット長とのマッチング。
		• 指定された IPv6 アクセス リストとのマッチング。
		（注） match コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。

ステップ 5	`Router(config-route-map)# set ipv6 precedence precedence-value`
	or
	`Router(config-route-map)# set ipv6 next-hop global-ipv6-address`
	or
	`Router(config-route-map)# set interface type number`
	or
	`Router(config-route-map)# set ipv6 default next-hop global-ipv6-address`
	or
	`Router(config-route-map)# set default interface type number`
	or
	`Router(config-route-map)# set vrf vrf-name`
		基準に一致したパケットで実行されるアクションを指定します。
		• IPv6 ヘッダーに precedence 値を設定します。
		• パケットのルーティング先となるネクスト ホップを設定します（ネクスト ホップは隣接していなければなりません）。
		• パケットの出力インターフェイスを設定します。
		• この宛先に明示ルートがない場合、パケットをルーティングする先のネクスト ホップを設定します。
		• 宛先への明示的なルートがない場合に、パケットの出力インターフェイスを設定します。
		• ポリシーベース ルーティング VRF の選択のために、ルート マップ内に VRF インスタンス選択を設定します。

ステップ 6	`Router(config-route-map)# exit`	ルータをグローバル コンフィギュレーション モードに戻します。

	コマンド	目的
ステップ 7	Router(config)# **interface** *type number*	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 8	Router(config-if)# **ipv6 policy route-map** *route-map-name*	インターフェイスで IPv6 PBR のルート マップを識別します。

検証

次のコマンドは、PBR の設定を確認するのに役立ちます。

- **show ipv6 policy** コマンドは、PBR の設定を表示します。

```
Router# show ipv6 policy
Interface                Routemap
GigabitEthernet0/0/0     src-1
```

- **show route-map** コマンドによって、ポリシーに一致した数など、特定のルート マップ情報が表示されます。

```
Router# show route-map
route-map bill, permit, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches:0 packets, 0 bytes
```

- **show tcam interface** コマンドは、サポートされるハードウェアおよびソフトウェアを表示します。

ハードウェア：

```
Router# show tcam interface gigabitEthernet 8/9 acl in ipv6 module 8

ICMP Neighbor Discovery Packet Types:
na - neighbor advertisement ra - router advertisement
ns - neighbor solicit rs - router solicit
r - redirect

IPV6 Address Types:
full - IPv6 Full eui - IPv6 EUI
eipv4 - IPv6 embeded IPv4
------------------------------------------------------
policy-route ipv6 host 1000::2(full) host 4000::2(full)
permit ipv6 any(eipv4) any
permit ipv6 any(eui) any
permit ipv6 any(full) any
```

ソフトウェア：

```
Router# show tcam interface gigabitEthernet 4/2 acl in ipv6 module 4

ICMP Neighbor Discovery Packet Types:
na - neighbor advertisement  ra - router advertisement
ns - neighbor solicit        rs - router solicit
r  - redirect

IPV6 Address Types:
full - IPv6 Full             eui - IPv6 EUI
eipv4 - IPv6 embeded IPv4
------------------------------------------------------
   permit       ipv6 any(eui) 0:FE80::/10(eui)
```

```
   permit       ipv6 any(full) 0:FE80::/10(eui)
   permit       ipv6 any(eui) FF00::/8(full)
   permit       ipv6 any(full) FF00::/8(full)
   permit       ipv6 any(eui) FE80::/10(full)
   permit       ipv6 any(full) FE80::/10(full)
   punt         ipv6 any(eui) any
   punt         ipv6 any(full) any
   permit       ipv6 any(eipv4) any
   permit       ipv6 any(eui) any
   permit       ipv6 any(full) any
```

- **show fm ipv6 pbr all** コマンドは、指定されたインターフェイスの IPv6 PBR VMR を表示します。

```
Router# show fm ipv6 pbr all
------------------------------------------------------------------------------
FM_FEATURE_IPv6_PBR      i/f: Gi3/3      rmap: empty1
==============================================================================
------------------------------------------------------
    Seq. No: 65536       Seq. Result : FM_RESULT_PERMIT
------------------------------------------------------
DPort  - Destination Port  SPort  - Source Port       Pro    - Protocol
PT     - Packet Type       DPT    - Dst. Packet Type  SPT    - Src. Packet Type
X      - XTAG              TOS    - TOS Value         Res    - VMR Result
RFM    - R-Recirc. Flag    MRTNPC - M-Multicast Flag  R      - Reflexive flag
       - F-Fragment flag          - T-Tcp Control     N      - Non-cachable
       - M-More Fragments         - P-Mask Priority(H-High, L-Low)
Adj.   - Adj. Index        C      - Capture Flag      T      - M(Mask)/V(Value)
FM     - Flow Mask         NULL   - Null FM           SAO    - Source Only FM
DAO    - Dest. Only FM     SADA   - Sour.& Dest. Only VSADA  - Vlan SADA Only
ISADA  - Intf. SADA        FF     - Full Flow         VFF    - Vlan Full Flow
IFF    - Intf. FF          F-VFF  - Either FF or VFF  IFF-FF - Either IFF or FF
A-VSD  - Atleast VSADA     A-FF   - Atleast FF        A-VFF  - Atleast VFF
A-SON  - Atleast SAO       A-DON  - Atleast DAO       A-SD   - Atleast SADA
SHORT  - Shortest          ISADA-L- ISADA Least       FF-L   - FF Least
IFF-L  - IFF Least         A-SFF  - Any short than FF A-EFF  - Any except FF
A-EVFF - Any except VFF    SA-L   - Source Least      DA-L   - Dest. Least
SADA-L - SADA Least        FF-LESS- FF Less           N-FF   - Not FF
N-IFF  - Not IFF           A-LVFF - Any less than VFF FULL   - Full Pkt Type
EUI    - EUI 64 Pkt Type   EMBD   - Embedded Pkt Type ELNK   - EUI Link Overlap
ESIT   - EUI Site Overlap  LINK   - Link Pkt Type     SITE   - Site Pkt Type
ERR    - Flowmask Error
+----+-+----------------------------------------+----------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                       |     Source IPv6 Addr                   |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+----------------------------------------+----------------------------------------+
----+----+----+---+---+-+------+----+------+

 1    V                                  FF00::                                      ::
FULL  EUI ----   0 --- - ----L- ---- SHORT
      M                                  FF00::                                      ::
EMBD  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                  FF00::                                      ::
FULL FULL ----   0 --- - ----L- ---- SHORT
      M                                  FF00::                                      ::
EMBD EMBD        0   0
      TM_PERMIT_RESULT

 3    V                                 0:FE80::                                     ::
EUI  EUI ----   0 --- - ----L- ---- SHORT
      M                                 0:FFC0::                                     ::
EUI  EUI        0   0
```

```
      TM_PERMIT_RESULT

 4    V                                    FE80::                                    ::
FULL  EUI ----   0 --- - ----L- ---- SHORT
      M                                    FFC0::                                    ::
EMBD  EUI        0   0
      TM_PERMIT_RESULT

 5    V                                  0:FE80::                                   ::
EUI FULL ----   0 --- - ----L- ---- SHORT
      M                                  0:FFC0::                                   ::
EUI EMBD        0   0
      TM_PERMIT_RESULT

 6    V                                    FE80::                                    ::
FULL FULL ----   0 --- - ----L- ---- SHORT
      M                                    FFC0::                                    ::
EMBD EMBD        0   0
      TM_PERMIT_RESULT

 7    V                                       ::                                     ::
---- ---- ----   0 --- - ----L- ---- SHORT
      M                                       ::                                     ::
---- ----        0   0
      TM_L3_DENY_RESULT

------------------------------------------------------
    Seq. No: 10          Seq. Result : FM_RESULT_ADJREDIRECT
------------------------------------------------------
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                       |     Source IPv6 Addr                    |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+

 1    V                                       ::                                     ::
----  EUI ----   0 --- - ----L- 0 SHORT
      M                                       ::                                     ::
----  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                       ::                                     ::
---- FULL ----   0 --- - ----L- 0 SHORT
      M                                       ::                                     ::
---- EMBD        0   0
      TM_PERMIT_RESULT

 3    V                                       ::                                     ::
---- ---- ----   0 --- - ----L- 0 SHORT
      M                                       ::                                     ::
---- ----        0   0
      TM_L3_DENY_RESULT

------------------------------------------------------
    Seq. No: 65537       Seq. Result : FM_RESULT_PERMIT
------------------------------------------------------
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                       |     Source IPv6 Addr                    |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+
```

```
 1    V                                        ::                                      ::
----  EUI ----   0 --- - ----L- ---- SHORT
      M                                        ::                                      ::
----  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                        ::                                      ::
---- FULL ----   0 --- - ----L- ---- SHORT
      M                                        ::                                      ::
---- EMBD       0   0
      TM_PERMIT_RESULT

 3    V                                        ::                                      ::
---- ---- ----   0 --- - ----L- ---- SHORT
      M                                        ::                                      ::
---- ----       0   0
      TM_L3_DENY_RESULT


Index : 0
        Feature_id : 4C adj : 5733EB50 vlan : 1027 dmac : 0000.1742.3558
        smac : 0018.7415.1980 encap : 1 mtu : 1518 TTL : 1
        Rdt Indx : 0 recirc : 0 Non-Cachable : 0 Priority : 1
```

- **show fm ipv6 pbr interface** コマンドは、指定したインターフェイスでの IPv6 PBR VMR を表示します。

```
Router# show fm ipv6 pbr interface gigabitEthernet 3/3
-------------------------------------------------------------------------------
FM_FEATURE_IPv6_PBR      i/f: Gi3/3      rmap: empty1
===============================================================================
-----------------------------------------------------
    Seq. No: 65536       Seq. Result : FM_RESULT_PERMIT
-----------------------------------------------------
DPort  - Destination Port  SPort  - Source Port       Pro    - Protocol
PT     - Packet Type       DPT    - Dst. Packet Type  SPT    - Src. Packet Type
X      - XTAG              TOS    - TOS Value         Res    - VMR Result
RFM    - R-Recirc. Flag    MRTNPC - M-Multicast Flag  R      - Reflexive flag
       - F-Fragment flag          - T-Tcp Control     N      - Non-cachable
       - M-More Fragments         - P-Mask Priority(H-High, L-Low)
Adj.   - Adj. Index        C      - Capture Flag      T      - M(Mask)/V(Value)
FM     - Flow Mask         NULL   - Null FM           SAO    - Source Only FM
DAO    - Dest. Only FM     SADA   - Sour.& Dest. Only VSADA  - Vlan SADA Only
ISADA  - Intf. SADA        FF     - Full Flow         VFF    - Vlan Full Flow
IFF    - Intf. FF          F-VFF  - Either FF or VFF  IFF-FF - Either IFF or FF
A-VSD  - Atleast VSADA     A-FF   - Atleast FF        A-VFF  - Atleast VFF
A-SON  - Atleast SAO       A-DON  - Atleast DAO       A-SD   - Atleast SADA
SHORT  - Shortest          ISADA-L- ISADA Least       FF-L   - FF Least
IFF-L  - IFF Least         A-SFF  - Any short than FF A-EFF  - Any except FF
A-EVFF - Any except VFF    SA-L   - Source Least      DA-L   - Dest. Least
SADA-L - SADA Least        FF-LESS- FF Less           N-FF   - Not FF
N-IFF  - Not IFF           A-LVFF - Any less than VFF FULL   - Full Pkt Type
EUI    - EUI 64 Pkt Type   EMBD   - Embedded Pkt Type ELNK   - EUI Link Overlap
ESIT   - EUI Site Overlap  LINK   - Link Pkt Type     SITE   - Site Pkt Type
ERR    - Flowmask Error
+----+-+---------------------------------------+---------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                      |     Source IPv6 Addr                  |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+---------------------------------------+---------------------------------------+
----+----+----+---+---+-+------+----+------+

 1    V                                  FF00::                                      ::
FULL  EUI ----   0 --- - ----L- ---- SHORT
```

```
      M                                     FF00::                                    ::
EMBD  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                     FF00::                                    ::
FULL FULL ----   0 --- - ----L- ---- SHORT
      M                                     FF00::                                    ::
EMBD EMBD        0   0
      TM_PERMIT_RESULT

 3    V                                  0:FE80::                                   ::
EUI  EUI ----   0 --- - ----L- ---- SHORT
      M                                  0:FFC0::                                   ::
EUI  EUI        0   0
      TM_PERMIT_RESULT

 4    V                                     FE80::                                    ::
FULL  EUI ----   0 --- - ----L- ---- SHORT
      M                                     FFC0::                                    ::
EMBD  EUI        0   0
      TM_PERMIT_RESULT

 5    V                                  0:FE80::                                   ::
EUI FULL ----   0 --- - ----L- ---- SHORT
      M                                  0:FFC0::                                   ::
EUI EMBD        0   0
      TM_PERMIT_RESULT

 6    V                                     FE80::                                    ::
FULL FULL ----   0 --- - ----L- ---- SHORT
      M                                     FFC0::                                    ::
EMBD EMBD        0   0
      TM_PERMIT_RESULT

 7    V                                        ::                                     ::
---- ---- ----   0 --- - ----L- ---- SHORT
      M                                        ::                                     ::
---- ----        0   0
      TM_L3_DENY_RESULT

-----------------------------------------------------
    Seq. No: 10          Seq. Result : FM_RESULT_ADJREDIRECT
-----------------------------------------------------
+----+-+---------------------------------------+---------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                      |     Source IPv6 Addr                  |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+---------------------------------------+---------------------------------------+
----+----+----+---+---+-+------+----+------+

 1    V                                        ::                                     ::
----  EUI ----   0 --- - ----L- 0 SHORT
      M                                        ::                                     ::
----  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                        ::                                     ::
---- FULL ----   0 --- - ----L- 0 SHORT
      M                                        ::                                     ::
---- EMBD        0   0
      TM_PERMIT_RESULT

 3    V                                        ::                                     ::
---- ---- ----   0 --- - ----L- 0 SHORT
```

```
      M                                          ::                                      ::
---- ----        0   0
      TM_L3_DENY_RESULT

-----------------------------------------------------
    Seq. No: 65537       Seq. Result : FM_RESULT_PERMIT
-----------------------------------------------------
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+
|Indx|T|    Dest IPv6 Addr                        |     Source IPv6 Addr                    |
DPT| SPT| PT |Pro|RFM|X|MRTNPC|Adj.|  FM  |
+----+-+-----------------------------------------+-----------------------------------------+
----+----+----+---+---+-+------+----+------+

 1    V                                          ::                                      ::
----  EUI ----   0 --- - ----L- ---- SHORT
      M                                          ::                                      ::
----  EUI        0   0
      TM_PERMIT_RESULT

 2    V                                          ::                                      ::
---- FULL ----   0 --- - ----L- ---- SHORT
      M                                          ::                                      ::
---- EMBD        0   0
      TM_PERMIT_RESULT

 3    V                                          ::                                      ::
---- ---- ----   0 --- - ----L- ---- SHORT
      M                                          ::                                      ::
---- ----        0   0
      TM_L3_DENY_RESULT


Index : 0
        Feature_id : 4C adj : 5733EB50 vlan : 1027 dmac : 0000.1742.3558
        smac : 0018.7415.1980 encap : 1 mtu : 1518 TTL : 1
        Rdt Indx : 0 recirc : 0 Non-Cachable : 0 Priority : 1
```

トラブルシューティングのヒント

表 61-2 では、IPv6 PBR の設定時に発生する問題のトラブルシューティングについて示します。

表 61-2　IPv6 の問題のトラブルシューティング

問題	ソリューション
詳細不明の問題があると考えられる場合	• **debug** fm ipv6 [all | events | pbr | vmrs] コマンドを使用します – **all** : すべての IPv6 デバッグ情報を表示します。 – **events** : FM IPv6 イベントに関するデバッグ情報を表示します。 – **pbr** : FM IPv6 ポリシーベース ルーティングに関するデバッグ情報を表示します。 – **vmrs** : FM IPv6 VMR に関するデバッグ情報を表示します。 • **debug ipv6 policy** コマンドを使用して、IPv6 ポリシー ルーティング パケットのアクティビティを表示します。

CHAPTER 62

Mini Protocol Analyzer の使用

この章では、Cisco 7600 シリーズ ルータ上で Mini Protocol Analyzer を使用する方法について説明します。Mini Protocol Analyzer 機能は Release12.2(33)SXI 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, All Releases*』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。

- 「Mini Protocol Analyzer の機能概要」（P.62-1）
- 「Mini Protocol Analyzer の設定」（P.62-2）
- 「キャプチャの開始および停止」（P.62-4）
- 「キャプチャ バッファの表示およびエクスポート」（P.62-6）
- 「Mini Protocol Analyzer の設定、操作、表示例」（P.62-7）

Mini Protocol Analyzer の機能概要

Mini Protocol Analyzer は SPAN セッションからネットワーク トラフィックをキャプチャし、キャプチャしたパケットをローカル メモリ バッファに保存します。提供されているフィルタリング オプションを使用することで、キャプチャするパケットを次のとおり制限できます。

- 選択した VLAN、ACL、または MAC アドレスからのパケット
- 特定の EtherType のパケット
- 特定のパケット サイズのパケット

即時コマンドを入力してキャプチャを開始、終了したり、キャプチャをスケジューリングして特定の日時にキャプチャを開始できます。

キャプチャしたデータは、コンソールに表示したり、ローカル ファイル システムに保存したり、または標準的なファイル転送プロトコルを使用して外部サーバへエクスポートできます。キャプチャしたファイルの形式は libpcap です。この形式は、多くのパケット分析プログラムおよび sniffer プログラムによってサポートされています。このファイル形式の詳細については、次の URL を参照してください。

http://www.tcpdump.org/

デフォルトでは、各パケットの最初の 68 バイトだけがキャプチャされます。

Mini Protocol Analyzer の設定

Mini Protocol Analyzer を使用してキャプチャ 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)# [no] monitor session number type capture`	キャプチャ用としてプロセッサに割り当てられているパケットを使用して SPAN セッション番号を設定します。キャプチャ セッションのコンフィギュレーション モードを開始します。セッション番号の範囲は 1 ～ 80 です。 接頭辞に **no** を使用するとセッションが削除されます。
ステップ 3	`Router(config-mon-capture)# buffer-size buf_size`	（任意）キャプチャ バッファのサイズを KB 単位で設定します。指定できる範囲は 32 ～ 65535 KB です。デフォルトは 2048 KB です。
ステップ 4	`Router(config-mon-capture)# description session_description`	（任意）キャプチャ セッションの説明を入力します。説明には最大 240 文字まで入力できますが、特殊文字は入力できません。説明にスペースを含める場合、引用符（""）で囲む必要があります。
ステップ 5	`Router(config-mon-capture)# rate-limit pps`	（任意）1 秒当たりにキャプチャできるパケット数（*pps*）を制限します。指定できる範囲は 10 ～ 100000 パケットで、デフォルトは 1 秒あたり 10000 パケットです。
ステップ 6	`Router(config-mon-capture)# source {{interface {single_interface | interface_list | interface_range | mixed_interface_list} | port-channel channel_id}} | {vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}}[rx | tx | both]`	キャプチャ セッションと送信元ポートまたは VLAN を対応付けて、モニタするトラフィックの方向を選択します。デフォルトは双方向です。
ステップ 7	`Router(config-mon-capture)# exit`	キャプチャ セッションのコンフィギュレーション モードを終了します。

キャプチャ セッションを設定する場合、次の情報に注意してください。

- 一度に設定できるキャプチャ セッションは 1 つだけです。同時キャプチャ セッションを複数設定することはできません。
- **source interface** コマンド引数は、単一のインターフェイス、2 つのインターフェイス番号（小さい番号が先、ダッシュで区切る）で指定するインターフェイスの範囲、またはインターフェイスと範囲をカンマで区切ったリストのいずれかです。

（注） 送信元インターフェイスのリストを設定する場合、カンマの前後にスペースを入れる必要があります。送信元インターフェイスの範囲を設定する場合、ダッシュの前後にスペースを入れる必要があります。

- **source vlan** コマンド引数は、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く）、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、または VLAN と範囲のリストのいずれかです。

（注）　送信元の VLAN のリストを設定する場合、カンマの前後にスペースを入れないでください。送信元の VLAN の範囲を設定する場合、ダッシュの前後にスペースを入れないでください。この要件は、送信元インターフェイスのリストと範囲を指定する場合の要件とは異なることに注意してください。

- キャプチャ セッションの設定時は、データのキャプチャは開始されません。「キャプチャの開始および停止」（P.62-4）に示すとおり、キャプチャは **monitor capture start** または **monitor capture schedule** コマンドによって開始されます。
- キャプチャ バッファは、デフォルトでは linear（直線）ですが、**monitor capture start** または **monitor capture schedule** コマンドのランタイム オプションとして circular（循環）に設定できます。
- 使用可能なハードウェア レート制限レジスタがない場合、キャプチャ セッションはディセーブルになります。
- VLAN フィルタが設定されている場合、送信元 VLAN は変更できません。VLAN フィルタを削除してから、送信元 VLAN を変更してください。

キャプチャ対象となるパケットのフィルタリング

キャプチャ対象となるパケットのフィルタリング用にいくつかのオプションが提供されています。レート制限が適用される前に、ハードウェアでは ACL および VLAN によるフィルタリングが実行され、ソフトウェアではその他すべてのフィルタが実行されます。ソフトウェアのフィルタリングを実行すると、キャプチャ レートが下がる可能性があります。

Mini Protocol Analyzer のキャプチャ対象となるパケットをフィルタリングするには、この作業をキャプチャ セッションのコンフィギュレーション モードで行います。

	コマンド	目的
ステップ 1	`Router(config-mon-capture)# [no] filter access-group {acl_number | acl_name}`	（任意）指定した ACL からのパケットだけをキャプチャします。
ステップ 2	`Router(config-mon-capture)# [no] filter vlan {vlan_ID | vlan_list | vlan_range | mixed_vlan_list}`	（任意）指定した送信元 VLAN（1 つまたは複数）からのパケットをキャプチャします。
ステップ 3	`Router(config-mon-capture)# [no] filter ethertype type`	（任意）指定した EtherType のパケットだけをキャプチャします。*type* は、10 進数、16 進数、または 8 進数で指定できます。
ステップ 4	`Router(config-mon-capture)# [no] filter length min_len [max_len]`	（任意）サイズが *min_len* ～ *max_len*（両方の値を含む）の範囲のパケットだけをキャプチャします。*max_len* が指定されていない場合は、サイズが *min_len* のパケットだけがキャプチャされます。*min_len* の範囲は 0 ～ 9216 バイト、*max_len* の範囲は 1 ～ 9216 バイトです。
ステップ 5	`Router(config-mon-capture)# [no] filter mac-address mac_addr`	（任意）指定された MAC アドレスからのパケットだけをキャプチャします。
ステップ 6	`Router(config-mon-capture)# end`	コンフィギュレーション モードを終了します。

キャプチャに関する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。

- **filter vlan** 引数は、1 ～ 4094 の範囲の単一の VLAN 番号（予約済み VLAN を除く）、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、または VLAN と範囲のリストのいずれかです。

（注）　フィルタリング用 VLAN のリストを設定する場合、カンマの前後にスペースを入れる必要があります。フィルタリング用 VLAN の範囲を設定する場合、ダッシュの前後にスペースを入れる必要があります。この要件は、前述した送信元の VLAN リストと範囲を指定する場合の要件とは異なることに注意してください。

- EtherType を 10 進数値として入力するには、先頭にゼロの付かない値（1 ～ 65535）を入力します。16 進数値を入力するには、4 文字の 16 進数の前にプレフィックスの 0x を入力します。8 進数値を入力するには、先頭にゼロを付けた数値（0 ～ 7）を入力します。たとえば、802.1Q EtherType を入力する場合、10 進数値では 33024、16 進数値では 0x8100、8 進数値では 0100400 となります。
- MAC アドレスは、ドット付き 16 進表記の 3 つの 2 バイト値で入力します。例：0123.4567.89ab
- **no** キーワードを使用するとフィルタが削除されます。

（注）　**no** キーワードを使用して VLAN フィルタを削除したあとは、コンフィギュレーション モードを終了して、キャプチャ コンフィギュレーション モードを再び開始し、**source vlan** コマンドを実行してからその他のキャプチャ設定を変更する必要があります。

- VLAN フィルタの設定時は、キャプチャの送信元または宛先は VLAN であることが必要です。ポート フィルタの設定時は、キャプチャの送信元または宛先はポートであることが必要です。

キャプチャの開始および停止

キャプチャを開始および停止するコマンドは、コンフィギュレーション設定として保存されていません。これらのコマンドは、コンソールから EXEC モードで実行されます。キャプチャをすぐに開始することも、キャプチャを開始する将来の日時を設定することもできます。次のいずれかの状況が発生すると、キャプチャが終了します。

- コンソールから、停止またはクリア コマンドが入力された。
- キャプチャ バッファがいっぱいになった（循環バッファとして設定されていない場合）。
- オプションで指定した秒数が経過した。
- オプションで指定したパケット数がキャプチャされた。

キャプチャが停止すると、SPAN セッションが終了し、キャプチャ セッションのパケットはプロセッサに転送されなくなります。

パケットのキャプチャを開始するときに、一部のコンフィギュレーション設定を上書きするかどうかを選択できます。

キャプチャを開始、停止、またはキャンセルするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **monitor capture** [**buffer size** *buf_size*][**length** *cap_len*][**linear** | **circular**][**filter** *acl_number* | *acl_name*] {**start** [**for** *count* (**packets** | **seconds**)] | **schedule at** *time date*}	オプションのランタイム設定を変更してキャプチャを開始します。キャプチャはただちに開始することも、指定した日時に開始することもできます。 • **buffer size** オプションでは、設定済みまたはデフォルトのキャプチャ バッファ サイズを上書きします。 • **length** オプションでは、各パケットからキャプチャするバイト数を決定します。*cap_len* の範囲は 0 ～ 9216 バイトで、デフォルトは 68 バイトです。値に 0 を指定すると、パケット全体がキャプチャされます。 • **circular** オプションは、キャプチャ バッファがいっぱいになった時点で、先に入力された項目から上書きするよう指定します。**linear** オプションは、キャプチャ バッファがいっぱいになった時点でキャプチャを停止するよう指定します。デフォルトは **linear** です。 • **filter** オプションにより、指定された ACL が適用されます。 • **for** オプションでは、指定した時間（単位：秒）が経過するか、または指定した数のパケットがキャプチャされたあと、キャプチャを停止するよう指定します。
ステップ 2	Router# **monitor capture stop**	キャプチャを停止します。
ステップ 3	Router# **monitor capture clear** [**filter**]	ランタイム コンフィギュレーション設定、保留中のスケジュール設定されたキャプチャ、およびキャプチャ バッファをクリアします。**filter** オプションを指定すると、ランタイム フィルタ設定だけがクリアされます。

上記のコマンドを使用する際は、次の点に注意してください。

- *time* および *date* の形式は、hh:mm:ss dd mmm yyyy です。時間は 24 時間表記で指定し、月は 3 文字の略語で指定します。たとえば、キャプチャの開始時刻を 2006 年 10 月 31 日の午後 7 時半に設定するには、19:30:00 31 oct 2006 と表記します。時間帯は、GMT で指定します。
- 開始コマンドでキャプチャ フィルタの ACL を使用する場合、設定済みの ACL が新しい ACL によって上書きされることはありません。新しい ACL はソフトウェアで実行されます。

キャプチャ バッファの表示およびエクスポート

キャプチャされたパケットまたはキャプチャ セッションに関する情報を表示したり、キャプチャされたパケットを分析用にエクスポートするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **show monitor capture**	キャプチャ セッションの設定を表示します。
ステップ 2	Router# **show monitor capture status**	キャプチャ セッションのステート、モード、パケットの統計情報を表示します。
ステップ 3	Router# **show monitor capture buffer** [*start* [*end*]] [**detail**][**dump** [*nowrap* [*dump_length*]] [**acl** *acl_number* | *acl_name*]]	キャプチャ バッファの内容を表示します。 • *start* および *end* パラメータでは、キャプチャ バッファ内のパケット番号インデックスを指定します。*start* インデックスが指定され、*end* インデックスが指定されていない場合、*start* インデックスの 1 つのパケットだけが表示されます。*start* および *end* インデックスがともに指定されている場合、これらのインデックス間にあるすべてのパケットが表示されます。指定できる範囲は 1 ～ 4294967295 です。 • **detail** オプションでは、各パケットについて、拡張およびフォーマットされたプロトコルとエンベロープ情報（パケットの到着時刻など）が追加されます。 • **dump** オプションは、パケットの内容を 16 進数で表示します。*nowrap* が *dump_length* とともに指定されている場合、パケットの内容を示す *dump_length* 文字の 16 進数が各パケットについて 1 行で表示されます。*dump_length* が指定されていない場合、72 文字の行が 1 行表示されます。*dump_length* の範囲は 14 ～ 256 です。 • **acl** オプションにより、指定された ACL に一致するパケットだけが表示されます。
ステップ 4	Router# **show monitor capture buffer** [*start* [*end*]] **brief** [**acl** *acl_number* | *acl_name*]	パケットのヘッダー情報だけを表示します。
ステップ 5	Router# **monitor capture export buffer** *url*	キャプチャ バッファの内容を指定されたファイル システムまたはファイル転送メカニズムにコピーします。

Mini Protocol Analyzer の設定、操作、表示例

ここでは、Mini Protocol Analyzer の設定、キャプチャ セッションの開始と停止、およびキャプチャ セッションの結果の表示の例をそれぞれ示します。

一般的な設定例

次に、Mini Protocol Analyzer の最小限の設定を行う例を示します。

```
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# end

Router# show mon cap
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

次に、バッファ サイズ、セッションの説明、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)# monitor session 1 type capture
Router(config-mon-capture)# buffer-size 4096
Router(config-mon-capture)# description “Capture from ports, no filtering.”
Router(config-mon-capture)# rate-limit 20000
Router(config-mon-capture)# end
Router#
Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x807
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68

Router#
```

次に、送信元をポートの混合リストとして設定する例を示します。

```
Router(config-mon-capture)# source interface gig 3/1 - 3 , gig 3/5
```

次に、送信元を VLAN の混合リストとして設定する例を示します。

```
Router(config-mon-capture)# source vlan 123,234-245
```

フィルタリング設定例

次に、次の属性を持つパケットをキャプチャするよう設定する例を示します。

- パケットは 123 または 234 ～ 245 の VLAN に所属
- パケットは 802.1Q EtherType（16 進数値 0x8100、10 進数値 33024）
- パケット サイズは 8192 バイト
- 送信元 MAC アドレスは 01:23:45:67:89:ab
- パケットは ACL 番号 99 に準拠

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 type capture
Router(config-mon-capture)# source vlan 123,234-245
Router(config-mon-capture)# filter ethertype 0x8100
Router(config-mon-capture)# filter length 8192
Router(config-mon-capture)# filter mac-address 0123.4567.89ab
Router(config-mon-capture)# filter access-group 99
Router(config-mon-capture)# end

Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 20000
redirect index     : 0x7E07
Capture vlan       : 1019
buffer-size        : 4194304
capture state      : OFF
capture mode       : Linear
capture length     : 68
Sw Filters          :
     ethertype   : 33024
     src mac     : 0123.4567.89ab
  Hw  acl          : 99

Router# show monitor session 1
Session 1
---------
Type                   : Capture Session
Description            : capture from ports
Source VLANs           :
    Both               : 123,234-245
Capture buffer size    : 4096 KB
Capture rate-limit
             value     : 20000
Capture filters        :
     ethertype         : 33024
     src mac           : 0123.4567.89ab
     acl               : 99

Egress SPAN Replication State:
Operational mode       : Centralized
Configured mode        : Distributed (default)

Router#
```

次に、サイズが 128 バイト未満のパケットをキャプチャする例を示します。

```
Router(config-mon-capture)# filter length 0 128
```

次に、サイズが 256 バイトを超えるパケットをキャプチャする例を示します。

```
Router(config-mon-capture)# filter length 256 9216
```

操作例

次に、キャプチャを開始および停止する例を示します。

```
Router# monitor capture start
Router# monitor capture stop
Router#
```

次に、キャプチャを開始して 60 秒後に停止する例を示します。

```
Router# monitor capture start for 60 seconds
Router#
```

次に、キャプチャを今後のある日時に開始する例を示します。

```
Router# monitor capture schedule at 11:22:33 30 jun 2008
capture will start at : <11:22:33 UTC Mon Jun 30 2008>  after 32465825 secs
Router#
```

次に、バッファ サイズを上書きして循環バッファに変更するオプションを指定して、キャプチャを開始する例を示します。

```
Router# monitor capture buffer size 65535 circular start
Router#
```

次に、キャプチャ バッファを外部サーバとローカル ディスクにエクスポートする例を示します。

```
Router# monitor capture export buffer tftp://server/user/capture_file.cap
Router# monitor capture export buffer disk1:capture_file.cap
```

表示例

次に、設定情報、セッションのステータス、およびキャプチャ バッファの内容を表示する例を示します。

コンフィギュレーションの表示

キャプチャ セッションの設定を表示するには、**show monitor capture** コマンドを入力します。

```
Router# show monitor capture
Capture instance [1] :
======================
Capture Session ID : 1
Session status     : up
rate-limit value   : 10000
redirect index     : 0x807
buffer-size        : 2097152
capture state      : OFF
capture mode       : Linear
capture length     : 68
```

次に、**show monitor session** *n* コマンドを使用して詳細を表示する例を示します。

```
Router# show monitor session 1
Session 1
---------
Type                  : Capture Session
Source Ports          :
    Both              : Gi3/1-3,Gi3/5
Capture buffer size   : 32 KB
Capture filters       : None

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Distributed (default)
```

次に、**show monitor session** *n* **detail** コマンドを使用して、全詳細を表示する例を示します。

```
Router# show monitor session 1 detail
Session 1
---------
Type                  : Capture Session
Description           : -
Source Ports          :
    RX Only           : None
    TX Only           : None
    Both              : Gi3/1-3,Gi3/5
Source VLANs          :
    RX Only           : None
    TX Only           : None
    Both              : None
Source RSPAN VLAN     : None
Destination Ports     : None
Filter VLANs          : None
Dest RSPAN VLAN       : None
Source IP Address     : None
Source IP VRF         : None
Source ERSPAN ID      : None
Destination IP Address : None
Destination IP VRF    : None
Destination ERSPAN ID  : None
Origin IP Address     : None
IP QOS PREC           : 0
IP TTL                : 255
Capture dst_cpu_id    : 1
Capture vlan          : 0
Capture buffer size   : 32 KB
Capture rate-limit
             value    : 10000
Capture filters       : None

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Distributed (default)
```

キャプチャ セッション ステータスの表示

キャプチャ セッション ステータスを表示するには、**show monitor capture status** コマンドを入力します。

```
Router# show monitor capture status
capture state      : ON
```

```
capture mode       : Linear
Number  of packets
          received : 253
           dropped : 0
          captured : 90
```

キャプチャ バッファの内容の表示

キャプチャ セッションの内容を表示するには、**show monitor capture buffer** コマンドを入力します。次に、このコマンドのいくつかのオプションを使用した場合の表示例を示します。

```
Router# show monitor capture buffer
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
 6     IP: s=10.12.0.1 , d=224.0.0.10, len 60


Router# show monitor capture buffer detail
 1      Arrival time : 09:44:30 UTC Fri Nov 17 2006
        Packet Length : 74 , Capture Length : 68
        Ethernet II :  0100.5e00.000a  0008.a4c8.c038  0800
        IP: s=10.12.0.5 , d=224.0.0.10, len 60, proto=88
 2      Arrival time : 09:44:31 UTC Fri Nov 17 2006
        Packet Length : 346 , Capture Length : 68
346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757463031


Router# show monitor capture buffer dump
 1     IP: s=10.12.0.5 , d=224.0.0.10, len 60
08063810:                       0100 5E00000A            ..^...
08063820: 0008A4C8 C0380800 45C0003C 00000000  ..$H@8..E@.<....
08063830: 0258CD8F 0A0C0005 E000000A 0205EE6A  .XM.....`.....nj
08063840: 00000000 00000000 00000000 00000064  ...............d
08063850: 0001000C 01000100 0000000F 0004      ..............
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F757465720415
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000000000800000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060400010012 44
 5     IP: s=7.0.84.23 , d=224.0.0.5, len 116
0806FCB0:                       0100 5E000005            ..^...
0806FCC0: 0015C7D7 AC000800 45C00074 00000000  ..GW,...E@.t....
0806FCD0: 01597D55 07005417 E0000005 0201002C  .Y}U..T.`......,
0806FCE0: 04040404 00000000 00000002 00000010  ................
0806FCF0: 455D8A10 FFFF0000 000A1201 0000      E]............


Router# show monitor capture buffer dump nowrap
 1     74    0100.5e00.000a  0008.a4c8.c038  0800 45C0003C000000
 2     346   0180.c200.000e  0012.44d8.5000  88CC 020707526F7574
 3     60    0180.c200.0000  0004.c099.06c5  0026 42420300000000
 4     60    ffff.ffff.ffff  0012.44d8.5000  0806 00010800060400
```

CHAPTER 63

Resilient Ethernet Protocol の設定

この章では、Cisco IOS Software Release 15.0(1)S で Resilient Ethernet Protocol を設定する方法について説明します。

この章の内容は次のとおりです。

- 「Resilient Ethernet Protocol の概要」（P.63-1）
- 「Resilient Ethernet Protocol の設定」（P.63-2）

Resilient Ethernet Protocol の概要

Resilient Ethernet Protocol（REP）は、シスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、イーサネット ネットワークでの L2 の復元力と高速フェールオーバーをサポートします。REP は次の機能を提供します。

- ネットワーク ループの制御
- リンク障害の処理
- コンバージェンス時間の短縮

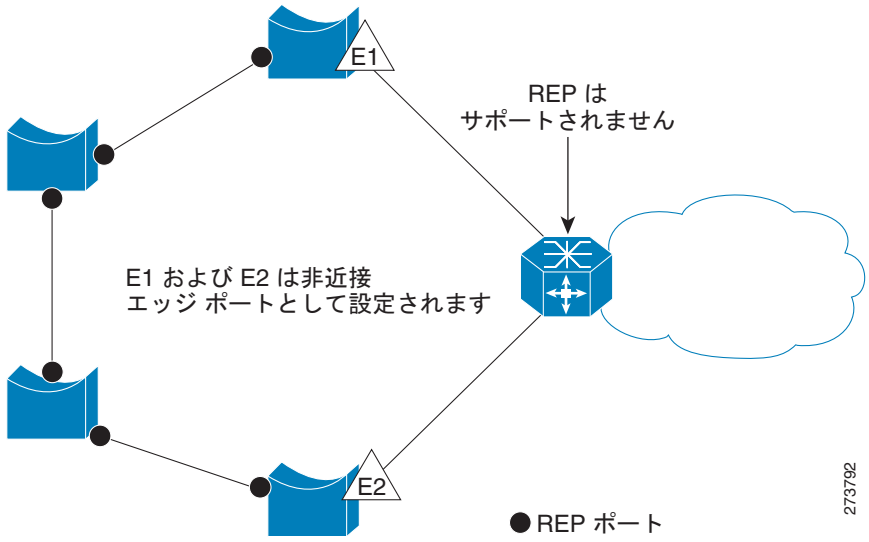
REP セグメントは、接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。REP はレイヤ 2 トランク インターフェイスおよび EVC ポートでサポートされます。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジング ループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。REP は、Cisco IP Next-Generation Network（NGN）キャリア イーサネット デザイン全体のネットワークの復元力を強化します。REP では、50 ～ 200 ミリ秒以内にネットワークおよびアプリケーションのコンバージェンスが実現するように設計されています。REP は既存のキャリア イーサネット ネットワークに容易に統合できるセグメント プロトコルです。これにより、ネットワーク設計者は STP ドメインの範囲を制限できます。また、REP は STP に対して潜在的なトポロジの変化を通知できるため、スパニングツリーとの相互運用も可能になります。

REP は分散型のセキュアなプロトコルで、リングのステータスを制御するマスター ノードを必要としません。したがって、障害の検出は、Loss of Signal（LOS; 信号消失）またはネイバーとの隣接関係の喪失によってローカルで行われます。どの REP ポートも、セキュア キーを取得し次第、代替ポートのブロックを解除して切替えを開始できます。REP セグメントは、相互接続されたポートのチェーンで、同じセグメント ID が設定されます。セグメントの各端はエッジ スイッチで終端します。セグメントが終端するポートはエッジ ポートと呼ばれます。

REP 非ネイバー エッジ

Cisco IOS Release 15.1.(01)S から有効になった新しい機能により、非 REP スイッチ側のポートを非ネイバー エッジ ポートとして設定できます。これらのポートはエッジ ポートの特性を継承し、障害発生時に迅速に収束できないという制限を克服します。

図 63-1　　非ネイバー エッジ ポート



アクセス リング トポロジでは、ネイバー スイッチで REP がサポートされていない場合があります（図 59-1 を参照）。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。その場合、送信される STP トポロジ変更通知（TCN）は、マルチ スパニングツリー（MST）STP メッセージになります。

Resilient Ethernet Protocol の設定

REP over Ethernet Virtual Circuit の設定については、http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html を参照してください。

Resilient Ethernet Protocol 設定可能タイマーの設定については、http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1607518 を参照してください。

CHAPTER 64

同期イーサネットと 1588V2 の設定

この章では、Cisco IOS Software Release 15.0(1)S で同期イーサネットと 1588V2 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 の『Cisco 7600 Series Router Cisco IOS Command Reference』を参照してください。
http://www.cisco.com/en/US/products/ps6922/prod_command_reference_list.html

この章の内容は次のとおりです。

- 「同期イーサネットについて」（P.64-1）
- 「Cisco 7600 ルータでの同期イーサネットの設定」（P.64-5）
- 「ネットワーク クロッキング」（P.64-22）
- 「ネットワーク クロッキングの設定方法」（P.64-24）
- 「1588V2 について」（P.64-29）
- 「1588V2 マスターでの ToD の設定」（P.64-33）
- 「1588V2 スレーブでの ToD の設定」（P.64-34）

同期イーサネットについて

Synchronous Ethernet（SyncE; 同期イーサネット）は、SONET または SDH でタイミングを渡すのと同じ方法でノードからノードへタイミングを渡すために物理レイヤ インターフェイスを使用する手順です。SyncE は G.8261、G.8262、G.8264、G.781 などの ITU-T 標準により定義され、イーサネットの PHY レイヤを使用してリモート サイトに周波数を送信します。SyncE over Ethernet は、費用対効果に優れた代替手段をネットワークに提供します。SyncE を機能させるには、同期パスの各ネットワーク要素が SyncE をサポートしている必要があります。

2 ポート ギガビット同期イーサネット SPA には、同期供給ユニット（SSU）からクロックを回復する BITS インターフェイスと呼ばれる専用の外部インターフェイスがあります。7600 ルータは SyncE に対してこのクロックを使用します。BITS インターフェイスは、E1（ヨーロッパ SSU）および T1（アメリカ BITS）フレーミングをサポートします。表 64-1 に、2 ポート ギガビット同期イーサネット SPA の BITS ポートに対するフレーミング モードを示します。

表 64-1　BITS ポートに対するフレーミング モード

BITS/SSU ポート サポート マトリクス	サポートされるフレーミング モード	SSM/QL サポート	Tx ポート	Rx ポート
T1	T1 ESF	Yes	Yes	Yes
T1	T1 SF	No	Yes	Yes
E1	E1 CRC4	Yes	Yes	Yes
E1	E1 FAS	No	Yes	Yes
E1	E1 CAS	No	No	Yes
E1	E1 CAS CRC4	Yes	No	Yes
2048kHz	2048kHz	No	Yes	Yes

Cisco 7600 ルータでは、SyncE を次の 4 つの異なる設定で実装できます。

- SyncE からのクロック回復：システム クロックが SyncE クロッキング ソースから回復されます（ギガビット インターフェイスおよび 10 ギガビット インターフェイスのみ）。ルータは、他の SyncE インターフェイスまたは ATM/CEoP インターフェイスに対してこのクロックを Tx クロックとして使用します。
- 外部インターフェイスからのクロック回復：システム クロックが BITS クロッキング ソースまたは GPS インターフェイスから回復されます（2 ポート ギガビット同期イーサネット SPA の場合）。
- 外部へのライン：イーサネットから受信されたクロックが外部の Synchronization Supply Unit（SSU; 同期供給ユニット）に転送されます。同期チェーン中に、受信されたクロックでは、許可されない誤動作およびジッターが発生することがあります。ルータは SyncE インターフェイスからクロックを回復し、BITS インターフェイスに必要な形式に変換し、BITS ポートから SSU に送信します。SSU は、クリーンアップを実行し、BITS インターフェイスにクロックを返します。このクロックは、SyncE ポートに対する Tx クロックとして使用されます。
- 外部へのシステム：システム クロックが、外部インターフェイスに対する Tx クロックとして使用されます。デフォルトでは、システム クロックは外部インターフェイスで送信されません。

ネットワーク クロッキングは、次のラインカードでサポートされます。

  - ES+
  - ITU-T G.709 DWDM 光インターフェイスがある 4x10GE または 2x10GE
  - SIP-400 上の 2 ポート ギガビット同期イーサネット SPA
  - ATM SPA（SPA-2xOC3-ATM、SPA-4xOC3-ATM、SPA-1xOC12-ATM、SPA-1xOC48-ATM、SPA-1xOC3-ATM-V2、SPA-2xOC3-ATM-V2、SPA-3xOC3-ATM-V2、SPA-1xOC12-ATM-V2）
  - CEoP SPA（-SPA-1CHOC3-CE-ATM、SPA-24CHT1-CE-ATM）
  - POS SPA（SPA-2xOC3-POS、SPA-4xOC3-POS、SPA-1xOC12-POS、SPA-2xOC12-POS）
  - チャネライズド SPA（8 ポート チャネライズド T1/E1 SPA、1 ポート チャネライズド OC3/STM-1 SPA）

スケルチング

スケルチングは、クロック ソースがダウンしたときに、必ず Alarm Indication Signal（AIS; アラーム検出信号）が Tx インターフェイスに送信されるプロセスです。スケルチング機能は、次の 2 つの場合に実装されます。

- 外部へのライン：ライン ソースがダウンした場合に、AIS が外部インターフェイスで SSU に送信されます。
- 外部へのシステム：ルータがすべてのクロック ソースを失った場合に、AIS が外部インターフェイスで SSU に送信されます。

スケルチングは、SSU や Primary Reference Clock（PRC）などの外部デバイスでのみ実行されます。

SSM および ESMC

ネットワーク クロッキングは、次のメカニズムを使用してネットワーク要素間でクロックの品質レベルを交換します。

- 同期ステータス メッセージ
- イーサネット同期メッセージング チャネル

同期ステータス メッセージ

ネットワーク要素は、Synchronization Status Message（SSM; 同期ステータス メッセージ）を使用して隣接する要素にクロックの Quality Level（QL; 品質レベル）について通知します。光インターフェイスや SONET/T1/E1 SPA フレーマなどの非イーサネット インターフェイスは SSM を使用します。SSM 機能の主な利点は次のとおりです。

- タイミング ループが回避されます。
- ネットワークの一部で障害が発生した場合に迅速に回復が行われます。
- ノードが、最も信頼性が高いクロック ソースからタイミングを派生させます。

イーサネット同期メッセージング チャネル

同期ネットワーク接続で論理通信チャネルを保持するために、イーサネットは、IEEE 802.3 Organization Specific Slow Protocol 標準に基づいた Ethernet Synchronization Messaging Channel（ESMC）と呼ばれるチャネルに依存します。ESMC は、物理レイヤの Ethernet Equipment Clock（EEC）の品質レベルを表す SSM コードをリレーします。

ESMC パケットは、クロック ソースとして設定されたポートに対してのみ受信され、システムのすべての SyncE インターフェイスで送信されます。これらのパケットは、RP でクロック選択アルゴリズムによって処理され、最良のクロックを選択するために使用されます。Tx フレームは、選択されたクロック ソースの QL 値に基づいて生成され、すべてのイネーブルな SyncE ポートに送信されます。

クロック選択アルゴリズム

クロック選択アルゴリズムは、指定されたソースから最良の利用可能な同期ソースを選択します。クロック選択アルゴリズムでは、同じ QL 値を持つクロック ソース間で非リバーティブな動作が発生し、最良の QL 値を持つ信号が常に選択されます。クロック オプション 1 の場合、デフォルト値はリバーティブであり、クロック オプション 2 の場合、デフォルト値は非リバーティブです。

クロック選択プロセスは、QL-enabled モードと QL-disabled モードで動作します。1 つのネットワーク要素で複数の選択プロセスが存在する場合、すべてのプロセスは同じモードで動作します。

QL-enabled モード

QL-enabled モードでは、次のパラメータが選択プロセスに関係します。

- 品質レベル

- QL-FAILED による信号失敗
- プライオリティ
- 外部コマンド

外部コマンドがアクティブでない場合は、アルゴリズムにより、信号失敗の状況が発生しない、品質レベルが最高である基準（クロック選択用）が選択されます。複数の入力の品質レベルが同等に最高である場合、最大の優先度を持つ入力が選択されます。複数の入力の優先度が同等に最大であり、品質レベルが同等に最高である場合、既存の基準は保持されます（基準がこのグループに属する場合）。その他の場合は、このグループから任意の基準が選択されます。

QL-disabled モード

QL-disabled モードでは、次のパラメータが選択プロセスに関係します。

- 信号失敗
- プライオリティ
- 外部コマンド

外部コマンドがアクティブでない場合は、アルゴリズムにより、信号失敗の状況が発生しない、優先度が最大である基準（クロック選択用）が選択されます。複数の入力の優先度が同等に最大である場合、既存の基準は保持されます（基準がこのグループに属する場合）。その他の場合は、このグループから任意の基準が選択されます。

ハイブリッド モード

SyncE 機能では、同期パスの各ネットワーク要素が SyncE をサポートする必要があります。Timing over Packet（ToP）により、非同期ネットワーク介したタイミングの転送が可能になります。ハイブリッド モードは、1588（PTP）から派生したクロックを使用してシステム クロックを動作させます。これは、入力ソースとして PTP スレーブの Timing over Packet（ToP）インターフェイスを設定することにより実現されます。1588v2 の概要については、http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76oveth.html#wp1061862 を参照してください。

（注）　ToP インターフェイスは、QL をサポートせず、QL-disabled モードでのみ動作します。

制約事項および使用上の注意事項

ES40 ラインカードで SyncE を設定する場合は、次の制約事項および使用上の注意事項に従ってください。

- ネットワーク クロック アルゴリズムがイネーブルな場合、ルータのすべての ES+ カードがシステム クロックをイーサネット インターフェイスの Tx クロック（同期モード）として使用します。ラインカードでは、同期モードをインターフェイスごとに変更することはできません。ラインカード全体が同じモードで動作します。
- ES+ カードでは、クロック ソースとして 1 度に最大 4 つのポートを設定できます。
- 20x1 ギガビット ES+ ラインカードの場合、各 NPU から最大 2 つのポートを選択できます。
- 40x1 ギガビット ES+ ラインカードの場合、各 NPU からポートを 1 つだけ選択できます。
- Cisco 7600 ルータでは、クロック ソースとして最大 6 つのポートを設定できます。
- クロック クリーンアップに対する外部へのラインは、ライン インターフェイスと外部（BITS）インターフェイスが同じ ES+ ラインカードに存在する場合のみサポートされます。

- SyncE 機能は SSO と共存しますが、SSO に準拠しません。クロック選択アルゴリズムは、スイッチオーバーで再び開始されます。スイッチオーバー中に、ルータはホールドオーバー モードになります。
- QL-enabled クロック選択で、WAN モードの ES+ SyncE インターフェイスを使用することはできません。QL-disabled モードのシステムでこれらのインターフェイスを使用するか、これらのインターフェイスで ESMC をディセーブルにし、これらのインターフェイスを QL-disabled インターフェイスとして使用する必要があります。
- TSM スイッチング遅延に影響が出るため、同じ優先度を持つ複数の入力ソースを設定しないことが推奨されます。
- ネットワーククロック ベースのクロック選択アルゴリズムと新しいアルゴリズムを同時に実装することはできません。これら両方のアルゴリズムは同時に使用できません。
- SyncE は、1 ギガビット イーサネット銅製 SFP（SFP GE-T および GLC-T）でサポートされません。

Cisco 7600 ルータでの同期イーサネットの設定

ここでは、ES+ ラインカードがある Cisco 7600 ルータで SyncE を設定する方法について説明します。SyncE は、次の 4 つの異なる設定を使用して Cisco 7600 ルータで実装されます。

- 「SyncE からのクロック回復の設定」（P.64-5）
- 「BITS ポートからのクロック回復の設定」（P.64-7）
- 「外部へのシステムの設定」（P.64-9）
- 「外部へのラインの設定」（P.64-10）

SyncE からのクロック回復の設定

ここでは、SyncE からのクロック回復の方法を使用して、Cisco 7600 ルータの ES+ カードを介して SyncE を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock synchronization ssm option** *option_Id Generation_Id*
5. **interface gigabitethernet** slot/port **or interface tengigabitethernet** slot/port
6. **[no]clock source** {internal | line | loop}
7. **synchronous mode**
8. **exit**
9. **network-clock input-source** *priority* {**interface** *interface_name slot/card/port* | {**external** *slot/card/port* }}
10. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** Router# enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** 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	**network-clock synchronization automatic** **例：** Router(config)# network-clock synchronization automatic	ネットワーク クロック選択アルゴリズムをイネーブルにします。このコマンドを実行すると、シスコ固有のネットワーククロック プロセスがディセーブルになり、G.781 ベースの自動クロック選択プロセスが有効になります。
ステップ 4	**network-clock synchronization ssm option** {*option_id* {*GEN1* | *GEN2*}} **例：** Router(config)# network-clock synchronization ssm option 2 GEN1	装置が同期ネットワークで動作するよう設定します。*option_id* 値 1 は、ヨーロッパの同期ネットワーク設計を表します。これがデフォルト値です。*option_id* 値 2 は、米国の同期ネットワーク設計を表します。
ステップ 5	**interface gigabitethernet** *slot/port* **or interface tengigabitethernet** *slot/port* **例：** Router(config)# int gig 5/1	設定するギガビット イーサネットまたは 10 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。 *slot/port* : インターフェイスの場所を指定します。
ステップ 6	**clock source** {*internal* | *line* | *loop*} **例：** Router(config-if)# clock source line	使用するクロック ソースを指定します。クロック ソースの 3 つのオプションは次のとおりです。 • internal : 内部クロックを使用します。 • line : ラインからクロックを回復します。 • loop : ローカル ループ タイミングを使用します。 SYNCE を実装するには、*line* オプションを使用します。
ステップ 7	**synchronous mode** **例：** Router(config-if)# synchronous mode	モードを同期モードに設定します。

	コマンド	目的
ステップ 8	**exit** **例：** `Router(config)# exit`	特定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 9	**network-clock input-source** *priority* {**interface** *interface_name slot/card/port* | **{external** *slot/card/port* }} **例：** `Router(config)# network-clock input-source 1 interface TenGigabitEthernet7/1`	SyncE からのクロック回復をイネーブルにします。
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

例

次に、Cisco 7600 ルータで SyncE からのクロック回復を設定する例を示します。

```
Router>enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# int gig 5/1
Router(config-if)# clock source line
Router(config-if)# synchronous mode
Router(config)# exit
Router(config)# network-clock input-source 1 interface TenGigabitEthernet7/1
Router(config)# exit
```

BITS ポートからのクロック回復の設定

ここでは、BITS ポートからのクロック回復を使用して、Cisco 7600 ルータの ES+ カードを介して SyncE を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock synchronization ssm option** *option_Id Generation_Id*
5. **network-clock input-source** *priority* {**interface** *interface_name slot*/*card*/*port* | {**external** *slot*/*card*/*port* }}

6. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**network-clock synchronization automatic** **例：** `Router(config)# network-clock synchronization automatic`	ネットワーク クロック選択アルゴリズムをイネーブルにします。このコマンドを実行すると、シスコ固有のネットワーククロック プロセスがディセーブルになり、G.781 ベースの自動クロック選択プロセスが有効になります。
ステップ 4	**network-clock synchronization ssm option** {*option_id* {*GEN1* | *GEN2*}} **例：** `Router(config)# network-clock synchronization ssm option 2 GEN1`	装置が同期ネットワークで動作するよう設定します。*option_id* 値 1 は、ヨーロッパの同期ネットワーク設計を表します。これがデフォルト値です。*option_id* 値 2 は、米国の同期ネットワーク設計を表します。
ステップ 5	**network-clock input-source** *priority* {**interface** *interface_name slot/card/port* | **{external** *slot/card/port* }} **例：** `Router(config-if-srv)# network-clock input-source 1 External 7/0/0 t1 sf`	BITS ポートからのクロック回復をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

例

次に、Cisco 7600 ルータで BITS ポートからのクロック回復を設定する例を示します。

```
Router>enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
```

```
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
Router(config)# exit
```

外部へのシステムの設定

ここでは、外部へのシステムの方法を使用して、Cisco 7600 ルータの ES+ カードを介して SyncE を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock synchronization ssm option** *option_Id Generation_Id*
5. **network-clock output-source system** *priority* {**external** *slot*/*card*/*port* [*j1* | *2m* | *10m*] }
6. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**network-clock synchronization automatic** **例：** `Router(config)# network-clock synchronization automatic`	ネットワーク クロック選択アルゴリズムをイネーブルにします。このコマンドを実行すると、シスコ固有のネットワーククロック プロセスがディセーブルになり、G.781 ベースの自動クロック選択プロセスが有効になります。
ステップ 4	**network-clock synchronization ssm option** {*option_id* {*GEN1* | *GEN2*}} **例：** `Router(config)# network-clock synchronization ssm option 2 GEN1`	装置が同期ネットワークで動作するよう設定します。*option_id* 値 1 は、ヨーロッパの同期ネットワーク設計を表します。これがデフォルト値です。*option_id* 値 2 は、米国の同期ネットワーク設計を表します。

	コマンド	目的
ステップ 5	**network-clock output-source system** *priority* {**external** *slot*/*card*/*port* [*j1* | *2m* | *10m*]} **例：** `Router(config)# network-clock output-source system 1 external 4/0/0 t1 sf`	外部の Tx インターフェイスで使用されるシステム クロックを設定します。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

例

次に、Cisco 7600 ルータで外部クロッキングへのシステムを設定する例を示します。

```
Router>enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
Router(config)# exit
```

次に、SSU を使用してクロック クリーンアップを設定する例を示します。

```
Router(config)# network-clock output-source line 1 interface GigabitEthernet1/11 External
1/0/0 t1 sf
Router(config)# network-clock input-source 1 External 7/0/0 t1 sf
```

外部へのラインの設定

ここでは、外部へのラインの方法を使用して、Cisco 7600 ルータの ES+ カードを介して SyncE を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock synchronization ssm option** *option_Id Generation_Id*
5. **interface gigabitethernet** slot/port **or interface tengigabitethernet** slot/port
6. **[no]clock source** {internal | line | loop}
7. **synchronous mode**
8. **exit**
9. **network-clock output-source line** *priority* **{interface** *interface_name* **| controller** {*t1* | *e1*} *slot*/*card*/*port*}} {**external** *slot*/*card*/*port*}

10. exit

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**network-clock synchronization automatic** **例：** `Router(config)# network-clock synchronization automatic`	ネットワーク クロック選択アルゴリズムをイネーブルにします。このコマンドを実行すると、シスコ固有のネットワーククロック プロセスがディセーブルになり、G.781 ベースの自動クロック選択プロセスが有効になります。
ステップ 4	**network-clock synchronization ssm option** {*option_id* {*GEN1* | *GEN2*}} **例：** `Router(config)# network-clock synchronization ssm option 2 GEN1`	装置が同期ネットワークで動作するよう設定します。*option_id* 値 1 は、ヨーロッパの同期ネットワーク設計を表します。これがデフォルト値です。*option_id* 値 2 は、米国の同期ネットワーク設計を表します。
ステップ 5	**interface gigabitethernet** *slot/port* **or interface tengigabitethernet** *slot/port* **例：** `Router(config)# int gig 5/1`	設定するギガビット イーサネットまたは 10 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。 *slot/port*：インターフェイスの場所を指定します。
ステップ 6	**clock source** {*internal* | *line* | *loop*} **例：** `Router(config-if)# clock source line`	使用するクロック ソースを指定します。クロック ソースの 3 つのオプションは次のとおりです。 • internal：内部クロックを使用します。 • line：ラインからクロックを回復します。 • loop：ローカル ループ タイミングを使用します。 SYNCE を実装するには、*line* オプションを使用します。
ステップ 7	**synchronous mode** **例：** `Router(config-if)# synchronous mode`	モードを同期モードに設定します。

	コマンド	目的
ステップ 8	**exit** **例：** `Router(config)# exit`	特定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 9	**network-clock output-source line** *priority* {**interface** *interface_name* | **controller** {*t1* | *e1*} *slot*/*card*/*port*}} {**external** *slot*/*card*/*port*} **例：** `Router(config-if-srv)# encapsulation dot1q 40 second-dot1q 42`	外部の Tx インターフェイスで使用されるライン クロックを設定します。
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

例

次に、Cisco 7600 ルータで SyncE からのクロック回復を設定する例を示します。

```
Router>enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
Router(config)# network-clock input-source 1 interface TenGigabitEthernet7/1
Router(config)# int gig 5/1
Router(config-if)# clock source line
Router(config-if)# synchronous mode
Router(config)# exit
Router(config)# network-clock output-source line 1 interface GigabitEthernet1/11 External 1/0/0
Router(config)# exit
```

ES+ カードでの同期の管理

次の管理コマンドを使用して、ES+ カードで同期を管理します。

- 品質レベルがイネーブルなクロック選択：グローバル コンフィギュレーション モードで **network-clock synchronization mode QL-enabled** コマンド を使用して、QL-enabled モードの自動選択プロセスを設定します。これは、SyncE インターフェイスが SSM を送信できる場合にのみ成功します。次に、グローバル コンフィギュレーション モードでネットワーク クロック同期（QL-enabled モード）を設定する例を示します。

  ```
  Router(config)# network-clock synchronization mode QL-enabled
  ```

- ESMC プロセス : グローバル コンフィギュレーション モードで **esmc process** コマンドを使用してシステム レベルで ESMC プロセスをイネーブルにします。コマンドの no 形式を使用すると、ESMC プロセスがディセーブルになります。プラットフォームに SyncE 対応インターフェイスがインストールされてない場合、このコマンドは失敗します。次に、グローバル コンフィギュレーション モードで ESMC をイネーブルにする例を示します。

```
Router(config)# esmc process
```

- ESMC モード : インターフェイス コンフィギュレーション モードで **esmc mode** [*tx* | *rx* |<*cr*>] コマンドを使用してインターフェイス レベルで ESMC プロセスをイネーブルにします。コマンドの no 形式を使用すると、ESMC プロセスがディセーブルになります。次に、インターフェイス コンフィギュレーション モードで ESMC をイネーブルにする例を示します。

```
Router(config-if)# esmc mode tx
```

- ネットワーク クロック ソースの品質レベル : インターフェイス コンフィギュレーション モードで **network-clock source quality-level** コマンドを使用して gigabitethernet ポートの ESMC に対して QL 値を設定します。この値は、グローバル インターワーキング オプションに基づきます。
  - オプション 1 が設定された場合、利用可能な値は QL-PRC、QL-SSU-A、QL-SSU-B、QL-SEC、および QL-DNU です。
  - オプション 2 が GEN 2 で設定された場合、利用可能な値は QL-PRS、QL-STU、QL-ST2、QL-TNC、QL-ST3、QL-SMC、QL-ST4、および QL-DUS です。
  - オプション 2 が GEN1 で設定された場合、利用可能な値は QL-PRS、QL-STU、QL-ST2、QL-SMC、QL-ST4、および QL-DUS です。

  グローバル コンフィギュレーション モードで **network-clock quality-level** コマンドを使用して BITS ポートの SSM に対して QL 値を設定します。次に、グローバル コンフィギュレーション モードで **network-clock quality-level** を設定する例を示します。

```
Router(config)# network-clock quality-level rx QL-PRC interface ToP3/0/20
```

  次に、インターフェイス コンフィギュレーション モードで network-clock source quality-level を設定する例を示します。

```
Router(config-if)# network-clock source quality-level QL-PRC
```

- wait-to-restore : **network-clock wait-to-restore** *timer* **global** コマンドを使用して wait-to-restore 時間を設定します。wait-to-restore 時間は 0 ～ 86400 秒の間で設定できます。デフォルト値は 300 秒です。wait-to-restore タイマーは、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで設定できます。次に、グローバル コンフィギュレーション モードで wait-to-restore タイマーを設定する例を示します。

```
Router(config)# network-clock wait-to-restore 10 global
```

  次に、インターフェイス コンフィギュレーション モードで wait-to-restore タイマーを設定する例を示します。

```
Router(config)# int ten 7/1
Router(config-if)# network-clock wait-to-restore 10
```

- ホールドオフ時間 : **network-clock hold-off** *timer* **global** コマンドを使用してホールドオフ時間を設定します。ホールドオフ時間は、ゼロまたは 50 ～ 10000 ミリ秒の間の任意の値に設定できます。デフォルト値は 300 ミリ秒です。**network-clock hold-off** *timer* は、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで設定できます。次に、hold-off 時間を設定する例を示します。

```
Router(config)# network-clock hold-off 50 global
```

- 強制スイッチ：**network-clock switch force** コマンドを使用して、ソースが利用可能であるか、または範囲内にあるかに関係なく同期ソースを強制的に選択します。次に、手動スイッチを設定する例を示します。

```
Router(config)# network-clock switch force interface tenGigabitEthernet 7/1 t1
```

- 手動スイッチ：**network-clock switch manual** コマンドを使用して、ソースが利用可能であり、範囲内にある場合に、同期ソースを手動で選択します。次に、手動スイッチを設定する例を示します。

```
Router(config)# network-clock switch manual interface tenGigabitEthernet 7/1 t1
```

- 手動および強制スイッチのクリア：**network-clock clear switch controller-id** コマンドを使用して手動および強制スイッチをクリアします。次に、スイッチをクリアする例を示します。

```
Router(config)# network-clock clear switch t0
```

- ソースのロックアウト：**network-clock set lockout** コマンドを使用してクロック ソースをロックアウトします。ロックアウトと示されたクロック ソースは SyncE に対して選択されません。ソースに対するロックアウトをクリアするには、**network-clock clear lockout** コマンドを使用します。次に、クロック ソースをロックアウトする例を示します。

```
Router(config)# network-clock set lockout interface tenGigabitEthernet 7/1
```

次に、クロック ソースに対するロックアウトをクリアする例を示します。

```
Router(config)# network-clock clear lockout interface tenGigabitEthernet 7/1
```

検証

SyncE 設定を検証するには、次のコマンドを使用します。

- 出力例を表示するには、**show network-clock synchronization** コマンドを使用します。

```
Router# show network-clocks synchronization
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : TenGigabitEthernet12/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No

Nominated Interfaces

 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*Te12/1               NA          Sync/En      1     QL-PRC    -         -
```

```
 AT6/0/0              NA          NA/En        1     QL-SSU-A  NA        NA
```

- グローバル レベルおよびインターフェイス レベルでネットワーククロック同期パラメータの全詳細を表示するには、**show network-clock synchronization detail** コマンドを使用します。

```
Router# show network-clocks synchronization detail
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : TenGigabitEthernet12/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 300 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 2
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (sf_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A
(ql_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A
(sf_change)-> 1A (ql_change)-> 1A

Nominated Interfaces

 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*Te12/1               NA          Sync/En      1     QL-PRC    -         -
 AT6/0/0              NA          NA/En        1     QL-SSU-A  NA        NA

Interface:
-----------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: Disable
SSM Rx: Disable
Priority: 251
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE

Local Interface: Te12/1
Signal Type: NA
Mode: Synchronous(Ql-enabled)
ESMC Tx: Enable
ESMC Rx: Enable
Priority: 1
QL Receive: QL-PRC
QL Receive Configured: -
```

```
QL Receive Overrided: -
QL Transmit: QL-DNU
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE

Local Interface: AT6/0/0
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: Enable
SSM Rx: Enable
Priority: 1
QL Receive: QL-SSU-A
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
```

- 出力例を表示するには、**show esmc** コマンドを使用します。

```
Router# show esmc
Interface: TenGigabitEthernet12/1
  Administative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-PRC
    QL Transmit: QL-DNU
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second

Interface: TenGigabitEthernet12/2
  Administative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-DNU
    QL Transmit: QL-DNU
    QL rx overrided: QL-DNU
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
```

- グローバル レベルおよびインターフェイス レベルで esmc パラメータの全詳細を表示するには、**show esmc detail** コマンドを使用します。

```
Router# show esmc detail
```

```
Interface: TenGigabitEthernet12/1
  Administative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-PRC
    QL Transmit: QL-DNU
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
    ESMC Tx Timer: Running
    ESMC Rx Timer: Running
    ESMC Tx interval count: 1
    ESMC INFO pkts in: 2195
    ESMC INFO pkts out: 6034
    ESMC EVENT pkts in: 1
    ESMC EVENT pkts out: 16

Interface: TenGigabitEthernet12/2
  Administrative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-DNU
    QL Transmit: QL-DNU
    QL rx overrided: QL-DNU
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
    ESMC Tx Timer: Running
    ESMC Rx Timer: Running
    ESMC Tx interval count: 1
    ESMC INFO pkts in: 0
    ESMC INFO pkts out: 2159
    ESMC EVENT pkts in: 0
ESMC EVENT pkts out: 10
```

（注）　SyncE インターフェイスの設定、その設定の検証、および 2 ポート ギガビット同期イーサネット SPA のトラブルシューティングについては、http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgeth.html#wpxref24513 を参照してください。

同期イーサネット設定のトラブルシューティング

Cisco 7600 ES+ ラインカードで同期イーサネット設定をトラブルシューティングする場合は、次のデバッグ コマンドが利用可能です。

デバッグ コマンド	目的
debug platform ssm	Rx 値、Tx 値、QL 値などの、SSM に関するデバッグ問題。
debug platform network-clock	正しく選択されなかったアラーム、OOR、active-standby ソースなどの、ネットワーク クロックに関するデバッグ問題。
debug esmc error **debug esmc event** **debug esmc packet** [**interface** *<interface name>*] **debug esmc packet rx** [**interface** *<interface name>*] **debug esmc packet tx** [**interface** *<interface name>*]	ESMC パケットが適切な品質レベル値で送受信されるかどうかを検証します。

トラブルシューティング シナリオ

（注）　トラブルシューティングを行う前に、すべてのネットワーク クロック同期設定が完了していることを確認します。

トラブルシューティング

表 64-2 には、同期イーサネット機能のトラブルシューティング ソリューションが記載されています。

表 64-2　トラブルシューティング シナリオ

問題	ソリューション

不適切なクロック制限が設定されたか、またはキュー制限モードがディセーブルになっています。	• インターフェイスでアラームが存在しないことを確認します。確認するには、**show network-clock synchronization detail** RP コマンドを使用します。
	
	警告　これらのデバッグ コマンドを TAC の管理下にない状態で使用することは推奨されません。
	
	• **show network-clock synchronization** コマンドを使用して、次の例に示されたように、システムがリバーティブ モードであるか、または非リバーティブ モードであるかを確認し、非リバーティブ設定を検証します。
	
	`RouterB#show network-clocks synchronization`
	`Symbols: En - Enable, Dis - Disable, Adis - Admin Disable NA - Not Applicable`
	`- Synchronization source selected`
	`# - Synchronization source force selected`
	`& - Synchronization source manually switched`
	`Automatic selection process : Enable`
	`Equipment Clock : 1544 (EEC-Option2)`
	`Clock Mode : QL-Enable`
	`ESMC : Enabled`
	`SSM Option : GEN1`
	`T0 : POS3/1/0`
	`Hold-off (global) : 300 ms`
	`Wait-to-restore (global) : 0 sec`
	`Tsm Delay : 180 ms`
	`Revertive : Yes<<<<If it is non revertive then it will show NO here.`
	`Nominated Interfaces`
	`Interface SigType Mode/QL Prio QL_IN ESMC Tx ESMC Rx`
	`Internal NA NA/Dis 251 QL-ST3 NA NA`
	`SONET 3/0/0 NA NA/En 3 QL-ST3 NA NA`
	`*PO3/1/0 NA NA/En 1 QL-ST3 NA NA`

問題	ソリューション
	SONET 2/3/0 NA NA/En 4 QL-ST3 NA NA
	• **debug network-clock errors**、**debug network-clock event**、および **debug network-clock sm** RP コマンドを使用して、現在の問題を再現し、ログを収集します。 **警告　これらのデバッグ コマンドを TAC の管理下にない状態で使用することは推奨されません。** • 問題が解消されない場合は、Technical Assistance Center（TAC）にご連絡ください。

問題	ソリューション
show network-clock synchronization detail コマンドを使用した場合に、品質レベル（QT）値が不適切です。	• **network clock synchronization SSM**（*option 1* |*option 2*）コマンドを使用して、フレーミングの不一致がないことを確認します。**show run interface** コマンドを使用して、特定のインターフェイスのフレーミングを検証します。SSM オプション 1 の場合、フレーミングは SDH または E1 である必要があり、SSM オプション 2 の場合、フレーミングは SONET または T1 である必要があります。 • **debug network-clock errors**、**debug network-clock event**、および **debug platform ssm** RP コマンドを使用して問題を再現するか、**debug hw-module subslot** コマンドをイネーブルにします。 **警告**　**これらのデバッグ コマンドを TAC の管理下にない状態で使用することは推奨されません。**
エラー メッセージ「%NETCLK-6-SRC_UPD: Synchronization source SONET 2/3/0 status (Critical Alarms(OOR)) is posted to all selection process」が表示されます。	• アラームまたは OOR があるインターフェイスは、キュー制限または優先度が大きい場合でも、選択プロセスの一部となることはできません。**debug platform network-clock** RP コマンドを使用してネットワーク クロックの問題をトラブルシューティングします。 • ルート プロセッサでイネーブルな **debug platform network-clock** コマンドを使用して問題を再現するか、**debug network-clock event** RP コマンドおよび **debug network-clock errors** RP コマンドをイネーブルにします。 **警告**　**これらのデバッグ コマンドを TAC の管理下にない状態で使用することは推奨されません。**

ネットワーク クロッキング

76-ES+XT-2TG3CXL ラインカードおよび 76-ES+XT-4TG3CXL ラインカードのネットワーク クロッキング サポートは、SIP-200 ラインカードおよび SIP-400 ラインカードを使用する既存のネットワーク クロッキング機能を基に構築されています。SIP-200 ラインカードおよび SIP-400 ラインカードの SPA インターフェイスによって提供される元のネットワーク クロック ソースはすべて、従来どおりに動作します。また、76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL のネットワーク クロッキング サポートを使用して次のものを設定できます。

- BITS クロック ソース
- 10GE インターフェイスのクロック ソース

これらの機能拡張によって、サービス プロバイダー アプリケーションに対する Synchronous Ethernet（SyncE; 同期イーサネット）機能のサポートが提供され、キャリア イーサネット環境で 76-ES+XT-2TG3CXL ラインカードおよび 76-ES+XT-4TG3CXL ラインカードが推奨される選択肢となります。

76-ES+XT-2TG3CXL ラインカードまたは 76-ES+XT-4TG3CXL ラインカードは、クロック同期に対して設定や現在のソース状態に応じて 3 つの異なるモードで動作します。

- フリーランニング：ネットワーク クロッキングに参加していないラインカード、またはクロックのアクティブ ソースとなっているラインカードは、フリーランニング モードで動作します。このモードでは、ラインカードの内部発振器がバックプレーンへの基準クロックを生成します。

（注）　不参加モードまたはディセーブル モードでは、ラインカードは Stratum 3 品質タイミング信号を外部基準クロックに配信します。別のラインカードにある他のインターフェイスは、それぞれの設定に応じて、バックプレーン基準クロックまたは外部基準クロックのいずれかを受信します。

（注）　ラインカードは、システム クロッキングに参加していない場合、オンボード発振器を使用するアクティブ ソースとして設定されている場合、または最初のクロック同期の前に有効なクロック ソースが存在していない場合だけ、フリーランニング モードで動作します。それ以外の場合、ラインカードは通常モードで動作します。

- 通常：通常モードでは、モジュールは外部提供のネットワーク タイミング基準と同期します。このタイミング基準は、シャーシ BITS 入力のいずれかがソースとなっているか、またはネットワーク インターフェイスから回復されたものです。このモードでは、入力基準の精度と安定性によって、出力信号の精度と安定性が決まります。
- ホールドオーバー：ホールドオーバー モードでは、ネットワーク タイミング モジュールが、通常モードでの動作時に使用された保存済みのタイミング基準に基づいてタイミング信号を生成します。回復された基準が失われたか、過度にドリフトした場合には、ホールドオーバー モードが自動的に選択されます。

（注）　ドリフト範囲は設定できません。デフォルトでは、ラインカード内部で ±9.2 ～ 12 ppm（parts per million）に設定されます。この ppm 設定は、Stratum 3/3E、ITU-T G.813 オプション 1 のクロック品質レベルを必要とするアプリケーションで一般的です。

（注）　ネットワーク クロックが設定されるまで、すべてのラインカードはフリーランニング モードで動作します。

SIP 200 のネットワーク クロッキングの詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwsip.html#wp1105490

http://www.cisco.com/en/US/products/hw/routers/ps368/module_installation_and_configuration_guides_chapter09186a008043ff58.html#wp1127288

ネットワーク クロッキングの設定方法

ここでは、ネットワーク クロッキングを設定する方法について説明します。

- 「BITS クロック サポートの設定」（P.64-24）
- 「クロック ソースとしての 10GE インターフェイスの設定」（P.64-26）
- 「クロック ソースの検証」（P.64-27）
- 「クロック ソースの回復」（P.64-29）

BITS クロック サポートの設定

システムのクロック ソースとして 76-ES+XT-2TG3CXL ラインカードまたは 76-ES+XT-4TG3CXL ラインカードで BITS ポートを選択して設定できます。これにより、システムのバックプレーン クロックとそれに対応する BITS ポート入力クロックが同期し、ネットワーク クロッキングをサポートするその他の全インターフェイスの伝送クロック基準として、BITS ポート入力クロックがシャーシ全体に配信されます。

使用上のガイドライン

次の注意事項に従ってください。

- ネットワーク クロッキング設定がスタートアップ コンフィギュレーションに存在する場合、クロッキング設定の解析後、5 分経過するまでその設定は適用されません。これにより、インターフェイスやコントローラが正常に稼働しなかった場合にバックプレーンでクロッキングが不安定になるのが回避されます。
- 76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL のネットワーク クロッキングはデフォルトでイネーブルになっています。
- Cisco IOS Release 12.2(33)SRD1 は、BITS 入力による Synchronization Status Messaging（SSM; 同期ステータス メッセージング）をサポートしません。
- Loss of Signal（LOS; 信号消失）、Loss of Frame（LOF; フレーム損失）、T1 ブルー アラーム、または E1 Alarm Indication Signal（AIS; アラーム表示信号）により BITS クロック ソース フラップが存在する場合、ソースが有効でアクティブになるまで 150 秒の間隔があります。
- Out-of-Range（OOR; 範囲外）スイッチオーバー（リバーティブ モード）が発生した場合、クロック オフセットが +12 ppm または -12 ppm のしきい値を超えるとソース スイッチオーバーが発生します。この場合は、ソースを再設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **network-clock slot** *slot* **bits** ***number*** {**2m** | **e1** [**crc4**] | **j1** [**esf**]| **t1** [**d4** | **esf** [**133ft** | **266ft** | **399ft** | **533ft** | **655ft**]}
4. **network-clock select** *priority* **slot** *slot* **bits** *number*
5. **exit**

手順の詳細

Cisco 76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL で BITS クロック サポートを設定するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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	**network-clock slot** *slot* **bits** *number* {**2m** | **e1** [**crc4**] | **j1** [**esf**]| **t1** [**d4** | **esf** [**133ft** | **266ft** | **399ft** | **533ft** | **655ft**]} **例：** `Router(config)# network-clock slot 1 bits 0`	（任意）BITS ポートの信号タイプを設定します。 デフォルトの信号タイプは、ESF フレーム同期を使用し、ライン ビルドアウト選択値が 133 フィートである T1 です。
ステップ 4	**network-clock select** *priority* **slot** *slot* **bits** *number* **例：** `Router(config)# network-clock select 1 slot 1 bits 0`	ソースに名前を付けて、ネットワーク クロックにタイミングを提供し、このクロック ソースの選択優先度を指定します。
ステップ 5	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例

次に、Cisco 76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL で BITS クロック サポートを設定する例を示します。

```
Router# enable
Router# configure terminal
Router(config)# network-clock slot 1 bits 0 ?
2m 2.048MHz square wave signal type
e1 E1 signal type
j1 Japan J1 signal type
t1 T1 signal type

Router(config)# network-clock slot 1 bits 0 t1 ?
d4 T1 D4 framing mode
esf T1 ESF framing mode

Router(config)# network-clock slot 1 bits 0 t1 d4 ?
133ft Line Build-Out Select 0 to 133 feet
266ft Line Build-Out Select 133 to 266 feet
```

```
399ft Line Build-Out Select 266 to 399 feet
533ft Line Build-Out Select 399 to 533 feet
655ft Line Build-Out Select 533 to 655 feet

Router(config)# network-clock slot 1 bits 0 t1 d4 266ft

Router(config)# network-clock select 1 slot 1 bits 0
Router(config)# exit
```

クロック ソースとしての 10GE インターフェイスの設定

これにより、ラインカードが 10GE インターフェイス（LAN PHY または WAN PHY）から受信したクロックを抽出し、システムのバックプレーン クロックをそのクロックと同期するように設定されます。次に、そのクロックが、ネットワーク クロッキング機能をサポートするシャーシで他の全インターフェイスの伝送クロック基準として使用されます。

使用上のガイドライン

次の注意事項に従ってください。

- ネットワーク クロッキング設定がスタートアップ コンフィギュレーションに存在する場合、クロッキング設定の解析後、5 分経過するまでその設定は適用されません。これにより、インターフェイスやコントローラが正常に稼働しなかった場合にバックプレーンでクロッキングが不安定になることが回避されます。
- 76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL のネットワーク クロッキングはデフォルトでイネーブルになっています。
- Cisco IOS Release 12.2(33)SRD1 は、WAN PHY の SONET/SDH フレームから受信した LAN PHY および SSM で Ethernet Synchronization Message Channel（ESMC）をサポートしません。
- インターフェイスの稼働イベントや停止イベントによりクロック ソース フラップが存在する場合、ソースが有効でアクティブになるまで 150 秒の間隔があります。
- 範囲外（OOR）スイッチオーバー（リバーティブ モード）が発生したが、インターフェイスは稼働状態の場合は、クロック オフセットが +12 ppm または -12 ppm のしきい値を超えるとソース スイッチオーバーが発生します。この場合は、ソースを再設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface TenGigabitEthernet** *slot*/*port*
4. **clock source {internal | line | loop}**
5. **exit**
6. **network-clock select** *priority* **interface TenGigabitEthernet** *slot*/*port*
7. **exit**

手順の詳細

10GE インターフェイスをクロック ソースとして設定するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	**enable** **例：** Router# enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** 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	**interface TenGigabitEthernet** *slot*/*port* **例：** Router(config)# interface tengigabitethernet 1/1	設定する 10 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。 • *slot*/*port*：インターフェイスの場所を指定します。
ステップ 4	**clock source** {**internal** | **line** | **loop**} **例：** Router(config-if)# clock source line	「ラインからクロックを回復する」ためにインターフェイスのクロック ソース タイプを選択します。これにより、このインターフェイスでシステムのクロック ソースを選択できるようになります。
ステップ 5	**exit** **例：** 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、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**network-clock select** *priority* **interface TenGigabitEthernet** *slot*/*port* **例：** Router(config)# network-clock select 1 interface TenGigabitEthernet 1/1	ソースに名前を付けて、ネットワーク クロックにタイミングを提供し、このクロック ソースの選択優先度を指定します。

例

次に、10GE インターフェイスをクロック ソースとして設定する例を示します。

```
Router# enable
Router# configure terminal
Router(config)# interface tengigabitethernet 1/1
Router(config-if)# clock source line
Router(config-if)# exit
Router(config)# network-clock select 1 interface TenGigabitEthernet 1/1
Router(config)# exit
```

クロック ソースの検証

show network-clocks コマンドを使用して、ルート プロセッサ（RP）側でネットワーク クロッキングを検証します。

```
Router# show network-clocks
 Active source = Slot 1 BITS 0
 Active source backplane reference line = Secondary Backplane Clock
 Standby source = TenGigabitEthernet1/1
```

```
 Standby source backplane reference line = Primary Backplane Clock
(Standby source not driving backplane clock currently)


 All Network Clock Configuration
---------------------------------
 Priority  Clock Source             State                          Reason
 1         POS3/0/1                Hardware not present
 2         Slot 1 BITS 0           Valid
 3         TenGigabitEthernet1/1   Valid

 Current operating mode is Revertive

 Current OOR Switchover mode is Switchover


There are no slots disabled from participating in network clocking

 BITS Port Configuration
-------------------------
 Slot    Port    Signal Type/Mode        Line Build-Out Select
 1       0       T1 D4                   DSX-1 (133 to 266 feet)
```

show platform hardware network-clocks コマンドを使用して、ラインカード側で出力を検証します。

```
Router-dfc# show platform hardware network-clocks

Local Loop Timing:

    Port 1: N    Port 2: N    Port 3: N    Port 4: N

Backplane Bus Status and Source:

    Primary   : Disabled, Port 0 RX_DEMAP Clock
    Secondary : Enabled,  BITS Rx Clock
    BITS      : Disabled, Port 0 RX_DEMAP Clock

ZL30138 Configuration and Status:

    DPLL1: Lock (2)
        Mode of Operation  : Automatic Normal
        Selected Reference : 4
        Ref0 Priority : 15        Ref1 Priority : 15
        Ref2 Priority : 15        Ref3 Priority : 15
        Ref4 Priority : 00        Ref5 Priority : 15
        Ref6 Priority : 15        Ref7 Priority : 15

    Reference Monitoring: Custom A frequency 25000 kHz
        Ref#    SCM    CFM    GST    PFM    Mode      Detected
        ------------------------------------------------------------
        0       0      0      0      0      CustA     38.88 MHz
        1       1      1      1      1      CustA     not detected
        2       0      0      0      1      CustA     38.88 MHz
        3       1      1      1      1      CustA     not detected
        4       0      0      0      0      Auto      1.544 MHz
        5       1      1      1      1      Auto      not detected
        6       1      1      1      1      Auto      not detected
        7       0      0      0      0      Auto      8 kHz

BITS Configuration and Status:

    Signal Type   : T1 D4 Framing
    Clock Divider : 1.544 MHz
```

```
Status          : Good
```

クロック ソースの回復

76-ES+XT-2TG3CXL および 76-ES+XT-4TG3CXL のクロック ソースの回復では、次の注意事項に従ってください。

BITS ポートをクロック ソースとして使用する場合：

- ラインカードを取り外すと、クロック状態は「Hardware not present」を示します。
- BITS Rx が LOS、LOF、ブルー アラーム（T1）、または AIS（E1）を報告すると、クロックは「Validate but not present」になります。
- BITS RX アラームが存在しない場合、クロック状態は「Valid」を示します。

10GE ポートをクロック ソースとして使用する場合：

- ラインカードを取り外すと、クロック状態は「Hardware not present」を示します。
- インターフェイスが停止すると、クロックは「Validate but not present」になります。
- インターフェイスが再び稼働すると、クロック状態は「Valid」になります。

10GE ポートと BITS ポートの両方のクロック回復に対して、クロック ソースが回復されると、ラインカードが RP に通知します。次に、150 秒のデバウンス期間の後に、参加しているすべてのラインカードに RP が制御メッセージを送信し、有効なクロック ソースと再同期します。

1588V2 について

IEEE 1588-2008 はプロトコル仕様標準です。IEEE 1588-2008 は、Precision Time Protocol Version 2（PTPv2）とも呼ばれます。これは、パケットベースのイーサネット インフラストラクチャに対して正確なタイミングと同期を提供するために特別に設計されています。

PTP ネットワーク要素

3 つの PTP ネットワーク要素は、マスター、スレーブ、および境界クロックです。

- PTP マスター : PTP マスターは Primary Reference Clock（PRC）または GPS からの正確なクロックを持ちます。このクロックにより、正確なタイムスタンプを派生するタイムスタンプ エンジンがイネーブルになります。
- PTP スレーブ : PTP スレーブは、マスターにより送信されたタイムスタンプから周波数とフェーズ クロックを回復するネットワーク要素です。
- 境界クロック : 境界クロックは、PTP マスターおよびスレーブとして動作します。境界クロックは、グランド マスターに対するスレーブとして動作し、グランド マスターから基準を派生します。境界クロックは、複数のダウンストリーム スレーブと独自の PTP セッションを開始します。境界クロックは、ネットワーク ホップの数を削減し、その結果、グランド マスターとスレーブの間でパケット ネットワークのパケット遅延が異なるようになります。

Timing over Packet

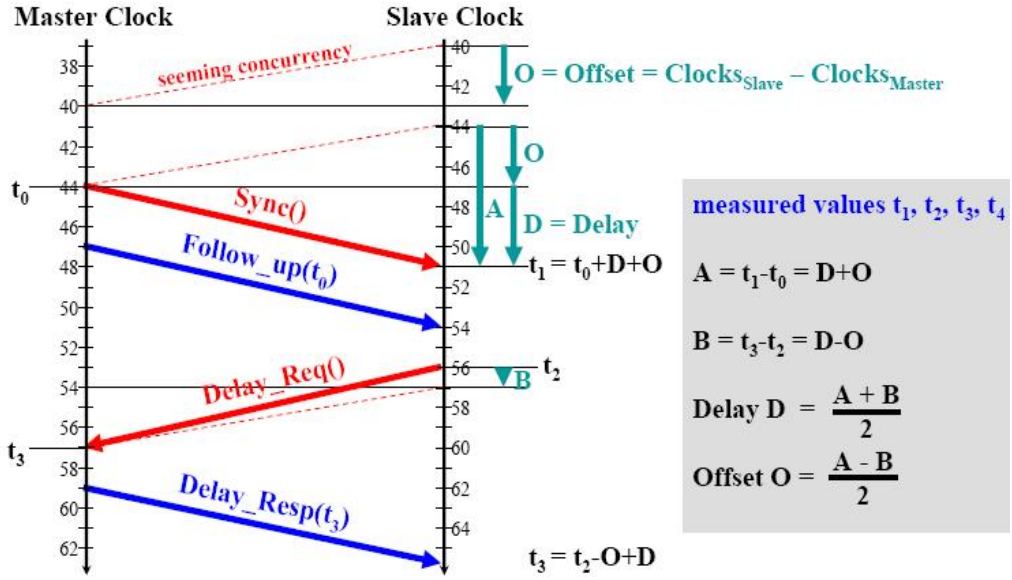
Timing over Packet（ToP）は、外部に対する 2 ポート ギガビット同期イーサネット SPA の PTP スタックのアドレスであるルート プロセッサで仮想インターフェイスとして動作します。他の PTP エンティティは、このインターフェイスの IP アドレスからパケットを送受信します。

宛先が ToP の IP アドレスであるパケットがルータで受信されると、ルータのハードウェアはルート プロセッサではなく 2 ポート ギガビット同期イーサネット SPA を使用するようリダイレクトします。ToP は 32 ビット マスクで設定されます。ToP では QOS はサポートされません。CoPP がサポートされています。

1588V2 の基本的な動作

ここでは、PTP の動作について説明します。図 64-1 に、PTPv2 マスターとスレーブ間でのメッセージ交換を示します。

図 64-1　　PTPv2 メッセージ交換



メッセージ交換は次の順序で行われます。

- マスターが SYNC メッセージをスレーブにリレーします。このメッセージが受信される時間が、スレーブのハードウェア補助装置によって記録されます。図 64-1 では、これは t1 として示されています。
- マスターは SYNC メッセージが独自のハードウェア補助装置から送信された実際の時間（t0）を記録し、前の SYNC メッセージのタイムスタンプを含むフォローアップ メッセージをスレーブにリレーします。
- ネットワーク遅延を計算するために、スレーブは「Delay Request」メッセージ（t2）をマスターに送信します。スレーブ ハードウェア補助装置が、メッセージが送信された時間を記録します。
- 遅延要求メッセージの受信時に、マスターは遅延応答メッセージ（t3）を t2 のタイムスタンプでスレーブに送信し返します。
- スレーブはタイムスタンプ（t0 ～ t3）を使用して、クロックを修正するためにオフセットおよび伝播遅延を計算します。

1588V2 でサポートされるモデル

1588V2 でサポートされる 2 つの PTP モデルは次のとおりです。

- サービス SPA モデル：

  サービス SPA モデルでは、パケットが SIP400 を介して 2 ポート ギガビット同期イーサネット SPA で開始および終了します。サービス SPA モデルは単純であり、既存のインフラストラクチャを使用し、さまざまなカプセル化と使用できます。

  2 ポート ギガビット同期イーサネット SPA は、リダイレクトされた PTP パケットを受信し、応答パケットを処理して中央スイッチング エンジンに送信します。これらのパケットは、クライアントの IP アドレスに基づいて転送されます。

  サービス SPA モデルの制限は次のとおりです。

  - システムのパケットの開始または終了時にタイムスタンプが設定されません。
  - PTP パケットの数は一定せず、Packet Delay Variation（PDV）と呼ばれる遅延が発生します。

- 直接 SPA モデル：

  2 ポート ギガビット同期イーサネット SPA は、7600 にある既存のラインカードのレシーバとトランスミッタでパケットにタイムスタンプを正確に設定できます。したがって、1588v2 の理想的な要件を満たすために、PTP パケットは同じ 2 ポート ギガビット同期イーサネット SPA で送受信されます。

  直接 SPA モデルでは、PTP パケットは、2 ポート ギガビット同期イーサネット SPA のイーサネット ポートを介して送受信されます。2 ポート ギガビット同期イーサネット SPA イーサネット インターフェイスに着信した PTP パケットは、FPGA により SPA の PTP スタックに転送されます。次に、設定（マスターまたはスレーブ）に基づいて、PTP スタックまたはアルゴリズムが必要な処理を行います。応答パケットは、SPA のイーサネット ポートから送信されます。

  直接 SPA モデルの制限は次のとおりです。

  - 限定されたカプセル化のみがサポートされます。
  - PTP パケットは、2 ポート ギガビット同期イーサネット SPA ポートでのみ受信されます。

サポートされるトランスポート モード

1588v2 でサポートされるトランスポート モードは次のとおりです。

- ユニキャスト モード：ユニキャスト モードでは、1588v2 マスターが Sync メッセージまたは Delay_Resp メッセージをスレーブのユニキャスト IP アドレスのスレーブに送信し、スレーブは Delay_Req をマスターのユニキャスト IP アドレスのマスターに送信します。
- ユニキャスト ネゴシエーション モード：ユニキャスト ネゴシエーション モードでは、マスターは最初にどのスレーブも認識しません。スレーブは、ネゴシエーション メッセージをマスターに送信します。1 つのマスターが複数のスレーブを持つことができるため、ユニキャスト ネゴシエーション モードは、スケーラビリティという面で優れています。
- 混合マルチキャスト モデル：混合マルチキャスト モデルでは、マスターはメッセージをマルチキャスト パケットで IP アドレス 224.0.1.129（1588v2 標準で定義済み）に送信します。スレーブは、このプロセスでマスターの IP アドレスを学習し、遅延要求メッセージを送信します。次に、マスターは、遅延応答メッセージをユニキャスト モードでスレーブに送信し返します。

  メッセージをマルチキャスト モードで送信するために、マスターはマルチキャスト出力インターフェイスを明示的に指定する必要があります。これにより、中継ネットワークが IP アドレス 224.0.1.129 をスレーブにルーティングすることが可能になります。

Time of Day（TOD）

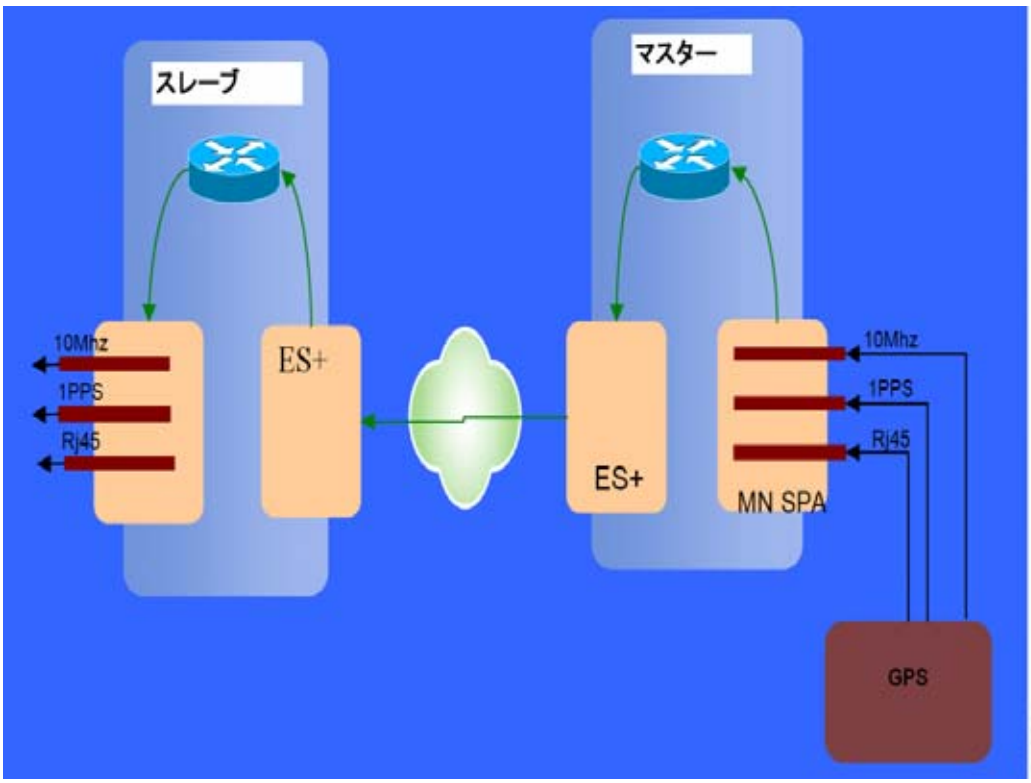
2 ポート ギガビット同期イーサネット SPA は、GPS 信号に対してタイムスタンプを取得または生成する 2 つの物理インターフェイスを提供します。

この物理インターフェイスは Time of Day（ToD）を取得するために使用され、次のようなフェーズになります。

- 1PPS インターフェイス
- RJ45 インターフェイス

図 64-2 に、1588V2 を使用した Time of Day（ToD）と 1 PPS の同期を示します。

図 64-2　1588V2 を使用した Time of Day（ToD）と 1 PPS の同期のブロック図



1588V2 マスターの Time of Day

1588V2 マスター モードでは、Time of Day（TOD）により、2 ポート ギガビット同期イーサネット SPA が RJ45 インターフェイスを介して GPS レシーバから時刻を受信することが可能になり、SPA の現在時刻と同期されます。ToD を正しく読み取るために、1588V2 マスターは、GPS デバイスからの 1PPS 入力を必要とします。

1588V2 スレーブの Time of Day

1588V2 スレーブ モードでは、2 ポート ギガビット同期イーサネット SPA が、1588v2 セッションから ToD を回復します。Precision Time Protocol（PTP）から回復された TOD と 1 PPS は個々のインターフェイスでリプレイされます。

制限事項

15.1(1)S リリース以降、次の制限が 1588V2 機能に適用されます。

- 1588v2 セッションから回復された TOD はシステム クロックと同期しません。
- GPS インターフェイスはクロック回復に対してのみ使用できます。システム クロックは、GPS インターフェイスで送信できません。
- サポートされる TOD 形式は UBOX、CISCO、および NTP のみです。

1588v2 セッションから回復されたクロックを使用するには、ToP インターフェイスをクロック ソースとして設定する必要があります。

1588V2 マスターでの ToD の設定

1588V2 マスターで ToD を設定するには、次のコマンドを使用します。

コマンド	目的
Router(config-ptp-clk)# **tod <slot>/<subslot> <Cisco/ntp/ubx>**	1588V2 で ToD を設定します。
Router(config-ptp-clk)# **input 1pps <slot>/<subslot>**	マスターに入力を提供します。

次に、1588V2 マスターで ToD を設定する例を示します。

```
Router# config terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# tod 3/3 cisco
Router(config-ptp-clk)# input 1pps 3/3
Router(config-ptp-clk)# clock-port MASTER master
Router(config-ptp-clk)# transport ipv4 unicast interface Gi3/3/1 negotiation
Router(config-ptp-clk)# end
```

1588V2 マスターでの ToD 設定の検証

次に、1588V2 マスターの ToD 設定を検証する例を示します。

```
Router# show ptp clock runn dom 0
PTP Ordinary Clock [Domain 0]
State          Ports          Pkts sent      Pkts rcvd

         FREQ_LOCKED    1              30052          5867

                              PORT SUMMARY

Name               Tx Mode      Role         Transport    State        Sessions

MASTER             unicast      master       To3/1/2      -            1

                            SESSION INFORMATION
```

```
MASTER [To3/1/2] [Sessions 1]

 Peer addr          Pkts in    Pkts out   In Errs    Out Errs

 4.4.4.4            5867       30052      0          1
```

show platform ptp tod all コマンドを使用すると、同じ出力が表示されます。

```
Router# show platform ptp tod all
--------------------------------
ToD/1PPS Info for SPA 3/1
--------------------------------
ToD CONFIGURED        : YES
ToD FORMAT            : CISCO
ToD DELAY             : 0
1PPS MODE             : INPUT
1PPS STATE            : UP
ToD STATE             : UP
ToD CLOCK             : Mon Aug 30  09:36:47 UTC 2010
```

1588V2 スレーブでの ToD の設定

1588V2 スレーブで ToD を設定するには、次のコマンドを使用します。

コマンド	目的
Router(config-ptp-clk)# **tod <slot>/<subslot> <Cisco/ntp/ubx>**	1588V2 で ToD を設定します。
Router(config-ptp-clk)# **output 1pps <slot>/<subslot>**	スレーブから出力を提供します。

次に、1588V2 スレーブで ToD を設定する例を示します。

```
Router# config terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# tod 3/3 cisco
Router(config-ptp-clk)# output 1pps 3/3
Router(config-ptp-clk)# clock-port SLAVE slave
Router(config-ptp-clk)# transport ipv4 unicast interface Gi3/3/1 negotiation
Router(config-ptp-clk)# clock source 1.1.1.1
Router(config-ptp-clk)# end
```

1588V2 スレーブでの ToD 設定の検証

次に、1588V2 スレーブで ToD 設定を検証する例を示します。

```
Router# show ptp clock runn dom 0

                    PTP Ordinary Clock [Domain 0]

        State          Ports          Pkts sent      Pkts rcvd

        ACQUIRING      1              5308           27185

                              PORT SUMMARY

Name              Tx Mode      Role         Transport    State        Sessions
```

```
SLAVE              unicast      slave        To3/1/2      -           1

                              SESSION INFORMATION

SLAVE [To3/1/2] [Sessions 1]

 Peer addr          Pkts in    Pkts out   In Errs    Out Errs

 3.3.3.3            27185      5308       0          0
```

show platform ptp tod all コマンドを使用すると、同じ出力が表示されます。

```
Router# show ptp clock runn dom 0

                      PTP Ordinary Clock [Domain 0]

         State          Ports          Pkts sent      Pkts rcvd

         PHASE_ALIGNED  1              21428          109772

                               PORT SUMMARY

Name               Tx Mode      Role         Transport    State        Sessions

SLAVE              unicast      slave        To3/1/2      -            1

                              SESSION INFORMATION

SLAVE [To3/1/2] [Sessions 1]
Peer addr          Pkts in    Pkts out   In Errs    Out Errs
Router# show platform ptp tod all
--------------------------------
ToD/1PPS Info for SPA 3/1
--------------------------------
ToD CONFIGURED        : YES
ToD FORMAT            : CISCO
ToD DELAY             : 0
1PPS MODE             : OUTPUT
OFFSET                : 0
PULSE WIDTH           : 0
ToD CLOCK             : Mon Aug 30  09:52:08 UTC 2010
       --------------------------------
```

CHAPTER 65

リンク ステート トラッキングの設定

この章では、Cisco IOS Software Release 15.1(01)S でリンク ステート トラッキ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 の『Cisco 7600 Series Router Cisco IOS Command Reference』を参照してください。
http://www.cisco.com/en/US/products/ps6922/prod_command_reference_list.html

この章の内容は次のとおりです。

- 「リンク ステート トラッキングの機能概要」（P.65-1）
- 「リンク ステート トラッキングの設定」（P.65-2）

リンク ステート トラッキングの機能概要

REP および MST セグメントでリンク障害が発生すると、関連するプロトコルはリンク障害イベントを処理します。ただし、スイッチへのプライマリ リンクがイネーブルになっている場合は、スイッチ上の対応するアップリンク ポートがディセーブルでも、REP および MST プロトコルはバックボーン側を認識せず、フェールオーバーを開始しません。ルータは、アクセス側からのトラフィックを受信し続けますが、バックボーン接続がないためにそのトラフィックをことごとくドロップします。リンク ステート トラッキングは、アップリンク インターフェイスがリンク ステータスをダウンリンク ポートへバインドできるようにすることで、この問題に対するソリューションを提供します。アップリンク ステート トラッキングは、一連のアップリンク ポートがディセーブルの場合に、CLI コマンドによってリンクされた他のポートもディセーブルになるように設定されています。アップストリーム インターフェイスすべてがディセーブルの場合のみ、ダウンリンク インターフェイスすべてのステートが errdisable になります。

LST は、コア側インターフェイスのステートに応じて、アクセス側で REP/MST の再コンバージェンスを開始します。コア側インターフェイスおよびアクセス側インターフェイスのリンク ステートは、リンク ステート トラッキング グループによりバインドされます。

LST は、以下を容易にします。

- リンク ステート グループ トラッキングのイネーブル化とディセーブル化。
- リンク ステート グループからのダウンストリーム インターフェイスの削除。
- errdisable インターフェイスでの shut/no shut の実行。

制約事項および使用上の注意事項

LST を設定する場合は、次の制約事項および使用上の注意事項に従ってください。

- 管理インターフェイスがリンク ステート グループに参加していないことを確認します。
- REP ポートは、アップリンク ポートとして設定できません。
- LST では、アップストリームまたはダウンストリームを問わず、どのインターフェイスも複数のリンク ステート グループに参加できません。
- 最大 10 のリンク ステート グループを設定できます。
- LST を初めて設定するときは、アップストリーム インターフェイスをリンク ステート グループに追加してからダウン ストリームを追加する必要があります。このようにしない場合は、ダウンリンク インターフェイスの状態が errdisable になります。
- 設定可能なインターフェイスは、物理的（ルーテッドとスイッチ ポートの両方）、ポートチャネル、サブインターフェイス、および VLAN です。
- アップストリーム インターフェイスは次のいずれかであることが必要です。
  - L3 インターフェイス（物理またはポートチャネル）
  - SVI
- ダウンストリーム インターフェイスは次のいずれかであることが必要です。
  - L2 インターフェイス
  - L2 ポートチャネル
  - EVC

リンク ステート トラッキングの設定

リンク ステート トラッキングを設定するには、次の作業を実行します。

	コマンドまたはアクション	目的
ステップ 1	**enable** Example: Router> enable	特権 EXEC モードをイネーブルにします。
ステップ 2	**configure terminal** Example: 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	**link state track** *number* Example: Router(config)# link state track 1	リンク ステート グループを作成して、LST をイネーブルにします。指定できる範囲は 1 ～ 10 です。デフォルト値は 1 です。
ステップ 4	**interface** *slot/port* Example: Router(config)# interface gigabitethernet 2/1	インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**link state group** *[number]* {**upstream** | **downstream**} Example: Router(config-if)# link state group 1 upstream	リンク ステート グループを指定し、グループ内のインターフェイスをアップストリームまたはダウンストリーム インターフェイスに設定します。グループ番号は 1 ～ 10 に設定できます。デフォルト値は 1 です。
ステップ 6	**end** Example: Router(config-if)# end	CLI を終了して特権 EXEC モードに戻ります。

次に、リンク ステート グループを作成してインターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# link state track 1
Router(config)# interface gigabitethernet3/1
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/3
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/5
Router(config-if)# link state group 1 downstream
Router(config-if)# interface gigabitethernet3/7
Router(config-if)# link state group 1 downstream
Router(config-if)# end
```

次に、設定を確認する例を示します。

show link state group コマンドは、リンク ステート グループの情報を表示します。

```
Router> show link state group 1
Link State Group: 1 Status: Enabled, Down
```

show link state group detail コマンドは、グループの詳細情報を表示します。

```
Router> show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi3/5(Dwn) Gi3/6(Dwn)
Downstream Interfaces : Gi3/1(Dis) Gi3/2(Dis) Gi3/3(Dis) Gi3/4(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi3/15(Dwn) Gi3/16(Dwn) Gi3/17(Dwn)
Downstream Interfaces : Gi3/11(Dis) Gi3/12(Dis) Gi3/13(Dis) Gi3/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

リンク ステート トラッキングのトラブルシューティング

表 65-1 に、LST 設定中の問題のトラブルシューティングについて示します。

表 65-1　LST の問題のトラブルシューティング

問題	ソリューション
アップストリーム インターフェイスがアップの場合でも、ダウンストリーム インターフェイスが errdisable ステートになる。	**show interfaces** <interface> **status err-disabled** コマンドを使用して、インターフェイスが前記のステートになる理由を確認します。 **show errdisable recovery** コマンドを使用して、errdisable リカバリ タイマーについての情報を表示します。

CHAPTER 66

IP および MPLS 向け BGP PIC エッジおよびコアの設定

この章では、Cisco 7600 シリーズ ルータ上で、インターネット プロトコル（IP）とマルチ プロトコル ラベル スイッチング（MPLS）向けのボーダー ゲートウェイ プロトコル（BGP）Prefix-Independent Convergence（PIC）エッジおよびコアを設定する方法について説明します。

IP および MPLS 向け BGP PIC エッジおよびコア

IP および MPLS 向け BGP PIC エッジおよびコア機能は、ネットワーク障害発生後のコンバージェンスを改善します。このコンバージェンスは、IP および MPLS ネットワークのコアの障害とエッジの障害の両方に適用されます。この機能を使用して、Routing Information Base（RIB; ルーティング情報ベース）、Forwarding Information Base（FIB; 転送情報ベース）および Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）に代替パスを作成、保存します。障害の検出時には、代替パスがすぐに引き継ぐことで、高速なフェールオーバーが実現されます。

機能の利点は次のとおりです。

- フェールオーバー用の代替パスにより、接続の復元を迅速化。
- トラフィック損失の削減。
- コンバージェンス時間が一定なので、すべてのプレフィックスで切り替え時間が同じ。

BGP PIC の前提条件

BGP PIC 機能には、次の前提条件が適用されます。

- BGP および IP または MPLS ネットワークがアクティブであること、およびカスタマー サイトが複数のパスによってプロバイダー サイトと接続されていること（マルチホーム）を確認します。
- バックアップ パスまたは代替パスには、最良パスのネクスト ホップと異なる固有のネクスト ホップがあることを確認します。これは BGP PIC エッジにのみ適用され、コアには適用されません。
- Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）プロトコルをイネーブルにして、直接接続されたネイバーのリンク障害を検出できるようにします。
- BGP PIC エッジおよびコアは、複数の VRF のネイティブ IPv4 およびネイティブ IPv6 をサポートします。
- BGP IPv6 PIC の拡張性は既存の BGP IPv4 PIC の拡張性と一致する必要があります。

制約事項

BGP PIC 機能の使用時には、次の制約事項に従ってください。

- BGP PIC 機能は、BGP マルチパスおよび非マルチパスでサポートされます。
- MPLS VPN では、MPLS VPN 相互自律システム オプション B を使った BGP PIC 機能はサポートされていません。
- BGP PIC 機能は、IPv4、IPv6、VPNv4、および VPNv6 アドレス ファミリのプレフィックスのみをサポートします。
- BGP PIC 機能は、マルチキャストまたは L2VPN 仮想ルーティングおよびフォワーディング（VRF）のアドレス ファミリで設定できません。
- 2 台の PE ルータが CE ルータへの相互パスまたは代替パスになると、トラフィックは CE ルータが失敗した場合にループする可能性があります。その場合は、どちらのルータも CE ルータに到達せず、トラフィックは存続可能時間（TTL）タイマーが切れるまで 2 つのルータ間で転送され続けます。
- BGP PIC は次のアドレス ファミリでサポートされます。
  - サービス プロバイダー コアのネイティブ IPv6 による IPv6
  - IPv4 MPLS コアによる IPv6 および VPNv6 とサービス プロバイダー エッジ ルータの 6PE および 6VPE による IPv6 および VPNv6
- PIC エッジをイネーブルにすると、ほぼ 2 倍の数の隣接エントリが使用されます。
- ロード バランス パスに MPLS TE トンネルがある場合、7600 は BGP PIC コアをサポートしません。

IP および MPLS 向け BGP PIC の設定

BGP PIC エッジおよびコアの設定の詳細については、次の URL の『*MPLS Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-bgp-mp-pic.html

CHAPTER 67

IPv4 トランスポートを介した VRF 対応 IPv6 トンネルの設定

この章では、Cisco IOS Software Release 15.2(2)S で IPv4 トランスポートを介した VRF 対応 IPv6 トンネルを設定する方法について説明します。

この章の内容は次のとおりです。

- 「VRF 対応 IPv6 トンネルの概要」（P.67-1）
- 「VRF 対応 IPv6 トンネルの設定」（P.67-2）
- 「IPv6 over IPv4 GRE トンネルの概要」（P.67-3）
- 「IPv6 over IPv4 GRE トンネルの設定」（P.67-4）

VRF 対応 IPv6 トンネルの概要

c7600 の現行の IPv6 トンネリング機能は、仮想ルーティングおよびフォワーディング（VRF）認識をサポートしません。IPv6 オーバーレイ アドレスと IPv4 トランスポート アドレスの転送テーブル ルックアップは、グローバル ルーティング テーブルで実行されます。この機能は、VRF の IPv6 オーバーレイ アドレスのトンネリング サポートを拡張します。

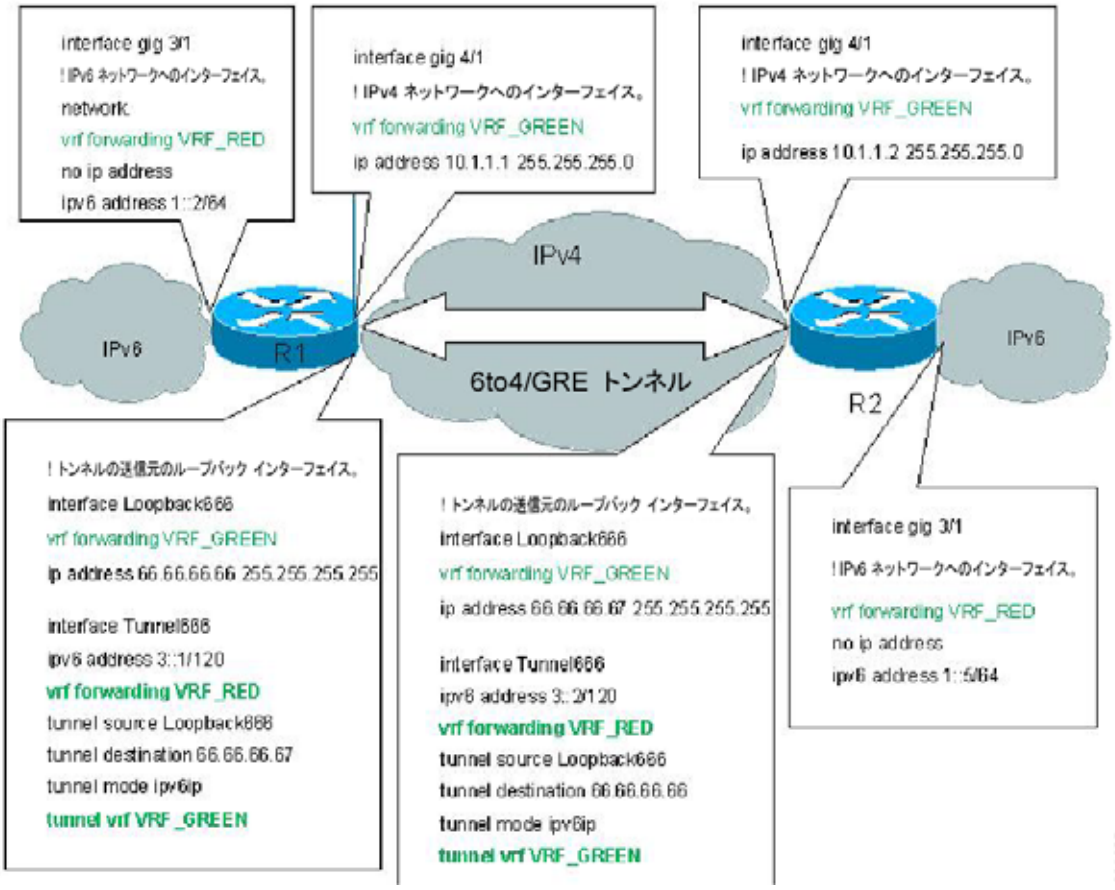
次のシナリオで、VRF 対応 IPv6 トンネル機能について説明します。

- VRF の IPv6 オーバーレイ アドレスおよびグローバル ルーティング テーブル（RT）の IPv4 トランスポート アドレス。
- VRF の IPv6 オーバーレイ アドレスおよび VRF の IPv4 トランスポート アドレス。

図 67-1 に、VRF の IPv6 オーバーレイ アドレス用トポロジと VRF の IPv4 トランスポート アドレスを示します。

図 67-1　　VRF 対応 IPv6 トンネルのトポロジ

VRF 対応 IPv6 over IPv4 トンネルは、コア側に対してラインカードを持つことができます。



VRF 対応 IPv6 トンネルの制約事項

次の制約事項が VRF 対応 IPv6 トンネル機能に適用されます。

- この機能は、IPv6IP および 6to4 トンネル モードをサポートします。
- EARL 制限により、VRF 間で送信元が同じトンネルはサポートされません。
- トンネルの送信元と宛先は、同じ VRF インスタンスにある必要があります。
- トンネルの IPv4 トランスポート アドレスとトンネル トラフィックが終了する物理インターフェイスは、同じ VRF インスタンスにある必要があります。
- 着信 IPv6 インターフェイスとトンネルは、同じ VRF インスタンスにある必要があります。
- この機能は、IPv6IP の自動トンネルと ISATAP をサポートしません。

VRF 対応 IPv6 トンネルの設定

VRF 対応 IPv6 トンネルの設定の詳細については、次の URL を参照してください。

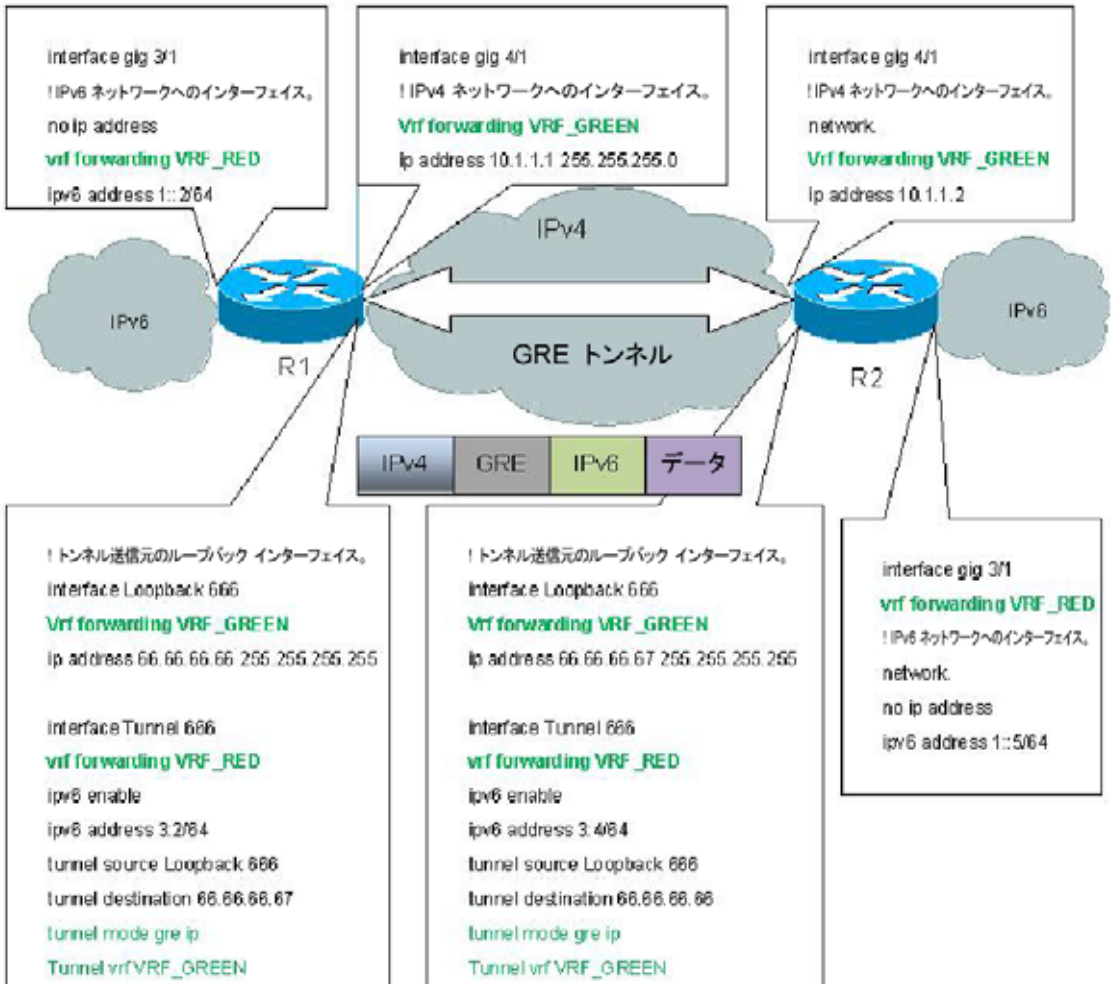
http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1524288

IPv6 over IPv4 GRE トンネルの概要

IPv6 トラフィックは、標準的な総称ルーティング カプセル化（GRE）トンネリング技術を使用する IPv4 GRE トンネル経由で伝送されます。GRE トンネルは、手動で設定された IPv6 トンネルと同様、リンクごとに個別のトンネルが設定された 2 つのポイント間のリンクです。GRE トンネルは、2 つのエッジ ルータ間またはエッジ ルータとエンド システム間に、定期的でセキュアな通信を必要とする安定した接続を実現します。この機能は、c7600 の VRF 対応 IPv6 over IPv4 GRE トンネルをサポートし、ラインカードの ES+ ファミリにのみ適用できます。

図 67-2　　VRF 対応 IPv6 over IPv4 GRE のトポロジ

VRF 対応 IPv6 over IPv4 GRE トンネルには、コア側に対する ES+ ラインカードが必要です。



IPv6 over IPv4 GRE トンネルの制約事項

次の制約事項が IPv6 over IPv4 GRE トンネルに適用されます。

- IPv4 トンネル側インターフェイスは、ES+ ラインカード上にある必要があります。

- GRE トンネル キーは、ハードウェアでサポートされません。
- トンネルをカプセル化した後の IPv4 フラグメンテーションは、ハードウェアでサポートされません。
- トンネルのカプセル開放用にフラグメント化された IPv4 パケットは、ハードウェアでサポートされません。
- IPv4 GRE キープアライブはサポートされますが、IPv6 GRE キープアライブはサポートされません。
- **vrf forwarding** コマンドと **tunnel vrf** コマンドを使用して設定された VRF インスタンスが異なる場合、キープアライブはサポートされません。
- EARL 制限により、VRF 間で送信元が同じトンネルはサポートされません。
- この機能は、SSO 準拠ではありません。
- 拡張された設定を使用して、トンネル モードを IPv6 over GRE から IPv6IP に変更するときに **mls mpls tunnel-recirc** コマンドをイネーブルにすると、トレースバックを含むエラー メッセージが表示されます。

IPv6 over IPv4 GRE トンネルの設定

IPv6 over IPv4 GRE トンネルの設定の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html#wp1525107

CHAPTER 68

ISIS IPv4 Loop Free Alternate Fast Reroute（LFA FRR）

ネットワークに障がいが発生すると、Loop Free Alternate（LFA）Fast Reroute（FRR）では、ダイナミック ルーティング プロトコルを使用して事前計算されるバックアップ ルートを使用します。バックアップ ルート（修復パス）は事前に計算され、プライマリ パスのバックアップとしてルータにインストールされます。ルータは、リンクまたは隣接ノードの障がいを検出すると、バックアップ パスに切り替えてトラフィック損失を回避します。

Release 15.1(2)S 以前は、リンクやルータに障がいが発生したり、保守に戻されたりすると、分散ルーティング アルゴリズムにより、ネットワーク内の変化に基づいて新しいルートが計算されました。新しいルートが計算される時間をルーティングの遷移と呼びます。ルーティングの遷移が計算されるまで、ネットワーク接続は中断されました。これは、代替パスが識別されるまで、障がいに隣接するルータは、障がいの発生したコンポーネントを介してデータ パケットを転送し続けるためです。

ルーティングの遷移によってサービス障がいが発生した状況は、失われたデータ パケットを再送信するハイレベル プロトコルによって隠されました。ただし、音声 / ビデオ データ トラフィックの場合には、パケット ドロップは受け入れられません。これらのデータ サービスの場合、ルーティングの遷移による中断や再コンバージェンスは、ユーザに対してトランスペアレントである必要があります。Release 15.1(2)S より導入された ISIS IPv4 Loop Free Alternate Fast ReRoute（LFA FRR）機能は、ルーティングの遷移時間を 50 ミリ秒に減少します。現在、IOS LFA FRR 機能は IGP Intermediate System-to-Intermediate System（ISIS）プロトコルだけでサポートされています。

（注） Release 15.1(3)S より導入された IOS LFA FRR 機能は、50 ミリ秒のルーティング遷移時間で、ES+ ラインカード上の Virtual Private LAN Service（VPLS; バーチャル プライベート LAN サービス）をサポートしています。

ISISI LFA FRR の制約事項

ISIS IPv4 LFA FRR 機能には、次の制約事項が適用されます。

- サポートされているネクストホップの最大数は 40 です。
- サポートされているプレフィックスの最大数は 10000 です。
- LFA FRR 機能は、IGP ISIS プロトコルだけでサポートされています。
- ユニキャスト修復パスだけがサポートされています。
- ISIS は、障がいのあるリンクと同じ Shared Risk Link Group（SRLG; 共有リスク リンク グループ）に属しているリンクを選択しません。

- リンクダウン検出時間が長くなるため、LFA FRR プライマリ パスには、LAN インターフェイスは推奨されません。ただし、LAN インターフェイスは修復パスに使用できます。
- VPLS over IP-FRR 用のコア側インターフェイスとして設定された LAN インターフェイスはサポートされません。
- VPLS over IP-FRR 用のコアでは、最大 6 つの Port-Channel（PoCH; ポートチャネル）インターフェイス（LAG-NNI）がサポートされます。
- **isis network point-to-point** コマンドを使用して、LAN インターフェイスに 1 つのネイバーを設定します。
- トラフィック エンジニアリング（TE）FRR フェールオーバーが LFA FRR フェールオーバーの後に続く場合、FRR で保護された TE トンネルが IP FRR の修復パスとして設定されているときは、50 ミリ秒のコンバージェンスは保証されません。
- プライマリ インターフェイスがトンネル インターフェイスである場合のプレフィックスについては、ISIS は LFA を計算しません。ただし、TE トンネル（プレーンおよび FRR 保護）は設定できます。
- プライマリまたはバックアップ トンネルとしての GRE トンネルは、VPLS に対してサポートされていません。
- 複数の等コスト プライマリ パスを持つ、IP FRR で保護されたプレフィックスの場合、すべてのプライマリ パスの修復パスとして、1 つの IP GRE トンネルだけがサポートされます。
- インポジションとディスポジションの両方向で VPLS over IOP-FRR をサポートするのは、ES+ カードのみです。
- ISIS 実装は、プライマリ Shortest Path First（SPF）が識別されたあと、LFA 計算が実行されるまで 5000 ミリ秒待機します。設定されたパスが保護されるのは、ISIS で LFA 計算が実行されたあとに限られます。
- サブインターフェイスは、修復インターフェイスのみに対してサポートされます。
- ISIS LFA FRR 機能は、IPV4 プレフィックスのみをサポートします。
- 修復パスが GRE トンネル（MPLS over GRE）を使用している場合、LFA FRR は、MPLS ラベル付きのトラフィックに対する 50 ミリ秒のコンバージェンスをサポートしません。
- ポートチャネルがプライマリ パスとして設定されている場合の IP FRR コンバージェンス時間は、50 ～ 100 ミリ秒です。**port-channel min-links** *link_number* **config** コマンドを使用して、ポートチャネルに障がいが発生した場合のコンバージェンス時間を減らします。

Cisco 7600 シリーズ ルータでの IOS IPFRR サポートの設定

Cisco 7600 シリーズ ルータに IOS LFA FRR サポートを設定できます。詳細については、http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_ipv4_lfafrr.html を参照してください。

検証

Distributed Forwarding Card（DFC; 分散型フォワーディング カード）およびスイッチ プロセッサ（SP）から検証情報を収集するためのリモート コマンドを使用して、IOS LFA FRR の設定を確認します。設定を確認するには、次のコマンドを使用します。

- **show mls cef** *ip-address* コマンドを使用して、FRR 保護に即して再循環がプログラムされているかどうかを確認します。

```
router-sp# show mls cef 192.168.3.0
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
3206   192.168.3.0/24      recirc (Hash: 0001)
                           recirc (Hash: 0002)
```

- **show mls cef** *ip-address* **detail** コマンドを使用して、特定のプレフィックス ルックアップ用に隣接エントリ アドレスとハードウェア共有（m 値）を取得します。

```
router-sp# show mls cef 192.168.3.0 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(3206   ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3206   ): 8 | 1 0    0 0 0 0   192.168.3.0        (A:425984 ,P:1,D:0,m:0 ,B:0 )
```

- **show mls cef adjacency entry** *entry_id* **detail** コマンドを使用して、再循環 VLAN や、着信パケットに付加されたラベル スタックなどの実際の隣接の詳細を表示します。

```
router-sp# show mls cef adjacency entry 425984 detail
Index: 425984  smac: 0000.0000.0000, dmac: 00d0.bc39.1000
               mtu: 65535, vlan: 1025, dindex: 0x7FFA, l3rw_vld: 1
               format: MPLS, flags: 0x8710
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 526346, exp: 0, ovr: 0
               op: PUSH_LABEL2
               packets: 0, bytes: 0
```

- **show mls cef mpls label** *label_id* **detail** コマンドを使用して、着信パケットに付加された内部ラベルに対応するプライマリおよび修復パスの隣接を確認します。

```
router-sp# show mls cef mpls label 526346 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
       D - FIB Don't short-cut, m - mod-num, E - ELSP?
Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2 eos2)
V(2152   ): B | 1 510  0 1 0 526346  0 0 0 0       0 0 (A:147458 ,P:0,D:0,m:0 :E:1) <<
VPN 510 entry is for primary path
M(2152   ): F | 1 FFF  0 1 1 FFFFF   0 0 0 0       0 0
V(2153   ): B | 1 511  0 1 0 526346  0 0 0 0       0 0 (A:163842 ,P:0,D:0,m:0 :E:1) <<
VPN 511 entry is for repair path
M(2153   ): F | 1 FFF  0 1 1 FFFFF   0 0 0 0       0 0
```

（注）　VPN 510 に対応するエントリはプライマリ パスを表し、VPN 511 は修復パスを表します。

CHAPTER 69

Y.1731 パフォーマンス モニタリング

この章では、Cisco IOS Software Release 15.1(2)S で Y.1731 パフォーマンス モニタリングを設定する方法について説明します。

この章の内容は次のとおりです。

- 「Y.1731 パフォーマンス モニタリングの概要」（P.69-1）
- 「Y.1731 PM の設定」（P.69-5）

Y.1731 パフォーマンス モニタリングの概要

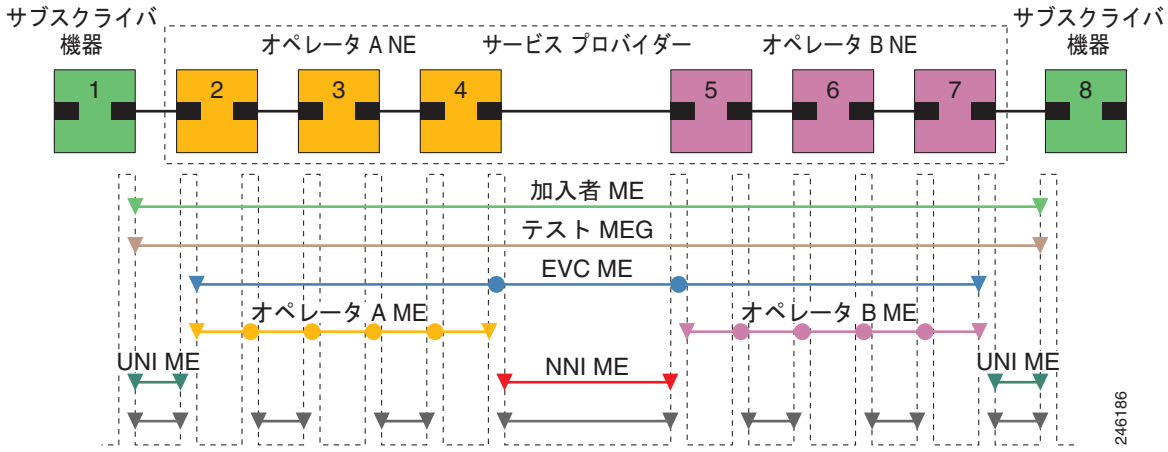
サービス プロバイダーが加入者に接続サービスを販売する場合、サービスの購入者と販売者の間で Service Level Agreement（SLA; サービス レベル契約）が交わされます。SLA にはプロバイダーが提供する属性が定義されており、これがサービス プロバイダーの法的義務となります。加入者が求めるパフォーマンスのレベルが高くなると、サービス プロバイダーは提供されているパフォーマンスのパラメータをモニタリングする必要があります。サービス プロバイダーのニーズに対応するために、組織は IEEE 802.1ag や ITU-T Y.1731 などさまざまな標準を定義し、パフォーマンス パラメータの測定に使用する手法とフレーム形式を規定しています。

Y.1731 Performance Monitoring（PM; パフォーマンス モニタリング）では、イーサネットのフレーム遅延、フレーム遅延変動、フレーム損失、フレーム スループット測定など、標準的なイーサネット PM 機能が提供されます。これらの測定は ITU-T Y-1731 標準で規定され、Metro Ethernet Forum（MEF; メトロ イーサネット フォーラム）標準グループによって認定されています。Y-1731 勧告に従い、7600 プラットフォームは 10 ms 間隔（1 秒につき 100 フレーム）で PM フレームを送信、受信、処理できなければなりません。所定のサービスに対して推奨される最大伝送時間は 100 ms（1 秒につき 10 フレーム）です。

フレーム遅延やフレーム遅延変動などの SLA パラメータを測定するために、少数の合成フレームがサービスとともにメンテナンス リージョンのエンド ポイントへ送信され、Maintenance End Point（MEP; メンテナンス エンド ポイント）が合成フレームに応答します。接続障害管理などの機能の場合、メッセージは送信頻度が低く、一方パフォーマンス モニタリング フレームはより頻繁に送信されます。

図 69-1 に、Y.1731 標準向けのポイントツーポイント Metro Ethernet 導入で一般的に組み込まれる Maintenance Entity（ME; メンテナンス エンティティ）と Maintenance End Point（MEP; メンテナンス ポイント）を示します。

図 69-1　一般的なメンテナンス エンティティとメンテナンス ポイントを使用したポイントツーポイント Metro Ethernet 導入



パフォーマンス モニタリングのパラメータは次のとおりです。

- 接続
- フレーム遅延とフレーム遅延変動
- フレームの損失率および可用性

接続

パフォーマンス モニタリングの最初の手順では、接続性の検証を行います。接続性の検証には Continuity Check Messages（CCM; 接続性チェック メッセージ）が最適ですが、これはディザスタ リカバリ用に最適化されています。SLA とディザスタ リカバリには時間的尺度に差があるため、CCM は通常は SLA のコンポーネントとして認められません。したがって、接続性の検証には接続障害監理（CFM）と Continuity Check Database（CCDB; 接続性チェック データベース）が使用されます。CFM の詳細については、http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1608025 を参照してください。

フレーム遅延とフレーム遅延変動

Ethernet frame Delay Measurement（ETH-DM; イーサネット フレーム遅延測定）をオンデマンドのイーサネット Operations, Administration & Maintenance（OAM）に使用して、フレーム遅延とフレーム遅延変動を測定します。

イーサネット フレーム遅延およびフレーム遅延変動は、ETH-DM 情報が含まれた周期的フレームをピア MEP に送信し、ピア MEP から ETH-DM 情報が含まれた周期的フレームを受信することで測定されます。この間に、各 MEP はフレーム遅延とフレーム遅延変動を測定します

イーサネット フレーム遅延測定では、最悪および最高の状態の遅延、平均遅延、平均遅延変動などの有益な情報も収集されます。イーサネット フレーム遅延測定では、入力方向のタイムスタンプがハードウェアベースで記録されます。これにより、双方向の遅延測定中に遅延の統計情報を実行時表示することができます。イーサネット フレーム遅延測定では、リモート Maintenance End Point（MEP; メンテナンス エンド ポイント）または CFM セッションごとに収集された直近の 100 サンプルが記録されます。

ITU-T Y.1731 標準では、次の 2 通りの遅延測定方法が規定されています。

- **1 方向 ETH-DM**
  各 MEP は、1 方向の ETH-DM 情報が含まれたフレームをポイントツーポイント ME 内のピア MEP に送信し、ピア MEP での 1 方向フレーム遅延測定および 1 方向フレーム遅延変動測定を支援します。1 方向フレーム遅延は両端のクロックが同期している必要がありますが、フレーム遅延変動ではクロックの同期は必要ありません。この測定では、Single Delay Measurement（1DM; 単一の遅延測定）または Delay Measurement Message（DMM; 遅延測定メッセージ）と Delay Measurement Reply（DMR; 遅延測定応答）フレームを組み合わせて使用します。
- **双方向 ETH-DM**
  各 MEP は、ETH-DM 要求情報が含まれたフレームをピア MEP に送信し、ピア MEP から ETH-DM 応答情報が含まれたフレームを受信します。双方向フレーム遅延およびフレーム遅延変動は、DMM および DMR フレームを使用して測定されます。

1DM 測定の前提条件を次に示します。

- 測定を行う 2 つのエンド ポイントのクロックが正確かつ的確に同期する。これは、IEEE 1588-2002 によって実現されます。
- 自動セッション作成がピアまたはレシーバでサポートされていません。受信専用セッションを設定する必要があります。
- すべてのセッション作成はレシーバのデータパスに設定する。これらはパッシブ リスナー セッションです。

（注）　Cisco 7600 ルータでは、2 ポートのギガビット同期イーサネット SPA を使用してクロックを同期させます。ES+ ラインカード上で、Precision Time Protocol（PTP; 高精度時間プロトコル）を時刻源プロトコルとして使用し、Real Time Clock（RTC; リアル タイム クロック）が 2 ポート ギガビット同期イーサネット SPA の時刻源と同期します。PTP が時刻源として選択されると、すべての Y.1731 PM 遅延パケットに 1588V2 のタイムスタンプが付けられます。

2 ポート ギガビット同期イーサネット SPA を搭載していない 7600 ルータの場合は、タイムスタンプと、時刻源プロトコルとしてネットワーク タイム プロトコル（NTP）を使用し、遅延測定が行われます。これは 1 方向遅延測定のみに当てはまります。
ラインカードで Time of Day（ToD）同期を開始するには、グローバル コンフィギュレーション モードで **platform time-source** コマンドを使用します。**platform time source** コマンドの詳細については、http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html を参照してください。

フレームの損失率および可用性

Ethernet frame Loss Measurement（ETH-LM; イーサネット フレーム損失測定）は、入力および出力サービス フレームに適用されるカウンタ値の収集に使用されます。このカウンタには、MEP ペアの間で送受信されるデータ フレーム数が計上されます。

ETH-LM は、ETH-LM 情報が含まれたフレームをピア MEP に送信し、同じく ETH-LM 情報が含まれたフレームをピア MEP から受信します。各 MEP はフレーム損失測定を実行し、これによって利用不能時間が発生します。ニアエンド フレーム損失とは、入力データ フレームに関連するフレーム損失を指します。遠端フレーム損失とは、出力データ フレームに関連するフレーム損失を指します。近端および遠端フレーム損失測定の両方が、使用不可時間を生じる近端重大エラー秒数および遠端重大エラー秒数に関係します。

ITU-T Y.1731 標準では、次の 2 つのフレーム損失測定方法が規定されています。

- **シングルエンド ETH-LM**：各 MEP は、ETH-LM 要求情報が含まれたフレームをピア MEP に送信し、ETH-LM 応答情報が含まれたフレームをピア MEP から受信して損失を測定します。

- **両終端 ETH-LM :** 各 MEP は、ETH-LM 情報が含まれた定期的な両終端フレームをポイントツーポイント ME のピア MEP に送信し、ピア MEP でのフレーム損失測定を容易にします。現在、Cisco 7600 ルータは、両終端 ETH-LM をサポートしていません。

サポートされるインターフェイス

Y.1731 PM は次のインターフェイスをサポートします。

- EVC BD OFM の LMM、DMM、1DM サポート
- PC EVC BD OFM の LMM、DMM、1DM サポート
- EVC Xconnect OFM の LMM、DMM、1DM サポート
- PC の EVC Xconnect OFM の LMM、DMM、1DM サポート
- EVC Xconnect IFM の LMM、DMM、1DM サポート
- PC の EVC Xconnect IFM の LMM、DMM、1DM サポート
- サブインターフェイス（ルーテッド ポート）の LMM、DMM、1DM サポート
- PC のサブインターフェイス（ルーテッド ポート）の LMM、DMM、1DM サポート

（注） PM は、EVC で使用できる Dot1q および QinQ カプセル化の両方によって、上記の EVC と CFM の設定でサポートされます。

制約事項および使用上の注意事項

ES+ ラインカード上で Y.1731 PM を設定する場合は、次の制約事項と使用上のガイドラインに従ってください。

- ルート プロセッサ CPU が他のプロセスで使用中の場合やソフトウェア転送を使用する場合、パフォーマンス モニタリング統計情報は正確ではありません。
- Y.1731 PM 測定は、ポイントツーポイントのネットワーク トポロジでのみ有効に機能します。
- Y.1731 PM は SSO 準拠ではありません。スイッチオーバー後はすべてのセッション データがクリアされ、IPSLA の再起動が必要になります。
- 1 方向セッションまたは双方向セッションで 1 方向の統計情報が必要な場合は、PTP がピア間で同期し、安定している必要があります。このような場合はセッションの開始を遅らせる必要があります。
- Cisco 7600 シリーズ ルータでは、ES+ ラインカードはスイッチポート非対応モードでのみサポートされます。PM はポート MEP ではサポートされません。
- PM は、次のインターフェイスではサポートされません。
  - mLACP インターフェイス
  - EVC BD IFM
  - スイッチポート OFM および IFM
  - ポート MEP
- PM は、VPLS の設定ではサポートされません。
- CFM がこれらのインターフェイスでサポートされないため、PM は Qinq サブインターフェイスでサポートされません。
- CLI とシステム ロギングはサポートされますが、PM は SNMP をサポートしません。

- フレームのスループットの測定はサポートされません。

ポートチャネルの PM サポートの制約事項は次のとおりです。

- メンバー リンクを追加または削除すると、セッションが無効になります。
- ポートチャネル インターフェイスでの損失測定は、ポートチャネルのすべての物理インターフェイスが 1 つの NPU 上にある場合のみサポートされます。この制約は遅延測定には適用されません。
- すべてのメンバー リンクに ES+ ポートが搭載されている必要があります。
- 手動の PC EVC ロード バランシング設定（UNI LAG）では PM はサポートされません。

Y.1731 PM の設定

Y.1731 PM の設定については、http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html を参照してください。

CHAPTER 70

マルチキャスト サービス リフレクション

マルチキャスト サービス リフレクション機能は、外部で受信したマルチキャスト宛先アドレスを組織の内部アドレッシング ポリシーに準拠したアドレスに変換できます。この機能を使用すると、リバース パス転送（RPF）を正常に機能させるために、変換境界の自社のネットワーク インフラストラクチャにルートを再配信する必要はありません。さらに、ネットワークの 2 つの入力点から同じフィードを受け取り、個別にルーティングすることができます。

マルチキャスト サービス リフレクション機能は、仮想インターフェイスで設定されます。パケットが仮想インターフェイス（元の IP）に転送される場合、この機能は内部 IP アドレスに元の IP アドレスをマップし、トラフィックは内部 IP アドレスに転送されます。したがって、組織はプライベートとパブリックのマルチキャスト ネットワークを論理的に分離できます。

マルチキャスト サービス リフレクションの機能アーキテクチャ

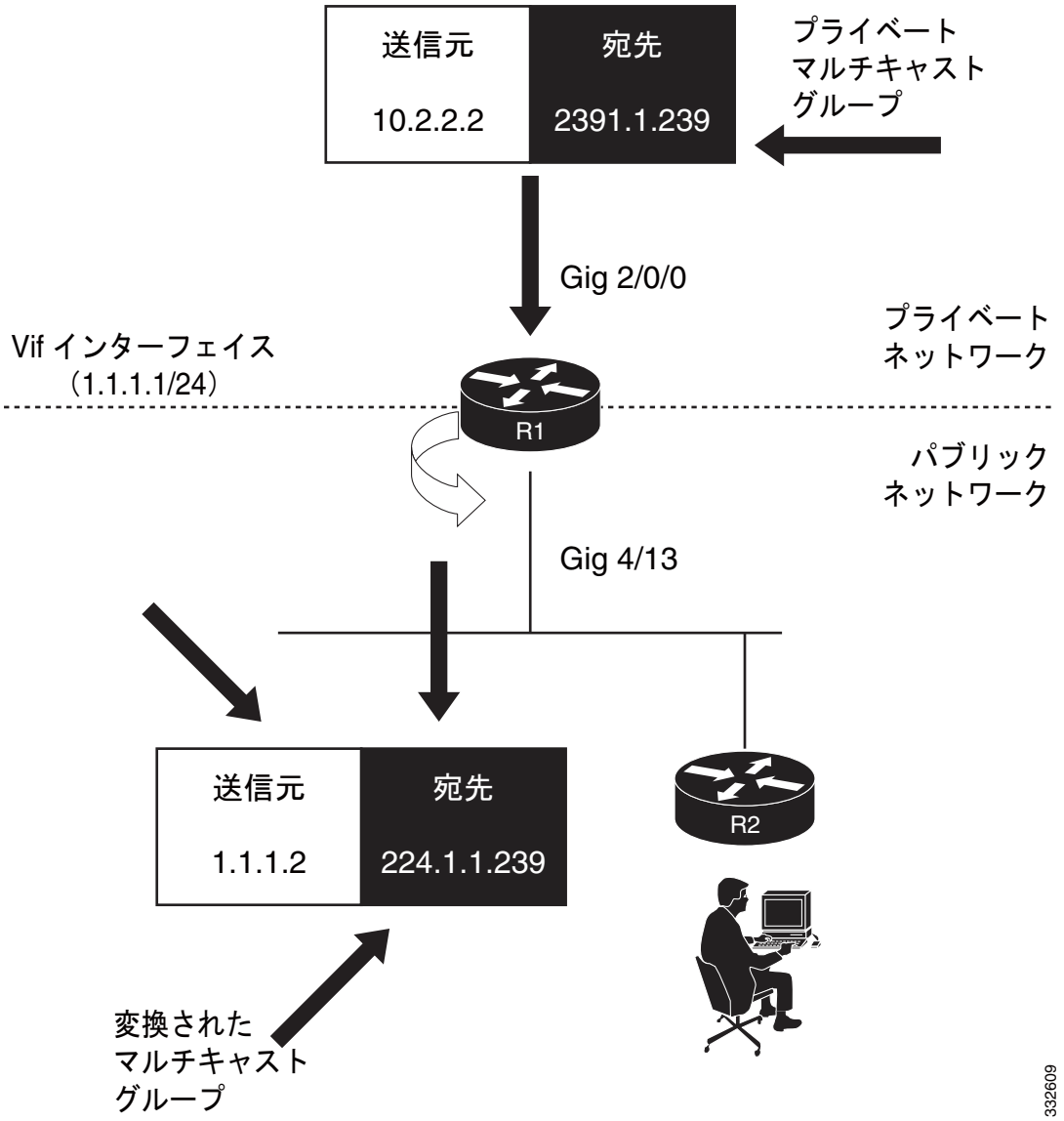
マルチキャスト サービス リフレクションでは、マルチキャスト ツリーを構築するために変換する必要があるグループにスタティックに参加するように仮想インターフェイスが設定されています。仮想インターフェイスは、次の情報を維持します。

- 入力インターフェイス
- プライベートからパブリックへのマルチキャスト グループ マッピング
- プール範囲を定義するマスク長
- 変換済みパケットの送信元

パケットが仮想インターフェイスに転送された場合、変換に反映されます。送信元 IP アドレスは RPF 障害を防ぐ仮想インターフェイス サブネットの IP アドレスに変更されます。最後に、宛先 IP アドレスは新しいマルチキャスト グループ IP アドレスに変換されます。

図 70-1 に、マルチキャスト サービス リフレクションの機能アーキテクチャを示します。

図 70-1　　マルチキャスト サービス リフレクションの機能アーキテクチャ



マルチキャスト サービス リフレクションの制約事項

次の制限は、マルチキャスト サービス リフレクション機能に適用されます。

- 仮想インターフェイスは、ボーダー ルータにインストールする必要があります。
- マルチキャスト サービス リフレクションでは、双方向マルチキャストはサポートされていません。
- Protocol Independent Multicast（PIM）/IGMP の制御パケットは変換されません。

- マルチキャスト サービス リフレクションは、P2P GRE トンネリングをサポートしません。
- マルチキャスト サービス リフレクションは、IPv6 マルチキャストをサポートしません。
- 1000 サービス リフレクション変換のみサポートされます。
- マルチキャスト サービス リフレクションは、PIM デンス モードではサポートされません。

マルチキャスト サービス リフレクションの設定

マルチキャスト サービス リフレクション機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface loopback** *loopback_id*
5. **description** *description*
6. **ip address** *ip_address subnet_mask*
7. **ip pim sparse-mode**
8. **exit**
9. **interface gigabitEthernet** *slot/port*
10. **ip address** *ip_address subnet_mask*
11. **ip pim sparse-mode**
12. **exit**
13. **interface gigabitEthernet** *slot/port*
14. **ip address** *ip_address subnet_mask*
15. **ip pim sparse-mode**
16. **exit**
17. **interface** *vif_id*
18. **ip address** *ip_address subnet_mask*
19. **ip pim sparse-mode**
20. **ip service reflect** *interface_id* **destination** *destination_ip1* to *destination_ip2* **mask-len** *subnet_mask_length* **source** *source_ip*
21. **ip igmp static-group** {* | *group-address* [**source** {*source-address* | **ssm-map**}]}
22. **exit**
23. **ip pim rp-address** *rp_address*
24. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** R1> enable	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** R1# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**distributed**] **例：** R1(config)# ip multicast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**interface loopback** loopback_if_number **例：** R1(config)# interface Loopback0	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	**description** description **例：** R1(config-if)# description Rendezvous Point for Public Net	インターフェイスについての説明です。
ステップ 6	ip address ip_address subnet_mask **例：** R1(config-if)# ip address 22.22.22.22 255.255.255.255	IP アドレスとサブネット マスクをインターフェイスに割り当てます。
ステップ 7	**ip pim sparse-mode** **例：** R1(config-if)# ip pim sparse-mode	インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 8	**exit** **例：** R1(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 9	**interface gigabitethernet** GigabitEthernet_interface_number **例：** R1(config)# interface GigabitEthernet2/0/0	インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 10	**ip address** ip_address subnet_mask **例：** R1(config-if)# ip address 2.1.1.1 255.255.0.0	IP アドレスとサブネット マスクをインターフェイスに割り当てます。
ステップ 11	**ip pim sparse-mode** **例：** R1(config-if)# ip pim sparse-mode	インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 12	**exit** **例：** R1(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 13	**interface gigabitethernet** GigabitEthernet_interface_number **例：** R1(config)# interface GigabitEthernet4/13	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 14	**ip address** ip_address subnet_mask **例：** R1(config-if)# ip address 23.1.1.2 255.255.0.0	IP アドレスとサブネット マスクをインターフェイスに割り当てます。
ステップ 15	**ip pim sparse-mode** **例：** R1(config-if)# ip pim sparse-mode	インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 16	**exit** **例：** R1(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 17	**interface** interface_name **例：** R1(config)# interface Vif1	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 18	**ip address** ip_address subnet_mask **例：** R1(config-if)# ip address 1.1.1.1 255.255.0.0	IP アドレスとサブネット マスクをインターフェイスに割り当てます。

	コマンド	目的
ステップ 19	**ip pim sparse-mode** **例：** R1(config-if)# ip pim sparse-mode	インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 20	**ip service reflect** input-interface **destination** destination-address **to** new-destination-address **mask-len** number **source** new-source-address **例：** R1(config-if)# ip service reflect GigabitEthernet2/0/0 destination 239.1.1.100 to 225.1.1.100 mask-len 32 source 1.1.1.2	仮想インターフェイスにルーティングされたマルチキャスト パケットを照合し、リライトします。 • 照合およびリライトされたパケットは、マルチキャスト パケット ルーティング（または宛先がユニキャストの場合はユニキャスト ルーティング）に戻され、インターフェイスから到着した他のパケットのように処理されます。
ステップ 21	**ip igmp static-group {* |** group-address **[source {**source-address **| ssm-map}]}** **例：** R1(config-if)# ip igmp static-group 239.1.1.100	インターフェイス上で指定グループのスタティックに接続されたメンバとしてルータを設定し、マルチキャスト グループ宛のトラフィックをインターフェイスに転送します。 **（注）** この手順は、マルチキャストからマルチキャストおよびマルチキャストからユニキャストへのシナリオのみに適用されます。
ステップ 22	**exit** **例：** R1(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 23	**ip pim rp-address** rp-address **例：** R1(config)# ip pim rp-address 22.22.22.22	特定のグループの PIM RP のアドレスを設定します。
ステップ 24	**end** **例：** R1(config-controller)# end	コンフィギュレーション セッションを終了します。

設定例

次に、マルチキャスト サービス リフレクションを設定する方法について説明します。

```
R11>enable
R11#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R11(config)#ip multicast-routing
R11(config)#interface Loopback0
```

```
R11(config-if)#description Rendezvous Point for Public Net
R11(config-if)#ip address 22.22.22.22 255.255.255.255
R11(config-if)#ip pim sparse-mode
R11(config-if)#exit

R11(config)#interface GigabitEthernet2/0/0

R11(config-if)#ip address 2.1.1.1 255.255.0.0

R11(config-if)#ip pim sparse-mode
R11(config-if)#exit

R11(config)#interface GigabitEthernet4/13
R11(config-if)#ip address 23.1.1.2 255.255.0.0
R11(config-if)#ip pim sparse-mode
R11(config-if)#exit

R11(config)#interface Vif1
R11(config-if)#ip address 1.1.1.1 255.255.0.0
R11(config-if)#ip pim sparse-mode
R1(config-if)#ip service reflect GigabitEthernet2/0/0 destination 239.1.1.100 to
225.1.1.100 mask-len 32 source 1.1.1.2
R1(config-if)#ip igmp static-group 239.1.1.100
R1(config-if)#exit
R1(config)#ip pim rp-address 22.22.22.22
R1(config)#exit
```

マルチキャスト サービス リフレクションの設定の詳細については、「Configuring Multicast Service Reflection」を参照してください。

APPENDIX A

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、使用方法の推奨事項を提供します。

オンライン診断テストは、次のカテゴリに分類されます。

- 「グローバル ヘルス モニタリング テスト」（P.A-1）
- 「ポート単位のテスト」（P.A-3）
- 「PFC レイヤ 2 フォワーディング エンジン テスト」（P.A-6）
- 「DFC レイヤ 2 フォワーディング エンジン テスト」（P.A-8）
- 「PFC レイヤ 3 フォワーディング エンジン テスト」（P.A-14）
- 「DFC レイヤ 3 フォワーディング エンジン テスト」（P.A-19）
- 「レプリケーション エンジン テスト」（P.A-25）
- 「ファブリック テスト」（P.A-26）
- 「完全メモリ テスト」（P.A-29）
- 「IPSEC サービス モジュール テスト」（P.A-32）
- 「ストレス テスト」（P.A-33）
- 「クリティカル リカバリ テスト」（P.A-34）
- 「一般的なテスト」（P.A-36）

オンライン診断テストの設定については、第 39 章「オンライン診断の設定」を参照してください。

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 テストは、次のテストで構成されます。

「TestSPRPInbandPing」（P.A-2）

「TestMacNotification」（P.A-3）

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 秒間隔で送信されます。

表 A-1　TestSPRPInbandPing テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	ディセーブルにしないでください。CPU 使用率でスパイクが発生すると、精度を保つためにテストが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	12.2(33)SRA 以降
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 テストは、レジスタに値を書き込み、これらのレジスタからその値を読み取ることで、特定用途向け集積回路（ASIC）のヘルスをモニタします。テストは、30 秒ごとに実行されます。テストが連続して 5 回失敗すると、スーパーバイザ エンジンをテストしている場合はスーパーバイザ エンジンがスイッチオーバー（またはリセット）し、モジュールをテストしている場合はモジュールの電源が切断されます。

表 A-2　TestScratchRegister テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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(33)SRA 以降
修正措置	誤作動しているスーパーバイザ エンジンをリセットするか、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 を装備したモジュール、WS-X6148-FE-SFP、WS-X6148A-GE-TX、および WS-X6148A-RJ-45

TestMacNotification

TestMacNotification テストは、DFC モジュールとスーパーバイザ エンジン間のデータとコントロール パスが正常に動作していることを確認します。このテストは、また、レイヤ 2 MAC アドレス テーブルにおいてレイヤ 2 MAC アドレスの一貫性を保ちます。テストは、6 秒ごとに実行されます。テストが連続して 10 回失敗すると、起動時または実行時にモジュールがリセットされます（デフォルト）。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。

表 A-3　TestMacNotification テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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(33)SRA 以降
修正措置	モジュールをリセットします。モジュールが 10 回連続して失敗した場合、または 3 回連続してリセットされた場合、電源が切断されます。
ハードウェア サポート	DFC が装備されたモジュール。

ポート単位のテスト

ポート単位のテストは、次のテストで構成されます。

「TestNonDisruptiveLoopback」（P.A-3）
「TestLoopback」（P.A-4）
「TestActiveToStandbyLoopback」（P.A-4）
「TestTransceiverIntegrity」（P.A-5）
「TestNetflowInlineRewrite」（P.A-5）

TestNonDisruptiveLoopback

TestNonDisruptiveLoopback テストは、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 パスを検証します。このテストでは、テスト ポートのグループを含む VLAN にレイヤ 2 パケットがフラッディングします。テスト ポート グループは、ポート ASIC チャネル当たり 1 つのポートで構成されています。テスト ポート グループの各ポートは、パケットを中断せずにループバックし、スーパーバイザ エンジンのインバンド ポートに送り返します。テスト ポート グループの複数のポートが同時にテストされます。

表 A-4　TestNonDisruptiveLoopback テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	ディセーブルにしないでください。

表 A-4　TestNonDisruptiveLoopback テストの属性 （続き）

デフォルト	オン。
リリース	12.2(33)SRA 以降
修正措置	連続して 10 回失敗すると、エラーによってポートがディセーブルになります。1 つのテスト サイクルですべてのポートがテストに失敗すると、エラーによってチャネルがディセーブルになります。すべてのチャネルが失敗する場合は、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 パスを検証します。このテストでは、テスト ポートおよびスーパーバイザ エンジンのインバンド ポートだけで構成されている VLAN にレイヤ 2 パケットがフラッディングします。パケットはポートにループバックし、同一 VLAN 上のスーパーバイザ エンジンに戻ります。

表 A-5　TestLoopback テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	起動時または活性挿抜（OIR）を行ったあとに実行します。
リリース	12.2(33)SRA 以降
修正措置	ポートでループバック テストが失敗する場合、エラーによってポートがディセーブルになります。すべてのポートが失敗する場合は、モジュールをリセットします。
ハードウェア サポート	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 パスを検証します。このテストでは、テスト ポートおよびスーパーバイザ エンジンのインバンド ポートだけで構成されている VLAN にレイヤ 2 パケットがフラッディングします。テスト パケットはターゲット ポートでループバックし、バスにフラッディングバックします（フラッディングされた VLAN では、アクティブ スーパーバイザ エンジンのインバンド ポートだけがリスニングします）。

表 A-6　TestActiveToStandbyLoopback テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	起動時または OIR を行ったあとに実行します。
リリース	12.2(33)SRA 以降
修正措置	ポートでループバック テストが失敗する場合、エラーによってポートがディセーブルになります。すべてのポートが失敗する場合は、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	スタンバイ スーパーバイザ エンジンだけ

TestTransceiverIntegrity

TestTransceiverIntegrity テストは、トランシーバで活性挿抜（OIR）を行ったときまたはモジュールを起動したときに、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に、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
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	該当なし。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
修正措置	エラーによってポートがディセーブルになります。
ハードウェア サポート	トランシーバを使用するすべてのモジュール

TestNetflowInlineRewrite

TestNetflowInlineRewrite テストは、NetFlow 検索操作、ACL の許可/拒否機能、およびポート ASIC のインライン書き換え機能を検証します。テスト パケットは、NetFlow テーブル ルックアップを通じて書き換え情報を取得します。パケットがターゲット ポートに到着すると、VLAN および送信元/宛先 MAC アドレスが書き換えられます。

表 A-8　TestNetflowInlineRewrite テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。中断時間は、ループバック ポート（スパニングツリー プロトコルなど）の設定によって異なります。
推奨事項	ダウンタイムにスケジューリングします。このテストは、起動時にだけ実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 フォワーディング エンジン テスト

PFC レイヤ 2 フォワーディング エンジン テストは、次のテストで構成されます。

「TestNewIndexLearn」（P.A-6）
「TestDontConditionalLearn」（P.A-7）
「TestBadBpduTrap」（P.A-7）
「TestMatchCapture」（P.A-8）
「TestStaticEntry」（P.A-8）

TestNewIndexLearn

TestNewIndexLearn テストは、TestNewLearn テストと TestIndexLearn テストの組み合わせです（「DFC レイヤ 2 フォワーディング エンジン テスト」（P.A-8）を参照）。

表 A-9　TestNewIndexLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降

表 A-9　TestNewIndexLearn テストの属性 （続き）

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 テストと TestConditionalLearn テストの組み合わせです（「DFC レイヤ 2 フォワーディング エンジン テスト」（P.A-8）を参照）。

表 A-10　TestDontConditionalLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストと TestBadBpdu テストの組み合わせです（「DFC レイヤ 2 フォワーディング エンジン テスト」（P.A-8）を参照）。

表 A-11　TestBadBpduTrap テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
推奨事項	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストと TestCapture テストの組み合わせになります（「DFC レイヤ 2 フォワーディング エンジン テスト」（P.A-8）を参照）。

表 A-12　TestMatchCapture テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
推奨事項	このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テーブルに読み込まれていることを確認します。この機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-13　TestStaticEntry テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
推奨事項	レイヤ 2 フォワーディング エンジンの学習機能で問題が発生している場合、このテストをオンデマンドで実行して、レイヤ 2 の学習機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 フォワーディング エンジン テスト

DFC レイヤ 2 フォワーディング エンジン テストは、次のテストで構成されます。

「TestDontLearn」（P.A-9）

「TestNewLearn」（P.A-9）
「TestIndexLearn」（P.A-10）
「TestConditionalLearn」（P.A-10）
「TestTrap」（P.A-11）
「TestBadBpdu」（P.A-12）
「TestProtocolMatchChannel」（P.A-12）
「TestCapture」（P.A-13）
「TestStaticEntry」（P.A-13）

TestDontLearn

TestDontLearn テストは、新しい送信元 MAC アドレスが学習されないときに、新しい送信元 MAC アドレスが MAC アドレス テーブルに読み込まれていないことを確認します。このテストは、レイヤ 2 フォワーディング エンジンの don't learn 機能が正常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。「don't learn」機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-14　TestDontLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 2 フォワーディング エンジンのレイヤ 2 送信元 MAC アドレス ラーニング機能を検証します。スーパーバイザ エンジンの場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、レイヤ 2 フォワーディング 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が確認されます。DFC 対応モジュールの場合、スーパーバイザ エンジンのインバンド ポートからスイッチ ファブリックを介して診断パケットが送信され、DFC 対応モジュールの 1 つのポートからループバックされます。レイヤ 2 学習機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-15　TestNewLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、既存の MAC アドレス テーブルのエントリが更新可能であることを確認します。このテストは、レイヤ 2 フォワーディング エンジンの Index Learn 機能が正常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、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-16　TestIndexLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、特定の条件下でレイヤ 2 送信元 MAC アドレスを学習する機能を検証します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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

エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、DFC ポートのいずれかからループ バックされます。Conditional Learn 機能は、レイヤ 2 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-17　TestConditionalLearn テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、スイッチ プロセッサに対するパケットのトラップまたはリダイレクトの機能を検証します。このテストは、レイヤ 2 フォワーディング エンジンの Trap 機能が正常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、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-18　TestTrap テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、スイッチ プロセッサに対するパケットのトラップまたはリダイレクトの機能を検証します。このテストは、レイヤ 2 フォワーディング エンジンの Trap 機能が正常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、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-19　TestBadBpdu テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 2 フォワーディング エンジンの特定のレイヤ 2 プロトコルを照合する機能を検証します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-20　TestProtocolMatchChannel テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降

表 A-20　TestProtocolMatchChannel テストの属性 （続き）

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 テストは、レイヤ 2 フォワーディング エンジンのキャプチャ機能が正常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、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-21　TestCapture テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 2 MAC アドレス テーブルにスタティック エントリを読み込む機能を検証します。スーパーバイザ エンジンでテストを実行する場合、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信され、スーパーバイザ エンジンのレイヤ 2 フォワーディング エンジンを使用してパケット検索を実行します。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 エンジンのインバンド ポートからスイッチ ファブリックを介して送信され、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 フォワーディング エンジンによる診断パケット検索の実行時に検証されます。

表 A-22　TestStaticEntry テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。

表 A-22　TestStaticEntry テストの属性 （続き）

推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 フォワーディング エンジン テスト

PFC レイヤ 3 フォワーディング エンジン テストは、次のテストで構成されます。

「TestFibDevices」（P.A-14）
「TestIPv4FibShortcut」（P.A-15）
「TestIPv6FibShortcut」（P.A-15）
「TestMPLSFibShortcut」（P.A-16）
「TestNATFibShortcut」（P.A-16）
「TestL3Capture2」（P.A-17）
「TestAclPermit」（P.A-17）
「TestAclDeny」（P.A-18）
「TestQoS」（P.A-19）

TestFibDevices

TestFibDevices テストは、FIB TCAM および隣接デバイスが機能しているかどうかを確認します。各 FIB TCAM デバイスに FIB エントリが 1 つインストールされています。診断パケットが送信され、TCAM デバイスにインストールされた FIB TCAM エントリによって診断パケットがスイッチングされていることが確認されます。これは、完全な TCAM デバイス テストではありません。各 TCAM デバイスにはエントリが 1 つしかインストールされていません。

（注）　IPv4FibShortcut テストおよび IPv6FibShortcut テストと比べた場合、このテストは、設定に応じて IPv4 または IPv6 パケットを使用して、すべての FIB および隣接デバイスをテストします。

表 A-23　TestFibDevices テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	ルーティング機能で問題が発生している場合は、このテストをオンデマンドで実行して、レイヤ 3 フォワーディング機能を検証します。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。

表 A-23　TestFibDevices テストの属性 （続き）

デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの IPV4 FIB フォワーディングが正常に動作していることを確認します。1 つの診断 IPV4 FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-24　TestIPv4FibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	ルーティング機能で問題が発生している場合は、このテストをオンデマンドで実行して、レイヤ 3 フォワーディング機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの IPV6 FIB フォワーディングが正常に動作していることを確認します。1 つの診断 IPV6 FIB と隣接エントリがインストールされています。診断 IPV6 パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-25　TestIPv6FibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。

表 A-25　TestIPv6FibShortcut テストの属性 （続き）

推奨事項	ルーティング機能で問題が発生している場合は、このテストをオンデマンドで実行して、レイヤ 3 フォワーディング機能を検証します。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	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの MPLS フォワーディングが正常に動作していることを確認します。1 つの診断 MPLS FIB と隣接エントリがインストールされています。診断 MPLS パケットが送信され、隣接エントリの MPLS ラベルに応じて診断パケットが転送されていることが確認されます。

表 A-26　TestMPLSFibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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する場合は、ヘルス モニタリング テストとして使用してください。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、NAT 隣接情報に基づいてパケットを書き換える機能（宛先 IP アドレスの書き換え）を検証します。1 つの診断 NAT FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた IP アドレスに応じて診断パケットが転送されていることが確認されます。

表 A-27　TestNATFibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。

表 A-27　TestNATFibShortcut テストの属性 （続き）

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は、ヘルス モニタリング テストとして使用してください（たとえば、NAT を使用している場合）。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が正常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 ロギングに使用されます。1 つの診断 FIB およびキャプチャ 2 ビット セット付きの隣接エントリがインストールされています。診断パケットが送信され、キャプチャ ビット情報に応じて診断パケットが転送されていることが確認されます。

表 A-28　TestL3Capture2 テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
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てください。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、ACL 許可機能が正常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 エントリが ACL TCAM にインストールされています。診断パケットが ACL TCAM エントリに一致し、適切に許可および転送されていることを確認するために、スーパーバイザ エンジンから対応する診断パケットが送信され、レイヤ 3 フォワーディング エンジンで検索されます。

表 A-29　TestACLPermit テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
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てください。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 2 およびレイヤ 3 フォワーディング エンジンの ACL 拒否機能が正常に動作していることを確認します。テストでは、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 ブリッジなどの各種の ACL 拒否シナリオを使用して、ACL 拒否機能が正常に動作しているかどうかを調べます。

表 A-30　TestACLDeny テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ
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(33)SRA 以降
修正措置	自動 ASIC リセット（リカバリ用）
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 テストは、レイヤ 3 フォワーディング エンジンの NetFlow フォワーディング機能が正常に動作していることを確認します。1 つの診断 NetFlow エントリと隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-31　TestNetflowShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断時間は、500 ミリ秒です。

表 A-31　TestNetflowShortcut テストの属性 （続き）

推奨事項	NetFlow が正常に動作していないと考えられる場合は、このテストをオンデマンドで実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、診断パケットの ToS 値が入力または出力を反映するために変更されるように、QoS 入力および出力 TCAM をプログラミングして、QoS 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。

表 A-32　TestQoS テストの属性

属性	**説明**
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断時間は、500 ミリ秒です。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 フォワーディング エンジン テスト

DFC レイヤ 3 フォワーディング エンジン テストは、次のテストで構成されます。

「TestFibDevices」（P.A-20）
「TestIPv4FibShortcut」（P.A-20）
「TestIPv6FibShortcut」（P.A-21）
「TestMPLSFibShortcut」（P.A-21）
「TestNATFibShortcut」（P.A-22）
「TestL3Capture2」（P.A-22）
「TestAclPermit」（P.A-23）
「TestAclDeny」（P.A-23）
「TestQoS」（P.A-24）
「TestNetflowShortcut」（P.A-24）

TestFibDevices

TestFibDevices テストは、FIB TCAM および隣接デバイスが機能していることを確認します。1 つの FIB エントリが各 FIB TCAM デバイスにインストールされています。診断パケットが送信され、TCAM デバイスにインストールされた FIB TCAM エントリによって診断パケットがスイッチングされていることが確認されます。これは、完全な TCAM デバイス テストではありません。各 TCAM デバイスにはエントリが 1 つしかインストールされていません。

（注）　IPv4FibShortcut テストおよび IPv6FibShortcut テストに対し、TestFibDevices テストは、設定に応じて IPv4 または IPv6 パケットを使用して、すべての FIB および隣接デバイスをテストします。

表 A-33　TestFibDevices テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの IPv4 FIB フォワーディング機能が正常に動作していることを確認します。1 つの診断 IPv4 FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-34　TestIPv4FibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降

表 A-34　TestIPv4FibShortcut テストの属性 （続き）

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 テストは、レイヤ 3 フォワーディング エンジンの IPv6 FIB フォワーディング機能が正常に動作していることを確認します。1 つの診断 IPv6 FIB と隣接エントリがインストールされています。診断 IPv6 パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-35　TestIPv6FibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの MPLS フォワーディング機能が正常に動作していることを確認します。1 つの診断 MPLS FIB と隣接エントリがインストールされています。診断 MPLS パケットが送信され、隣接エントリの MPLS ラベルを使用して診断パケットが転送されていることが確認されます。

表 A-36　TestMPLSFibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降

表 A-36　TestMPLSFibShortcut テストの属性 （続き）

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 テストは、NAT 隣接情報に基づいてパケットを書き換える機能（宛先 IP アドレスの書き換えなど）を検証します。1 つの診断 NAT FIB と隣接エントリがインストールされています。診断パケットが送信され、書き換えられた IP アドレスに応じて診断パケットが転送されていることが確認されます。

表 A-37　TestNATFibShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンのレイヤ 3 キャプチャ（キャプチャ 2）機能が正常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 ロギングに使用されます。1 つの診断 FIB およびキャプチャ 2 ビット セット付きの隣接エントリがインストールされています。診断パケットが送信され、キャプチャ ビット情報に応じて診断パケットが転送されていることが確認されます。

表 A-38　TestL3Capture2 テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降

表 A-38　TestL3Capture2 テストの属性 （続き）

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 テストは、ACL 許可機能が正常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 エントリが ACL TCAM にインストールされています。診断パケットが ACL TCAM エントリに一致し、正常に許可および転送されていることを確認するために、スーパーバイザ エンジンから対応する診断パケットが送信され、レイヤ 3 フォワーディング エンジンで検索されます。

表 A-39　TestACLPermit テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 2 およびレイヤ 3 フォワーディング エンジンの ACL 拒否機能が正常に動作していることを確認します。テストでは、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 ブリッジなどの各種の ACL 拒否シナリオを使用します。

表 A-40　TestACLDeny テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。
推奨事項	ACL を使用している場合は、ダウンタイムにスケジューリングします。
デフォルト	オフ。
リリース	12.2(33)SRA 以降

表 A-40　TestACLDeny テストの属性 （続き）

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 テストは、診断パケットの ToS 値が入力または出力を反映するために変更されるように、QoS 入力および出力 TCAM をプログラミングして、QoS 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。

表 A-41　TestQoS テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。
推奨事項	ダウンタイムにスケジューリングします。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、レイヤ 3 フォワーディング エンジンの NetFlow フォワーディング機能が正常に動作していることを確認します。1 つの診断 NetFlow エントリと隣接エントリがインストールされています。診断パケットが送信され、書き換えられた MAC および VLAN 情報に応じて診断パケットが転送されていることが確認されます。

表 A-42　TestNetflowShortcut テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ループバック ポートの場合は、ディスラプティブです。中断する時間は、通常、1 秒未満です。
推奨事項	NetFlow が正常に動作していないと考えられる場合は、このテストをオンデマンドで実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、次のテストで構成されます。

「TestL3VlanMet」（P.A-25）
「TestIngressSpan」（P.A-25）
「TestEgressSpan」（P.A-26）

TestL3VlanMet

TestL3VlanMet テストは、レプリケーション エンジンのマルチキャスト機能が正常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、2 つの異なる VLAN に診断パケットのマルチキャスト レプリケーションを実行するように設定されています。テストでは、スーパーバイザ エンジンのインバンド ポートから診断パケットが送信されたあと、レプリケーション エンジンに設定された 2 つの VLAN のインバンド ポートに 2 つのパケットが送り返されていることを確認します。

表 A-43　TestL3VlanMet テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	スーパーバイザ エンジンの場合は、ノンディスラプティブです。 DFC が装備されたモジュールの場合は、ディスラプティブです。ループバック ポートで中断される時間は、通常、1 秒未満です。
推奨事項	このテストをオンデマンドで実行して、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します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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、WS-65xx モジュール、WS-67xx モジュール、および WS-68xx モジュール

TestIngressSpan

TestIngressSpan テストは、ポート ASIC が入力 SPAN のパケットにタグを付けることができることを確認します。このテストは、両方の SPAN キューに対する書き換えエンジンの入力 SPAN 操作が正常に動作していることも確認します。

表 A-44　TestIngressSpan テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	両方の SPAN セッションで、ディスラプティブです。モジュール上のループバック ポートの場合も、ディスラプティブです。中断時間は、ループバック ポート（スパニング ツリー プロトコルなど）の設定によって異なります。
推奨事項	このテストをオンデマンドで実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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、WS-65xx モジュール、および WS-67xx モジュール

TestEgressSpan

TestEgressSpan テストは、両方の SPAN キューに対する書き換えエンジンの出力 SPAN レプリケーション機能が正常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
ディスラプティブ/ノンディスラプティブ	両方の SPAN セッションで、ディスラプティブです。中断する時間は、通常、1 秒未満です。
推奨事項	このテストをオンデマンドで実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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、WS-65xx モジュール、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 テストは、次のテストで構成されます。

「TestFabricSnakeForward」（P.A-27）
「TestFabricSnakeBackward」（P.A-27）
「TestSynchedFabChannel」（P.A-28）
「TestFabricCh0Health」（P.A-28）
「TestFabricCh1Health」（P.A-29）

TestFabricSnakeForward

TestFabricSnakeForward テストは、内部スネーク テストと外部スネーク テストの 2 つのテストで構成されます。内部スネーク テストは、ファブリック ASIC 内でテスト パケットを生成します。テスト データ パスは限られていて、パケットはファブリック ASIC 内に留まります。外部スネーク テストはスーパーバイザ エンジンのインバンド ポートを使用してテスト パケットを生成します。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 に同期化されているかどうかによって、使用されるテストが決まります。同期化されている場合は、外部スネーク テストが使用されます。同期化されていない場合は、内部スネーク テストが使用されます。両方のテストで、どのモジュールにも同期化されていないチャネルだけがテストに関与します。フォワード方向は、スネークが小さい番号のチャネルから大きい番号のチャネルに向かうことを示します。

表 A-46　TestFabricSnakeForward テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	オンデマンドで実行します。このテストによって、CPU 使用率が高くなる可能性があります。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
修正措置	スーパーバイザ エンジンが強制終了し、ROMMON に入ります。SFM がリセットします。
ハードウェア サポート	Supervisor Engine 720 および SFM。

TestFabricSnakeBackward

TestFabricSnakeBackward テストは、内部スネーク テストと外部スネーク テストの 2 つのテストで構成されます。内部スネーク テストは、ファブリック ASIC 内でテスト パケットを生成します。テスト データ パスは限られていて、パケットはファブリック ASIC 内に留まります。外部スネーク テストはスーパーバイザ エンジンのインバンド ポートを使用してテスト パケットを生成します。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 に同期化されているかどうかによって、使用されるテストが決まります。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、どのモジュールにも同期化されていないチャネルだけがテストに関与します。フォワード方向は、スネークが大きい番号のチャネルから小さい番号のチャネルに向かうことを示します。

表 A-47　TestFabricSnakeBackward テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	オンデマンドで実行します。このテストによって、CPU 使用率が高くなる可能性があります。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。

表 A-47　TestFabricSnakeBackward テストの属性 （続き）

リリース	12.2(33)SRA 以降
修正措置	スーパーバイザ エンジンが強制終了し、ROMMON に入ります。SFM がリセットします。
ハードウェア サポート	Supervisor Engine 720 および SFM。

TestSynchedFabChannel

TestSynchedFabChannel テストは、モジュールおよびファブリック両方のファブリック同期化ステータスを定期的にチェックします。ファブリック対応モジュールだけで使用できます。このテストはパケット スイッチング テストではないので、データ パスを伴いません。テストでは、モジュールとファブリックに SCP 制御メッセージが送信されて、同期化ステータスの照会が行われます。

表 A-48　TestSynchedFabChannel テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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てください。
デフォルト	オン。
リリース	12.2(33)SRA 以降
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 連続のリセット サイクルによって、モジュールの電源が切断されます。失敗の種類に応じて、ファブリックのスイッチオーバーが起動される場合があります。
ハードウェア サポート	すべてのファブリック対応モジュール。

TestFabricCh0Health

TestFabricCh0Health テストは、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 パスのヘルスを絶えずモニタします。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修正不能であると診断され、モジュールがリセットされます。3 回連続したリセット サイクルによって、ファブリックのスイッチオーバーが実行される場合があります。

表 A-49　TestFabricSCh0Health テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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てください。
デフォルト	オン。
リリース	12.2(33)SRA 以降

表 A-49　TestFabricSCh0Health テストの属性 （続き）

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 パスのヘルスを絶えずモニタします。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修正不能であると診断され、モジュールがリセットされます。3 回連続したリセット サイクルによって、ファブリックの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
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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てください。
デフォルト	オン。
リリース	12.2(33)SRA 以降
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 モジュール。

完全メモリ テスト

完全メモリ テストは、次のテストで構成されます。

「TestFibTcamSSRAM」（P.A-30）

「TestAsicMemory」（P.A-30）

「TestAclQosTcam」（P.A-30）

「TestNetflowTcam」（P.A-31）

「TestQoSTcam」（P.A-31）

（注）　メモリ テストを実行したあとにスーパーバイザ エンジンを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 エンジンでメモリ テストを実行してください。オンデマンド オンライン診断テストの実行に関する詳細については、「オンデマンド オンライン診断の設定」（P.39-3）を参照してください。

TestFibTcamSSRAM

TestFibTcamSSRAM テストは、FIB TCAM およびレイヤ 3 隣接の SSRAM メモリをチェックします。

表 A-51　TestFibTcamSSRAM テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。数時間、中断します。
推奨事項	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っている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。このテストの実行後に、スーパーバイザ エンジンを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(33)SRA 以降
修正措置	該当なし。
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 テストは、アルゴリズムを使用して、モジュール上のメモリをテストします。

表 A-52　TestAsicMemory テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。約 1 時間、中断します。
推奨事項	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っている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。このテストの実行後に、スーパーバイザ エンジンを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(33)SRA 以降
修正措置	該当なし。
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 テストは、PFC3B、PFC3BXL、PFC3C および PFC3CXL 上の ACL および QOS TCAM 両方の全ビットをテストし、位置をチェックします。PFC3A ではサポートされていません。

表 A-53　TestAclQosTcam テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。約 1 時間、中断します。
推奨事項	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っている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。このテストの実行後に、スーパーバイザ エンジンを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(33)SRA 以降
修正措置	該当なし。
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 テストは、Netflow TCAM の全ビットをテストし、位置をチェックします。

表 A-54　TestNetflowTcam テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。数分間、中断します。テストの対象のタイプに応じて、中断する時間が異なります。
推奨事項	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っている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。このテストの実行後に、スーパーバイザ エンジンを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(33)SRA 以降
修正措置	該当なし。
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 テストは、QoS TCAM デバイスに対して完全メモリ テストを実行します。

表 A-55　TestQoSTcam テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。数分間、中断します。テストの対象のタイプに応じて、中断する時間が異なります。

表 A-55　TestQoSTcam テストの属性 （続き）

推奨事項	このテストを使用するのは、ハードウェアに問題があると考えられる場合、またはハードウェアをライブ ネットワークに設置する前だけにしてください。テストを行っている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。このテストの実行後に、スーパーバイザ エンジンを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(33)SRA 以降
修正措置	該当なし。
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 テストは、次のテストで構成されます。

「TestIPSecClearPkt」（P.A-32）
「TestHapiEchoPkt」（P.A-33）
「TestIPSecEncryptDecryptPkt」（P.A-33）

TestIPSecClearPkt

TestIPSecClearPkt テストは、スーパーバイザ エンジンのインバンド ポートから暗号エンジンまで、スイッチ ファブリックまたはバスを介してパケットを送信します。パケットは暗号エンジンからスーパーバイザ エンジンのインバンド ポートに暗号化されずに送り返されます。パケットでは、暗号化が行われず、パケット データ フィールドが未使用であることがチェックされます。レイヤ 2 検索によって、パケットがスーパーバイザのインバンド ポートおよび暗号エンジン間に送信されます。

表 A-56　TestIPSecClearPkt テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	このテストをオンデマンドで実行します。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、コントロール パスを使用して Hapi Echo パケットを暗号エンジンに送信します。Hapi Echo パケットが暗号エンジンに送信されたあと、暗号エンジンからエコーが返されます。パケットは、インデックス転送を使用してスーパーバイザ エンジンのインバンド 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 に送り返されます。

表 A-57　TestHapiEchoPkt テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。
推奨事項	このテストをオンデマンドで実行します。このテストは、オンデマンド CLI から実行できません。
デフォルト	オン。
リリース	12.2(33)SRA 以降
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、IPSec サービス モジュール（WS-SVC-IPSEC、SPA-IPSEC）のスーパーバイザ エンジンのインバンド ポートと暗号エンジン間でパケットを交換することで、暗号機能をチェックします。複数の交換が行われたら、パケットがチェックされ、暗号エンジンが暗号/復号化プロセスを行ったあとに元のデータが失われていないかどうかが確認されます。レイヤ 2 検索によって、パケットがスーパーバイザのインバンド ポートおよび暗号エンジン間に送信されます。

表 A-58　TestIPSecEncryptDecryptPkt テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。デフォルトによって、テストが 1 分ごとに実行されます。
推奨事項	このテストは起動時にだけ実行できます。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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 テストは、次のテストで構成されます。

「TestTrafficStress」（P.A-34）

「TestEobcStressPing」（P.A-34）

TestTrafficStress

TestTrafficStress テストは、モジュール上のすべてのポートを各ペアに設定して、スイッチと搭載されているモジュールでストレス テストを実行します。設定後、ペア間で相互にパケットが送信されます。パケットがスイッチを所定の期間通過できるように設定されると、テストによってパケットが廃棄されていないことが確認されます。

表 A-59　TestTrafficStress テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。数分間、中断します。
推奨事項	このテストは、ネットワークに設置する前にハードウェア品質を調べるために使用します。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
修正措置	該当なし。
ハードウェア サポート	Supervisor Engine 720 および Supervisor Engine 32。

TestEobcStressPing

TestEobcStressPing テストは、スーパーバイザ エンジンを使用したモジュールの EOBC リンクに対してストレス テストを実行します。このテストは、スーパーバイザ エンジンがいくつかの sweep-ping プロセス（デフォルトでは 1 つ）を開始したときに起動します。sweep-ping プロセスは、20,000 SCP-ping パケットでモジュールの ping を処理します。各 packet-ping がタイムアウトする前にすべての 20,000 パケットが応答する場合（2 秒）、テストが正常に完了しています。テストが失敗する場合は、テスト時の EOBC バス上のトラフィック バーストを考慮して、5 回まで再試行できます。

表 A-60　TestEobcStressPing テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。数分間、中断します。
推奨事項	このテストは、ネットワークに設置する前にハードウェア品質を調べるために使用します。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
修正措置	該当なし。
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 テストは、次のテストで構成されます。

- 「TestL3HealthMonitoring」（P.A-35）
- 「TestTxPathMonitoring」（P.A-35）
- 「TestSynchedFabChannel」（P.A-36）

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。これらのテストについては、「ファブリック テスト」（P.A-26）を参照してください。

TestL3HealthMonitoring

TestL3HealthMonitoring テストは、ハードウェア障害を検出した際にシステムが自己再生を試みるときに必ず、ローカル DFC でスイッチングされる IPv4 および IPv6 パケットに対する診断テストなどの一連の診断テストを起動します。この際、テストの目的で前面パネルのポート（通常、ポート 1）がシャットダウンされます。診断テストが失敗する場合は、ハードウェア障害を修正できないため、自己再生シーケンスがもう一度行われます。

表 A-61　TestL3HealthMonitoring テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。中断する時間は、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（スパニングツリー プロトコルなど）によって異なります。テストの実行中にフォワーディング機能とポート機能が中断します。
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(33)SRA 以降
修正措置	該当なし。
ハードウェア サポート	DFC が装備されたモジュール。

TestTxPathMonitoring

TestTxPathMonitoring テストは、定期的に Supervisor Engine 720 と WS-X67xx シリーズ モジュールの各ポートにインデックス誘導型パケットを送信して、ASIC 同期化を確認し、関連する問題を修正します。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
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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(33)SRA 以降
修正措置	適用不可（自己再生）
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 テストは、モジュールおよびファブリック両方のファブリック同期化ステータスを定期的にチェックします。ファブリック対応モジュールだけで使用できます。このテストはパケット スイッチング テストではないので、データ パスを伴いません。テストでは、モジュールとファブリックに SCP 制御メッセージが送信されて、同期化ステータスの照会が行われます。

表 A-63　TestSynchedFabChannel テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
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てください。
デフォルト	オン。
リリース	12.2(33)SRA 以降
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	すべてのファブリック対応モジュール

一般的なテスト

一般的なテストは、次のテストで構成されます。

「ScheduleSwitchover」（P.A-36）
「TestFirmwareDiagStatus」（P.A-37）

ScheduleSwitchover

ScheduleSwitchover テストは、オンライン診断スケジューリング機能を使用して、いつでもユーザがスイッチオーバーを起動できるようになっています。

表 A-64　ScheduleSwitchover テストの属性

属性	説明
ディスラプティブ/ノンディスラプティブ	ディスラプティブ。
推奨事項	ダウンタイムにこのテストをスケジューリングし、スイッチオーバー後のスタンバイ スーパーバイザ エンジンへの継承機能をテストします。
デフォルト	オフ。
リリース	12.2(33)SRA 以降
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 テストは、モジュールの起動時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
ディスラプティブ/ノンディスラプティブ	ノンディスラプティブ。
推奨事項	このテストは起動時にだけ実行できます。
デフォルト	デフォルトによって、このテストは起動時またはリセット/OIR を行ったあとに実行されます。
リリース	12.2(33)SRA 以降
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

APPENDIX B

略語

表 B-1 に、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 アダプテーション層）
ACE	Access Control Entry（アクセス コントロール エントリ）
ACL	Access Control List（アクセス コントロール 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	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（属性値）
BDD	Binary Decision Diagrams
BECN	Backward Explicit Congestion Notification（逆方向明示的輻輳通知）
BGP	Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）
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

表 B-1　略語リスト （続き）

略語	説明
CEF	シスコ エクスプレス フォワーディング
CHAP	Challenge Handshake Authentication Protocol（チャレンジ ハンドシェイク認証プロトコル）
CIR	Committed Information Rate（認定情報レート）
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（コネクションレス型ネットワーク サービス）
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	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code（データ カントリ コード）
dCEF	Distributed Cisco Express Forwarding（分散 CEF）
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（分散型フォワーディング カード）
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（サービス拒否）
dot1q	802.1Q
DRAM	Dynamic RAM（ダイナミック RAM）
DRiP	Dual Ring Protocol（重複リング プロトコル）
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point（DiffServ コード ポイント）

表 B-1　略語リスト （続き）

略語	説明
DSPU	Downstream SNA Physical Units（ダウンストリーム SNA 物理ユニット）
DTP	Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）
DTR	Data Terminal Ready（データ ターミナル レディ）
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（電気的に消去可能でプログラミング可能な 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（イーサネット アウトオブバンド チャネル）
EOF	End Of File
ESI	End-System Identifier
FAT	File Allocation Table
FECN	Forward Explicit Congestion Notification（順方向明示的輻輳通知）
FM	Feature Manager
FRU	Field Replaceable Unit（現地交換可能ユニット）
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（インターネット制御メッセージ プロトコル）
IDB	Interface Descriptor Block
IDP	Initial Domain Part または Internet Datagram Protocol（インターネット データグラム プロトコル）
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（統合ローカル管理インターフェイス）

表 B-1　略語リスト （続き）

略語	説明
IP	Internet Protocol（インターネット プロトコル）
IPC	Inter-Processor Communication（プロセッサ間通信）
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System
ISL	Inter-Switch Link（スイッチ間リンク）
ISO	International Organization for 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（LAN エミュレーション 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 コントロール）
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（メンテナンス オペレーション プロトコル）
MOTD	Message-Of-The-Day
MLSE	Maintenance Loop 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）

表 B-1　略語リスト （続き）

略語	説明
MST	Multiple Spanning-Tree（マルチ スパニングツリー）
MTU	Maximum Transmission Unit（最大伝送単位）
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）
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（ネットワーク タイム プロトコル）
NVRAM	Nonvolatile RAM（不揮発性 RAM）
OAM	Operation, Administration, and Maintenance（運用管理および保守）
ODM	Order Dependent Merge
OSI	Open System Interconnection（オープン システム インターコネクション）
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	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（物理副層）
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

表 B-1　略語リスト （続き）

略語	説明
PVST+	Per-VLAN Spanning-Tree+
QDM	QoS Device Manager
QM	QoS Manager
QoS	Quality of Service（QoS）
RACL	Router Interface Access Control List
RADIUS	Remote Authentication Dial-In User Service
RAM	Random-Access Memory（ランダムアクセス メモリ）
RCP	Remote Copy Protocol（リモート コピー プロトコル）
RGMP	Router-Ports Group Management Protocol
RIB	Routing Information Base（ルーティング情報ベース）
RIF	Routing Information Field（ルーティング情報フィールド）
RMON	Remote Network Monitor（リモート ネットワーク モニタ）
ROM	Read-Only Memory
ROMMON	ROM Monitor（ROM モニタ）
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（リバース パス転送）
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy Plus
RSPAN	Remote SPAN（リモート SPAN）
RST	Reset（リセット）
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（同期データ リンク制御）
SGBP	Stack Group Bidding Protocol
SIMM	Single In-line Memory Module（シングル インライン メモリ モジュール）
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

表 B-1　略語リスト （続き）

略語	説明
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（サブネットワーク アクセス プロトコル）
SNMP	簡易ネットワーク管理プロトコル
SRM	Single Router Mode
SSO	Stateful Switchover
SPAN	スイッチド ポート アナライザ
SREC	S-Record format, Motorola defined format for ROM contents（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
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（伝送制御プロトコル/インターネット プロトコル）
Trivial File Transfer Protocol（TFTP）	Trivial File Transfer Protocol
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（ユーザ データグラム プロトコル）
UNI	User-Network Interface（ユーザ ネットワーク インターフェイス）
UTC	Coordinated Universal Time（協定世界時）
VACL	VLAN Access Control List（VLAN アクセス コントロール 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）

表 B-1　略語リスト （続き）

略語	説明
VINES	Virtual Network System
VLAN	Virtual LAN（仮想 LAN）
VMPS	VLAN メンバーシップ 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 ルーティングおよび転送）
VTP	VLAN トランキング プロトコル
VVID	Voice VLAN ID（音声 VLAN ID）
WAN	Wide Area Network（ワイドエリア ネットワーク）
WCCP	Web Cache Communication Protocol
WFQ	Weighted Fair Queueing（均等化キューイング）
WRED	Weighted Random Early Detection（重み付けランダム早期検出）
WRR	Weighted Round-Robin（重み付きラウンドロビン）
XNS	Xerox Network System

APPENDIX C

Cisco IOS Release 15.S ソフトウェア イメージ

表 C-1 に、Cisco IOS Release 15.S に付属のソフトウェア イメージを一覧表示します。これらのイメージは、Cisco 7600 ルータだけで使用できます。別のプラットフォーム（Catalyst 6500 シリーズ スイッチなど）上でこれらのいずれかのイメージを実行しようとすると、次の項で示すエラー メッセージの 1 つが表示されます。

（注） Cisco 7600 ルータと Catalyst 6500 スイッチの両方をサポートするには、特別なイメージ（rsp72043-adventerprisek9-mz、s3223-adventerprisek9-mz、および s72033-adventerprisek9-mz）が使用できます。これらのいずれかのイメージの入手方法または代替イメージが使用できるかについては、代理店にお問い合わせください。

表 C-1　Cisco 7600 Release 15.S ソフトウェア イメージ

イメージ ファイル名	説明
c7600rsp72043-adventerprisek9-mz（RSP720） c7600s72033-adventerprisek9-mz（Sup720） c7600s3223-adventerprisek9-mz（Sup32）	高度な企業サービス ソフトウェア イメージ
c7600rsp72043-advipservicesk9-mz（RSP720） c7600s72033-advipservicesk9-mz（Sup720） c7600s3223-advipservicesk9-mz（Sup32）	高度な IP サービス ソフトウェア イメージ
c7600rsp72043-ipservices-mz（RSP720） c7600s72033-ipservices-mz（Sup720） c7600s3223-ipservices-mz（Sup32）	IP サービス ソフトウェア イメージ
c7600rsp72043-ipservicesk9-mz（RSP720） c7600s72033-ipservicesk9-mz（Sup720） c7600s3223-ipservicesk9-mz（Sup32）	IP サービス SSH ソフトウェア イメージ
c7600rsp720_rp-rm2.srec（RSP720）	ルート プロセッサ用 ROMmon ソフトウェア イメージ（15.S で RSP720 だけに使用可能）
c7600rsp720_sp-rm2.srec（RSP720）	スイッチ プロセッサ用 ROMmon ソフトウェア イメージ（15.S で RSP720 だけに使用可能）

各イメージの機能については、次の Feature Navigator ツールを参照してください。
http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

非準拠プラットフォームのソフトウェア イメージ メッセージ

Cisco IOS Release 15.S イメージは、Cisco 7600 ルータだけで使用できます。Cisco 7600 ルータ以前、イメージは Catalyst 6500 シリーズ スイッチでも実行されていました。しかし、現在では、別のプラットフォーム上で Cisco 7600 イメージを実行しようとすると、次のいずれかのエラー メッセージが表示されます。

- 15.S ソフトウェア イメージを Cisco 7600 ルータ以外のプラットフォーム上で実行しようとすると、次のメッセージが表示されます。

```
%C6K_PLATFORM-1- DETECTED_NON_C7600_CHASSIS: Software has detected an attempt to run a
c7600 image on an incompatible chassis ([char])
Explanation: You are loading a special 7600 12.2SR image on a Catalyst 6500 Series
Switch .
Recommended Action: You are loading a special Cisco 7600 Series Router image on a
Catalyst 6500 Series Switch. Thank you for registering your chassis for approval to
use this image.  If you have not registered this chassis, please contact your Cisco
account representative in order to gain approval for use of this image.
```

- Cisco 7600 イメージを別のプラットフォーム（Catalyst 6500 スイッチなど）上で実行しようとすると、次のメッセージが表示されます。

```
%C6K_PLATFORM-1-DISABLE_NON_C7600_CHASSIS: Software has detected an attempt to run a
c7600 image on an incompatible chassis ([char]). This image may not boot.

Explanation: Software detected an attempt to load a Cisco 7600 series router image on
an incompatible chassis.
Recommended Action: Verify that you are using a Cisco 7600 series chassis; if you are
attempting to run this on a Catalyst 6500 series switch please contact your account
representative about selecting an appropriate image for your platform.
```

INDEX

数字

4K VLAN（4,096 個の VLAN サポート） 14-2
802.10 SAID（デフォルト） 14-6
802.1Q
　ISL VLAN へのマッピング 14-14, 14-17
　カプセル化 10-3
　トランク 10-3
　　制約事項 10-5
　トンネリング 17-1
　　設定時の注意事項 17-4
　　トンネル ポートの設定 17-6
　レイヤ 2 プロトコル トンネリング
　　「レイヤ 2 プロトコル トンネリング」を参照
802.1Q Ethertype、カスタム設定 10-15
802.1Q VLAN から ISL VLAN へのマッピング 14-14, 14-17
802.1X
　「ポートベースの認証」を参照
802.1x の許可ポート 49-4
802.1x の無許可ポート 49-4
802.3ad
　「LACP」を参照
802.3X フロー制御 8-12

A

AAA 35-1, 36-1, 40-1
access-enable host timeout（サポートなし） 36-2
ACE および ACL 35-1, 36-1, 40-1
aggregate ポリシング
　「QoS ポリシング」を参照
any transport over MPLS（AToM） 26-19
　Ethernet over MPLS 26-25
　旧リリースの AToM との互換性 26-21
ARP スプーフィング 42-1
AToM 26-19
auto-sync コマンド 7-7

B

BackboneFast
　「STP BackboneFast」を参照
Bandwidth-Remaining Ratio（BRR）、IP 加入者 24-5, 24-21, 24-22, 24-24
boot bootldr コマンド 2-20
boot config コマンド 2-20
boot system flash コマンド 2-16
boot system コマンド 2-15, 2-20
boot コマンド 2-16
BPDU、RSTP 形式 20-16
BPDU ガード
　「STP BPDU ガード」を参照

C

Call Home
　アラート グループ 60-6
　説明 60-1
　デフォルト設定 60-18
　メッセージ
　　形式オプション 60-2
　メッセージ形式オプション 60-2
call home 60-1
　mail-server プライオリティ 60-10
　smart call home の機能 60-2

SMTP サーバ 60-9
宛先プロファイル 60-4
重大度しきい値 60-8
情報の表示 60-14
通信のテスト 60-11
定期的な通知 60-8
電子メール オプションの設定 60-9
パターン マッチング 60-9
レート制限メッセージ 60-9
連絡先情報 60-3
call home 宛先プロファイル
設定 60-5
説明 60-4
属性 60-5
表示 60-16
call home アラート グループ
設定 60-6
説明 60-6
登録 60-7
call home 通知
syslog の XML 形式 60-29
syslog のフルテキスト形式 60-28
call home の連絡先
情報の割り当て 60-3
CEF
設定
MSFC2 29-5
スーパーバイザ エンジン 29-5
パケットの書き換え 29-2
例 29-3
レイヤ 3 スイッチング 29-2
Certificate Authority（CA） 60-3
CGMP 33-8
channel-group グループ
コマンド 12-9, 12-13
コマンド例 12-10
Cisco Cache Engine 56-2
Cisco Group Management Protocol
「CGMP」を参照
Cisco IOS Release 12.2SRB ソフトウェア イメージ C-1
Cisco IOS ユニキャスト リバース パス転送 35-2
CiscoView 1-2
CIST リージョナル ルート
「MSTP」を参照
CIST ルート
「MSTP」を参照
class-map コマンド 45-57
Class of Service（CoS） 45-112
class コマンド 45-66
Concurrent Routing and Bridging（CRB） 22-1
CONFIG_FILE 環境変数
コンフィギュレーション ファイル、表示 2-20
説明 2-19
config-register コマンド 2-17
config terminal コマンド 2-3
configure terminal コマンド 2-17, 8-2
configure コマンド 2-3
Control plane Policing and Protection（CoPP）
加入者単位 24-4
CoPP
概要 40-31
制御プレーン コンフィギュレーション モード、開始 40-33
制御プレーン コンフィギュレーション モードの開始 40-33
制御プレーンへの QoS サービス ポリシーの適用 40-33
設定
MLS QoS のイネーブル化 40-33
サービスポリシー マップ 40-33
トラフィックと照合する ACL 40-33
パケット分類基準 40-33
統計のモニタリング 40-35
トラフィック分類
ACL 例 40-42
概要 40-40
サンプル クラス 40-40
注意事項 40-41
定義 40-40

パケット分類の注意事項 40-34
表示
ダイナミックな情報 40-35
適合バイト数およびパケット数 40-35
レート情報 40-35
CoPP。「control plane policing and protection（CoPP）」を参照
copy running-config startup-config コマンド 2-5
copy system
running-config nvram
startup-config コマンド 2-20
CoS、上書きのプライオリティ 16-7, 16-8

D

dCEF 29-4, 29-5
debug fm private-hosts コマンド 38-31
debug private-hosts コマンド 38-32
debug コマンド
IP MMLS 31-26
DEC スパニングツリー プロトコル 22-2
Deficit Weighted Round Robin 45-99
description コマンド 8-14
destination-ip フローマスク 52-3
destination-source-ip フローマスク 52-3
DHCP Option 82
回線 ID サブオプション 41-5
概要 41-4
パケット形式、サブオプション
回線 ID 41-5
リモート ID 41-5
リモート ID サブオプション 41-5
DHCP スヌーピング
Option 82 データ挿入 41-4
イネーブル化 41-10, 41-11, 41-12, 41-14
概要 41-1
スヌーピング データベース エージェント 41-6
設定 41-9
設定時の注意事項 41-7
データベース エージェントのイネーブル化 41-15
デフォルト設定 41-7
バインディング データベース
「DHCP スヌーピング バインディング データベース」を参照
バインディング テーブルの表示 41-19
メッセージ交換プロセス 41-4
DHCP スヌーピング増加バインディング制限 41-8, 41-16
DHCP スヌーピング データベース エージェント
TFTP ファイルからの読み取り（例） 41-17
イネーブル化（例） 41-16
概要 41-6
データベースへの追加（例） 41-19
DHCP スヌーピング バインディング データベース
エントリ 41-3
説明 41-3
DHCP スヌーピング バインディング テーブル
「DHCP スヌーピング バインディング データベース」を参照
DHCP バインディング データベース
「DHCP スヌーピング バインディング データベース」を参照
DHCP バインディング テーブル
「DHCP スヌーピング バインディング データベース」を参照
DiffServ
ショート パイプ モード 48-32
ショート パイプ モードの設定 48-35
ユニフォーム モード 48-33
ユニフォーム モードの設定 48-40
Diffserv コード ポイント（DSCP） 45-113
DiffServ トンネリング モード 48-4
DoS 保護
「DoS 保護」を参照
PFC 設定時の注意事項および制約事項 40-24
Supervisor Engine 720 レイヤ 3 セキュリティ機能 レート リミッタ 40-19
スーパーバイザ エンジン 720 40-11
FIB 収集レート リミッタ 40-19

FIB 受信レート リミッタ 40-19
ICMP リダイレクト レート リミッタ 40-20
IGMP 到達不能レート リミッタ 40-18
IPv4 マルチキャスト レート リミッタ 40-21
IPv6 マルチキャスト レート リミッタ 40-22
IP エラー レート リミッタ 40-21
MTU 障害レート リミッタ 40-20
QoS ACL 40-13
SYN 攻撃を受けているネットワーク 40-14
TCP 代行受信 40-14
TTL 障害レート リミッタ 40-18
uRPF 障害レート リミッタ 40-18
uRPF チェック 40-13
VACL ログ レート リミッタ 40-20
出力 ACL ブリッジド パケット レート リミッタ 40-17
セキュリティ ACL 40-12
デフォルト設定 40-24
トラフィック ストーム制御 40-14
入力 ACL ブリッジド パケット レート リミッタ 40-17
マルチキャスト FIB ミス レート リミッタ 40-21
マルチキャスト IGMP スヌーピング レート リミッタ 40-20
マルチキャスト直接接続レート リミッタ 40-22
レイヤ 2 PDU レート リミッタ 40-21
レイヤ 2 プロトコル トンネリング レート リミッタ 40-21
パケット廃棄統計のモニタリング
monitor session コマンドの使用 40-26
VACL 取り込みの使用 40-27
DSCP
「QoS DSCP」を参照
DSCP ベースのキューのマッピング 45-90
duplex コマンド 8-7, 8-8
DWRR 45-99
Dynamic Host Configuration Protocol スヌーピング
「DHCP スヌーピング」を参照

E

eFSU。「enhanced Fast Software Upgrade（eFSU）」を参照
enable コマンド 2-3, 2-17
encapsulation frame-relay ietf コマンド 53-34
enhanced Fast Software Upgrade（eFSU）
issu loadversion コマンド 6-13
SSO、RPR、および RPR+ モード 6-8
新しいソフトウェア バージョンの許可 6-18
エラー処理 6-4
概要 6-1
互換性マトリクス チェックのディセーブル化 6-11
サポートされてない OIR 6-8
実行 6-9
使用上の注意事項および制限事項 6-7
冗長モードの確認 6-12
スイッチオーバーの強制実行（issu runversion コマンド） 6-16
スタンバイ RP に対する新しいソフトウェアの認定（issu commitversion コマンド） 6-19
スタンバイ RP への新しいソフトウェアのロード 6-13
中断（issu abortversion コマンド） 6-21
停止時間 6-3
手順 6-9
動作 6-2
ラインカードの最大停止時間の表示 6-15
ラインカードのメモリの予約 6-3
ラインカードのメモリの予約、禁止 6-3
EoMPLS
VLAN モード 26-25
VLAN モードの設定 26-25
設定 26-25
注意事項および制約事項 26-20
ポート モード 26-25
ポート モード設定時の注意事項 26-29
erase startup-config コマンド
コンフィギュレーション ファイルの削除 2-6
ERSPAN 53-1

ES-20 ラインカード上の UDE
制約事項 24-7, 65-2
EtherChannel
channel-group グループ
コマンド 12-9, 12-13
コマンド例 12-10
interface port-channel
コマンド例 12-8
interface port-channel（コマンド） 12-8
lacp システム プライオリティ
コマンド例 12-11
Min-Links 12-12
PAgP、概要 12-3
port-channel load-balance
コマンド 12-11, 12-12
コマンド例 12-12
STP 12-6
switchport trunk encapsulation dot1q 12-6
概要 12-1
設定
レイヤ 2 12-9
設定（作業） 12-8
設定時の注意事項 12-6
ポートチャネル インターフェイス 12-5
モード 12-2
レイヤ 2、設定 12-9
ロード バランシング
概要 12-6
設定 12-12
EtherChannel ガード
「STP EtherChannel ガード」を参照
Ethernet over MPLS（EoMPLS） 26-19
Ethernet over MPLS（EoMPLS）設定
EoMPLS VLAN モード 26-26
EoMPLS ポート モード 26-29
EXP 変換 48-4
Extensible Authentication Protocol over LAN 49-1

F

FIB TCAM 26-3
Flex Link 11-1
設定 11-3
設定時の注意事項 11-2
説明 11-1
デフォルト設定 11-2
モニタリング 11-4

G

GTP-SLB IPv6 サポートの設定 23-4
GTP-SLB の IPv6 サポート 23-1

H

hello タイム、MSTP 20-46
hello タイム、STP 20-35
http
//www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html 4-5
//www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html 53-36, 53-39

I

ICMP 到達不能メッセージ 36-1
ID
シリアル ID 60-25
IEEE 802.10 SAID（デフォルト） 14-6
IEEE 802.1Q
「802.1Q」を参照
IEEE 802.1Q Ethertype
カスタム設定 10-15
IEEE 802.1w
「RSTP」を参照
IEEE 802.3ad
「LACP」を参照

IEEE 802.3X フロー制御 8-12
IEEE ブリッジング プロトコル 22-2
IGMP
join メッセージ 33-2
イネーブル化 33-10
インターネット グループ管理プロトコル 33-1
クエリー 33-3
クエリー時間、設定 33-12
スヌーピング
概要 33-2
高速脱退 33-5
マルチキャスト グループからの脱退 33-4
マルチキャスト グループへの加入 33-2
スヌーピング クエリア
イネーブル化 33-9
概要 33-2
設定時の注意事項 32-8, 33-8
脱退処理
イネーブル化 33-13
IGMPv3 31-10
IGMPv3、IGMP v3lite、および URD を使用した送信元固有マルチキャスト 31-10
IGMP v3lite 31-10
In Service Software Upgrade（ISSU） 6-1
Integrated Routing and Bridging（IRB） 22-1
interface access コマンド 24-34
interface-destination-source-ip フローマスク 52-3
interface port-channel
コマンド例 12-8
interface port-channel（コマンド） 12-8
interfaces range macro コマンド 8-4
interfaces range コマンド 8-3
interfaces コマンド 8-2
interface コマンド 2-3
IP CEF、トポロジ（図） 29-4
ip flow-export destination コマンド 52-25
ip flow-export source コマンド 52-25, 52-26, 52-27, 57-2, 57-3, 57-4
ip-full フローマスク 52-3
ip http server 1-1
ip-interface-full フローマスク 52-3
IP MLS
NDE
「NDE」を参照
エージング タイム 52-22
フローマスク
destination-ip 52-3
destination-source-ip 52-3
interface-destination-source-ip 52-3
ip-full 52-3
ip-interface-full 52-3
概要 52-3
最小限 52-21
IP MMLS
debug コマンド 31-26
イネーブル化
ルータ インターフェイス上 31-11
概要 31-2
キャッシュ、概要 31-2
サポートされない機能 31-9
設定時の注意事項 31-8
デフォルト設定 31-7
パケットの書き換え 31-3
表示ルータ
マルチキャスト ルーティング テーブル、表示 31-21
フロー
部分的および完全スイッチング 31-4
ルータ
PIM、イネーブル化 31-10
インターフェイス上でのイネーブル化 31-11
インターフェイス情報の表示 31-18
グローバルなイネーブル化 31-10
レイヤ 3 の MLS キャッシュ 31-2
ip multicast-routing コマンド
IP マルチキャストのイネーブル化 31-10
IP phone、設定 16-5
ip pim コマンド

IP PIM のイネーブル化 31-11
IP precedence 45-113
IP subscriber awareness
Control plane Policing and Protection（CoPP） 24-4
interface access コマンド 24-34
IP 加入者インターフェイス 24-3
IP 加入者セッション 24-3
QoS 24-5
Bandwidth-Remaining Ratio（BRR） 24-5, 24-21, 24-22, 24-24
デュアルプライオリティ キュー 24-5, 24-26
プライオリティ レート伝播 24-5, 24-26, 24-27
QoS に関する推奨事項 24-21
Radius アカウンティング 24-4
概要 24-1
加入者単位の機能 24-4
合法的傍受 24-4
サポートされない機能 24-28
セキュリティ ACL 24-4
設定 24-29, 24-30
設定時の注意事項 24-28
設定例 24-31
利点 24-2
IPv4 マルチキャスト VPN 27-1
IPv6 マルチキャスト PFC3 および DFC3 レイヤ 3 スイッチング 30-1
ip wccp version コマンド 56-8
IP アカウンティング、IP MMLS 31-9
IP アドレス
BOOTP プロトコルによる割り当て 2-6
デフォルトに設定 2-6
IP スタティック ルート 2-5
IP の番号付けなし 22-1
IP マルチキャスト
IGMP スヌーピング 33-10
MLDv2 スヌーピング 32-10
概要 33-1
IP マルチキャスト MLS
「IP MMLS」を参照
ISL カプセル化 10-3
ISL トランク 10-3
ISSU、「In Service Software Upgrade（ISSU）」を参照

J

join メッセージ、IGMP 33-2

L

LACP
システム ID 12-5
LACP over EVC ポート チャネル
検証 23-13
コンフィギュレーション コマンド、設定の手順 23-5, 23-8, 64-6, 64-8, 64-9, 64-11
例 23-12
LER 48-2, 48-6, 48-7
LLDP
設定
デフォルト設定 17-10
Logical Operator Unit
「LOU」を参照
LOU
最大数の決定 36-6
説明 36-6
LSR 48-2, 48-7

M

MAC アドレス
BOOTP コンフィギュレーション ファイルへの追加 2-6
MAC アドレスベースのブロッキング 35-1
MAC アドレス リダクション 20-2
MAC 移動（ポート セキュリティ） 50-2
main-cpu コマンド 7-7
min-links 12-12
MLDv2 32-1

イネーブル化 32-10
クエリー 32-5
スヌーピング
概要 32-1
高速脱退 32-7
マルチキャスト グループからの脱退 32-6
マルチキャスト グループへの加入 32-4
スヌーピング クエリア
イネーブル化 32-9
概要 32-1
脱退処理
イネーブル化 32-13
MLDv2 スヌーピング 32-1
MLD スヌーピング
クエリー時間、設定 32-12
MLD レポート 32-4
MLS
MSFC しきい値 31-15
しきい値の設定 31-15
mls aging コマンド
IP MLS の設定 52-22
mls flow コマンド
IP MLS の設定 52-20, 52-21
mls ip multicast コマンド
IP MMLS のイネーブル化 31-12, 31-13, 31-14, 31-16, 31-17, 31-23, 31-24
mls nde flow コマンド
プロトコル フロー フィルタの設定 52-30
ポート フィルタの設定 52-29
ホストおよびポート フィルタの設定 52-29
ホスト フロー フィルタの設定 52-29
mls nde sender コマンド 52-23
MPLS 26-2
any transport over MPLS 26-19
IP から MPLS へのパス 26-3
MPLS から IP へのパス 26-4
MPLS から MPLS へのパス 26-4
QoS のデフォルト設定 48-15
VPN 48-12
VPN に関する注意事項および制約事項 26-16
基本的な設定 26-9
コア 26-4
実験フィールド 48-3
集約ラベル 26-2
出力 26-4
注意事項および制約事項 26-7
入力 26-3
非集約ラベル 26-2
ラベル 26-2
レイヤ 2 VPN ロードバランシング 26-9
MPLS DiffServ トンネリング モード 48-31
mpls l2 transport route コマンド 26-21
MPLS QoS
E-LSP 48-2
EXP 値マッピングの設定 48-30
EXP ビット 48-2
IP Precedence 48-2
QoS タグ 48-2
QoS のグローバルなイネーブル化 48-18
queueing-only モード 48-19
機能 48-3
クラス マップの設定 48-20
コマンド 48-16
サービス クラス 48-2
差別化サービス コード ポイント 48-2
出力 EXP 変換の設定 48-29
分類 48-2
ポリシー マップの設定 48-23
ポリシー マップの表示 48-28
MPLS QoS の設定
MPLS パケットを分類するためのクラス マップ 48-20
MPLS VPN、制限および制約事項 26-16
MQC 45-1
サポート対象
ポリシー マップ 45-3
サポート対象外
CAR 45-2

キューイング 45-2
MSTP
CIST、説明 20-20
CIST リージョナル ルート 20-21, 20-23
CIST ルート 20-22
CST
定義 20-20
リージョン間の動作 20-21
hello タイムの設定 20-46
IEEE 802.1D との相互運用性
移行プロセスの再起動 20-50
説明 20-26
IEEE 802.1s
実装 20-24
ポートの役割名の変更 20-24
用語 20-22
IST
定義 20-20
マスター 20-21
リージョン内の動作 20-21
MST リージョン
CIST 20-20
IST 20-20
サポートされるスパニングツリー インスタンス 20-20
設定 20-39
説明 20-19
ホップ カウント メカニズム 20-23
VLAN と MST インスタンスのマッピング 20-39
概要 20-18
拡張システム ID
異常動作 20-41
セカンダリ ルート スイッチへの影響 20-42
ルート スイッチへの影響 20-41
境界ポート
設定時の注意事項 20-39
説明 20-23
ステータスの表示 20-50
ステータス、表示 20-50
設定
MST リージョン 20-39
高速コンバージェンス用リンク タイプ 20-49
最大エージング タイム 20-48
最大ホップ カウント 20-48
スイッチ プライオリティ 20-45
セカンダリ ルート スイッチ 20-42
転送遅延時間 20-47
ネイバー タイプ 20-49
パス コスト 20-44
ポート プライオリティ 20-43
ルート スイッチ 20-41
設定時の注意事項 20-38
デフォルト設定 20-38
モードのイネーブル化 20-39
ルート スイッチ
異常動作 20-41
拡張システム ID の影響 20-41
設定 20-41
MTU サイズ（デフォルト） 14-6
Multicast Listener Discovery version 2
「MLDv2」を参照

N

NBAR 45-1
NDE
イネーブル化 52-17
概要 52-1
指定
宛先 TCP/UDP ポート フィルタ 52-29
宛先ホスト フィルタ 52-29
プロトコル フィルタ 52-30
設定の表示 52-30
設定、表示 52-30
フィルタ
宛先 TCP/UDP ポート、指定 52-29
宛先ホスト、指定 52-29
概要 52-8

送信元ホストおよび宛先 TCP/UDP ポート、指定 52-29
プロトコル、指定 52-30
マルチキャスト 52-15
NDE の設定、デフォルト 52-15
NDE のデフォルト設定 52-15
NDE バージョン 8 52-11
NetFlow Multiple Export Destinations 52-25
NetFlow データ エクスポート
「NDE」を参照
NetFlow バージョン 9 52-4
Network-Based Application Recognition 45-1
Nonstop Forwarding
「NSF」を参照
NSF 5-1
NSF with SSO は、IPv6 マルチキャスト トラフィックを未サポート 5-1
NVRAM
設定値の保存 2-5

O

OIR 8-15

P

PACL。「Private Hosts 機能」を参照
PAgP
概要 12-3
PBR 1-4, 22-4
PFC3BXL
MPLS でサポートされるコマンド 26-8
MPLS に関する注意事項および制約事項 26-7
MPLS ラベル スイッチング 26-1
VPN スイッチング 26-15
VPN でサポートされるコマンド 26-17
再循環 26-4
サポート対象 Cisco IOS 機能 26-5
ハードウェア機能 26-5
PFC の RSP720 との互換性 4-1
PIM、IP MMLS 31-10
PIM スヌーピング
VLAN におけるイネーブル化 34-5
概要 34-4
グローバルなイネーブル化 34-5
指定ルータのフラッディング 34-6
police コマンド 45-69
policy-map コマンド 45-58, 45-65
port-channel load-balance
コマンド 12-11, 12-12
コマンド例 12-11, 12-12
PortFast
「STP PortFast」を参照
PortFast BPDU フィルタリング
「STP PortFast BPDU フィルタリング」を参照
private-hosts mac-list コマンド 38-15
private-hosts mode コマンド 38-17
private-hosts promiscuous コマンド 38-19
private-hosts vlan-list コマンド 38-21
Private Hosts 機能
PACL がある場合のトラフィックの制限 38-3
VLAN のホストの独立 38-2
概要 38-1
プロトコル独立型 MAC ACL 38-1
ポート ACL（PACL） 38-5
ポート タイプ 38-3
private hosts 機能
debug fm private-hosts コマンド 38-31
debug private-hosts コマンド 38-32
private-hosts mac-list コマンド 38-15
private-hosts mode コマンド 38-17
private-hosts promiscuous コマンド 38-19
private-hosts vlan-list コマンド 38-21
private-hosts コマンド 38-14
show fm private-hosts コマンド 38-23
show private-hosts access-lists コマンド 38-26
show private-hosts configuration コマンド 38-28

show private-hosts interface configuration コマンド 38-29
show private-hosts mac-list コマンド 38-30
コマンド リファレンス 38-13
スプーフィングからの保護 38-9
設定（概要） 38-10
設定時の注意事項 38-5, 38-6
設定（詳細手順） 38-11
マルチキャストの動作 38-9
private-hosts コマンド 38-14
PVLAN
「プライベート VLAN」を参照
PVLAN ポートのポート セキュリティ 50-3
PVRST
「Rapid-PVST」を参照 20-18

Q

QoS
Class of Service（CoS）、定義 45-112
DSCP（定義） 45-113
IP precedence 45-113
Type of Service（ToS） 45-113
マーキング 45-113
QoS CoS
ポートの値、設定 45-83
レイヤ 3 スイッチング エンジンの最終的な ToS 値 45-11
QoS DSCP
定義 45-113
内部値 45-9
マップ、設定 45-78
QoS L3 スイッチング エンジン
機能の概要 45-16
分類、マーキング、ポリシング 45-9
QoS MSFC
マーキング 45-17
QoS OSM 出力ポート
機能の概要 45-13
QoS ToS
定義 45-113
レイヤ 3 スイッチング エンジンの最終的な CoS 値 45-11
QoS trust-cos
ポート キーワード 45-14, 45-16
QoS trust-dscp
ポート キーワード 45-14, 45-16
QoS trust-ipprec
ポート キーワード 45-14, 45-16
QoS untrusted ポート キーワード 45-14, 45-16
QoS VLAN ベースまたはポート ベース 45-10, 45-52
QoS アウト オブ プロファイル 45-20
QoS イーサネット出力ポート
スケジューリング 45-102
スケジューリング、輻輳回避、およびマーキング 45-11, 45-13
QoS イーサネット入力ポート
分類、マーキング、スケジューリング、輻輳回避 45-6
QoS、加入者単位 24-5
QoS 機能を使用した QoS トラフィック フロー 45-4
QoS キュー
送信、帯域幅の割り当て 45-99
QoS 受信キュー 45-8, 45-94, 45-97
ドロップしきい値 45-22
QoS スケジューリング（定義） 45-113
QoS 送信キュー 45-23, 45-92, 45-93, 45-95, 45-96
サイズ比 45-100, 45-101
QoS デフォルト設定 45-102, 46-2
QoS 統計データ エクスポート 46-1
宛先ホストの設定 46-8
時間間隔の設定 46-7, 46-9
設定 46-2
QoS 二重送信キュー
しきい値
設定 45-84, 45-88
QoS の機能拡張、SP720 4-5
QoS の最終的なレイヤ 3 スイッチング エンジン CoS 値および ToS 値 45-11

QoS の内部 DSCP 値 45-9
QoS の輻輳回避
QoS
輻輳回避 45-112
QoS のマッピング
CoS 値から DSCP 値 45-76, 45-78
DSCP 値から CoS 値 45-81
DSCP 変換 45-74, 48-29
DSCP マークダウン値 45-28, 45-80, 48-16
IP precedence 値から DSCP 値 45-79
QoS 分類（定義）
QoS
分類 45-112
QoS ポート
信頼状態 45-82
QoS ポート ベースまたは VLAN ベース 45-52
QoS ポリシング 45-113
定義 45-113
マイクロフロー、ルーティングされないトラフィックに対するイネーブル化 45-51
QoS ポリシング ルール
作成 45-56
集約 45-17
マイクロフロー 45-17
QoS マーキング
信頼できないポート 45-14
信頼できるポート 45-14
定義 45-113
QoS マークダウン 45-20
QoS マルチレイヤ スイッチ フィーチャ カード 45-17
QoS ラベル（定義） 45-113

R

Radius アカウンティング、加入者単位 24-4
Rapid-PVST
イネーブル化 20-37
概要 20-18
reload コマンド 2-17
Remote Source-Route Bridging（RSRB） 22-1
RIF キャッシュのモニタリング 8-15
rommon コマンド 2-18
ROM モニタ
起動プロセス 2-14
Route Processor Redundancy
「冗長構成（RPR+）」を参照
Route Switch Processor 720（RSP720）
GE バンドルでのロード バランシング 4-4
GRE トンネル上のパケット フラグメンテーション 4-4
IPv6 ACL の機能拡張 4-3
PFC の互換性 4-1
QoS の機能拡張 4-5
概要 4-1
拡張性 4-3
機能のサポート 4-2
サポートされない機能 4-6
シャーシのサポート 4-1
スイッチング モード 4-8
ハードウェア コンポーネント 4-2
ハイ アベイラビリティ 4-3
パフォーマンスの改善 4-2
フラッシュ メモリ 4-6
ポート 4-6
未知のユニキャスト パケットのレート制限 4-3
RPF
エラー 31-5
非 RPF マルチキャスト 31-5
マルチキャスト 31-2
ユニキャスト 35-2
RPR+
「冗長構成（RPR+）」を参照
RPR および RPR+ による IPv6 マルチキャスト トラフィックのサポート 7-1
RSTP
BPDU
形式 20-16
処理 20-17

IEEE 802.1D との相互運用性
移行プロセスの再起動 20-50
説明 20-26
トポロジの変更 20-18
「MSTP」も参照
アクティブ トポロジ 20-13
概要 20-13
高速コンバージェンス
エッジ ポートおよび Port Fast 20-14
説明 20-14
ポイントツーポイント リンク 20-14, 20-49
ルート ポート 20-14
指定スイッチ、定義 20-13
指定ポート、定義 20-13
提案合意ハンドシェイク プロセス 20-14
ポートの役割
説明 20-13
同期 20-15
ルート ポート、定義 20-13

S

SAID 14-6
service-policy input コマンド 45-53, 45-72, 45-75, 45-78, 48-30
service-policy コマンド 45-58
show boot コマンド 2-20
show catalyst6000 chassis-mac-address コマンド 20-3
show ciscoview package コマンド 1-3
show ciscoview version コマンド 1-3
show configuration コマンド 8-14
show eobc コマンド 8-15
show fm private-hosts コマンド 38-23
show hardware コマンド 8-2
show ibc コマンド 8-15
show interfaces コマンド 8-2, 8-11, 8-12, 8-14, 8-15, 10-7, 10-12
表示、インターフェイス タイプ番号 8-2
表示、速度およびデュプレックス モード 8-8
show ip flow export コマンド
NDE エクスポート フローの IP アドレスおよび UDP ポートの表示 52-27
show ip interface コマンド
IP MMLS インターフェイスの表示 31-19
show ip mroute コマンド
IP マルチキャスト ルーティング テーブルの表示 31-21
show ip pim interface コマンド
IP MMLS ルータ設定の表示 31-19
show mls aging コマンド 52-23
show mls entry コマンド 29-6
show mls ip multicast group コマンド
IP MMLS グループの表示 31-22, 31-25
show mls ip multicast interface コマンド
IP MMLS インターフェイスの表示 31-22, 31-25
show mls ip multicast source コマンド
IP MMLS の送信元の表示 31-22, 31-25
show mls ip multicast statistics コマンド
IP MMLS 統計情報の表示 31-22, 31-25
show mls ip multicast summary
IP MMLS 設定の表示 31-22, 31-25
show mls nde コマンド 52-30
NDE フロー IP アドレスの表示 52-27
show mls rp コマンド
IP MLS 設定の表示 52-21
show module コマンド 7-8
show private-hosts access-lists コマンド 38-26
show private-hosts configuration コマンド 38-28
show private-hosts interface configuration コマンド 38-29
show private-hosts mac-list コマンド 38-30
show protocols コマンド 8-15
show rif コマンド 8-15
show running-config コマンド 2-4, 8-14, 8-15
show startup-config コマンド 2-5
show version コマンド 2-3, 2-17, 2-18, 8-15
smart call home 60-1
Transport Gateway（TG）集約ポイント 60-2
宛先プロファイル（説明） 60-4

サービス契約の要件 60-3
説明 60-2
登録要件 60-2
SMARTnet
smart call home の登録 60-2
SNMP
サポートおよびマニュアル 1-1
source-only-ip フローマスク 52-3
SPAN
概要 53-1
設定 53-12
VLAN フィルタリング 53-30
ソース 53-16, 53-20, 53-26, 53-28
設定時の注意事項 53-6
spanning-tree backbonefast
コマンド 21-13, 21-14
コマンド例 21-14
spanning-tree cost
コマンド 20-33
コマンド例 20-33, 20-34
spanning-tree portfast
コマンド 21-9
コマンド例 21-9
spanning-tree portfast bpdu-guard
コマンド 21-12
spanning-tree port-priority
コマンド 20-31, 20-32
spanning-tree uplinkfast
コマンド 21-13
コマンド例 21-13
spanning-tree vlan
コマンド 20-28, 20-30, 20-31, 21-15
コマンド例 20-28, 20-30, 20-31
spanning-tree vlan cost
コマンド 20-33
spanning-tree vlan forward-time
コマンド 20-36
コマンド例 20-36
spanning-tree vlan hello-time
コマンド 20-35
コマンド例 20-35
spanning-tree vlan max-age
コマンド 20-36
コマンド例 20-37
spanning-tree vlan port-priority
コマンド 20-31
コマンド例 20-32
spanning-tree vlan priority
コマンド 20-34
コマンド例 20-35
SPAN 宛先ポートの許可リスト 53-15
speed コマンド 3-2, 8-6
STP
EtherChannel 12-6
概要 20-1
802.1Q トランク 20-12
BPDU 20-3
概要 20-2
ディセーブル ステート 20-11
トポロジ 20-5
フォワーディング ステート 20-10
ブロッキング ステート 20-7
プロトコル タイマー 20-4
ポート ステート 20-5
ラーニング ステート 20-9
リスニング ステート 20-8
ルート ブリッジ選択 20-4
設定 20-26
hello タイム 20-35
イネーブル化 20-27, 20-29
最大エージング タイム 20-36
セカンダリ ルート スイッチ 20-30
転送遅延時間 20-36
ブリッジ プライオリティ 20-34
ポート コスト 20-33
ポート プライオリティ 20-31
ルート ブリッジ 20-29
デフォルト 20-27

STP BackboneFast
spanning-tree backbonefast
コマンド 21-13, 21-14
コマンド例 21-14
概要 21-4
図
スイッチの追加 21-7
設定 21-13
STP BPDU ガード
spanning-tree portfast bpdu-guard
コマンド 21-12
概要 21-2
設定 21-12
STP EtherChannel ガード 21-6
STP PortFast
BPDU フィルタリング 21-2
設定 21-10
spanning-tree portfast
コマンド 21-9
コマンド例 21-9
概要 21-2
設定 21-8
STP UplinkFast
spanning-tree uplinkfast
コマンド 21-13
コマンド例 21-13
概要 21-3
設定 21-12
STP ブリッジ ID 20-2
STP ルート ガード 21-7, 21-15
STP ループ ガード
概要 21-7
設定 21-15
Supervisor Engine 2、サポート対象外
Supervisor Engine 32
サポートされるシャーシ 9-1
フラッシュ メモリ 9-1
ポート 9-2
switchport
設定 10-13
例 10-12
switchport access vlan 10-10, 10-14
例 10-14
switchport mode access 10-4, 10-14
例 10-14
switchport mode dynamic 10-9
switchport mode dynamic auto 10-4
switchport mode dynamic desirable 10-4
デフォルト 10-5
例 10-13
switchport mode trunk 10-4, 10-9
switchport nonegotiate 10-4
switchport trunk allowed vlan 10-11
switchport trunk encapsulation 10-8
switchport trunk encapsulation dot1q 10-4
例 10-13
switchport trunk encapsulation isl 10-4
switchport trunk encapsulation negotiate 10-4
デフォルト 10-5
switchport trunk native vlan 10-10
switchport trunk pruning vlan 10-11

T

TACACS+ 35-1, 36-1, 40-1
TCP 代行受信 35-2
TDR
ケーブル接続の確認 8-16
注意事項 8-16
テストの開始および中止 8-16
Time Domain Reflectometer（TDR）
「TDR」を参照
TopN レポート
「スイッチ TopN レポート」を参照
traceroute、レイヤ 2
1 ポートに複数のデバイス 59-2
ARP 59-2
CDP 59-1

IP アドレスおよびサブネット 59-2
MAC アドレスおよび VLAN 59-2
説明 59-1
マルチキャスト トラフィック 59-2
ユニキャスト トラフィック 59-1
traceroute、レイヤ 2
使用上の注意事項 59-1
trust-dscp
「QoS trust-dscp」を参照
trust-ipprec
「QoS trust-ipprec」を参照
Type of Service（ToS） 45-113

U

UDE 25-1
概要 25-2
設定 25-3
UDE および UDLR 25-1
UDLD
イネーブル化
グローバル 51-3
ポート 51-4
概要 51-1
デフォルト設定 51-3
UDLR 25-1
設定 25-6
トンネル
ARP および NHRP 25-3
（例） 25-7
バック チャネル 25-1
Unidirectional Link Routing（UDLR）
「UDLR」を参照
UplinkFast
「STP UplinkFast」を参照
URD 31-10

V

VACL 37-1
MAC アドレスベース 37-4
SVI 37-8
WAN インターフェイス 37-1
概要 37-1
設定 37-4
例 37-9
マルチキャスト パケット 37-3
レイヤ 3 VLAN インターフェイス 37-8
レイヤ 4 ポート演算 36-5
ロギング
制約事項 37-10
設定 37-10
設定例 37-11
VLAN
4,096 個の VLAN サポート 14-2
ID（デフォルト） 14-6
VLAN 1 の最小化 10-11
VTP ドメイン 14-2
インターフェイスの割り当て 14-13
概要 14-1
拡張範囲 14-2
設定 14-1
設定（作業） 14-10
設定時の注意事項 14-8
デフォルト 14-6, 14-8
トークン リング 14-3
トランク
概要 10-3
トランク上で許可される 10-11
名前（デフォルト） 14-6
標準範囲 14-2
プライベート
「プライベート VLAN」を参照
予約範囲 14-2
vlan
コマンド 14-11, 14-13, 52-19, 52-20, 53-20

コマンド例　14-12
vlan database
コマンド　14-11, 14-13, 52-19, 52-20, 53-20
vlan mapping dot1q
コマンド　14-16, 14-17
コマンド例　14-18
VLAN トランキング プロトコル
「VTP」を参照
VLAN ブリッジ スパニングツリー プロトコル　22-2
VLAN ベースの QoS フィルタリング　45-59
VLAN 変換
コマンド例　14-16, 14-17
VLAN モード　26-25
VPN
設定例　26-17
注意事項および制約事項　26-16
VTP
アドバタイズメント　13-3
概要　13-1, 66-1
クライアント、設定　13-11
サーバ、設定　13-11
設定時の注意事項　13-7
ディセーブル化　13-11
デフォルト設定　13-6
統計情報　13-14
ドメイン　13-2, 66-1
VLAN　14-2
トランスペアレント モード、設定　13-11
バージョン 2
イネーブル化　13-10
概要　13-3
プルーニング
概要　13-5
設定　10-11, 13-10
モード
クライアント　13-2
サーバ　13-2
トランスペアレント　13-2
モニタリング　13-14

W

WCCP
サービス グループ　56-9
プロトコル バージョンの指定　56-8
ルータでの設定　56-2, 56-15
Web Cache Communication Protocol
「WCCP」を参照
web キャッシュ
「キャッシュ エンジン」を参照
Web キャッシュ サービス
説明　56-6
Web キャッシング
「WCCP」も参照　56-6
「Web キャッシュ サービス」を参照
Web スケーリング　56-2
Web ブラウザ インターフェイス　1-1
WRR　45-99

X

xconnect コマンド　26-21

Y

Y.1731 パフォーマンス モニタリング　69-1

あ

アウト オブ プロファイル
「QoS アウト オブ プロファイル」を参照
アクセス インターフェイス（IP 加入者）　24-3
アクセス コントロール エントリおよびリスト　35-1, 36-1, 40-1
アクセスポート、設定　10-13
アクセス リスト、WCCP を使用　56-11
アップグレードに関する注意事項　26-21
アドバタイズメント、VTP　13-3
アドレス

IP、「IP アドレス」を参照
MAC、「MAC アドレス」を参照
アラーム
マイナー 55-12
メジャー 55-12

い

イーサネット、ポート デュプレックスの設定 8-13
イネーブル化
IP MMLS
ルータ インターフェイス上 31-11
インターネット グループ管理プロトコル
「IGMP」を参照
インターフェイス
設定 8-2
設定、概要 8-1
設定、速度 8-5
設定、デュプレックス モード 8-5
範囲 8-3
番号 8-1
命名する 8-14
レイヤ 2 モード 10-4
わかりやすい名前、追加 8-14
インターフェイス、アクセス（IP 加入者） 24-3

え

エージング タイム
IP MLS 52-22
加速 MSTP 20-47
最大
MSTP 20-48
最大 MSTP 20-48
エクストラネット MVPN アーキテクチャ 28-1

お

オペレーティング・システム イメージ
「システム イメージ」を参照
音声 VLAN
Cisco 7960 Phone、ポート接続 16-1
IP 電話への接続 16-5
音声トラフィック用のポート設定
802.1Q フレーム 16-5
概要 16-1
設定時の注意事項 16-4
データ トラフィック用の IP Phone の設定
着信フレームの CoS の上書き 16-7, 16-8
デフォルト設定 16-4
オンライン診断
概要 39-1
診断の健全性チェック 39-11
スケジュール スイッチオーバー 39-10
設定 39-2
テストの実行 39-6
テストの説明 A-1
メモリ テスト 39-10
オンライン診断テスト A-1

か

書き換え、パケット
CEF 29-2
IP MMLS 31-3
拡張 interface range コマンド 8-3
拡張システム ID、MSTP 20-41
拡張範囲 VLAN 14-2
「VLAN」を参照
加重ラウンドロビン 45-99
仮想 LAN
「VLAN」を参照
活性挿抜
「OIR」を参照
加入者。「IP subscriber awareness」を参照

カプセル化　10-3
環境変数
　CONFIG_FILE　2-19
　制御　2-20
　表示　2-20
環境モニタ機能
　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　55-12
環境モニタリング
　CLI コマンドの使用　55-10
　LED 表示　55-12
　SNMP トラップ　55-12
　Syslog メッセージ　55-12
関連資料　liv

き

キャッシュ エンジン　56-1
キャッシュ エンジン クラスタ　56-1
キャッシュ ファーム
　「キャッシュ エンジン クラスタ」を参照
キュー
　デュアルプライオリティ（IP 加入者）　24-5, 24-26

く

クエリー、IGMP　33-3
クエリー、MLDv2　32-5
組み込み CiscoView　1-2
クラス マップ コンフィギュレーション　45-62
グローバル パラメータ、設定　2-2

こ

高速コンバージェンス　20-14
高速スパニングツリー
　「RSTP」を参照
高速スパニングツリー プロトコル
　「RSTP」を参照
合法的傍受、加入者単位　24-4
高容量電源のサポート　55-4
コミュニティ VLAN　15-3
コミュニティ ポート　15-3
コンフィギュレーション
　ファイル、保存　2-5
コンフィギュレーション ファイルの保存　2-5
コンフィギュレーション レジスタのブート フィールド
　値の表示　2-18
　変更作業　2-16

さ

サーバ ID
　説明　60-26
サービス プロバイダー ネットワーク、MSTP および RSTP　20-19
再循環　26-4, 45-12
最大エージングタイム、MSTP　20-48
最大エージング タイム、STP　20-36
最大ホップ カウント、MSTP　20-48
再マーキングされた DSCP に対する出力 ACL のサポート　45-12, 45-53
サブドメイン、プライベート VLAN　15-2
差別化サービス コード ポイント
　「QoS DSCP」を参照
サンプリングされた NDE
　説明　52-9

し

シスコ エクスプレス フォワーディング　26-3
システム
　グローバル パラメータの設定　2-2
　コンフィギュレーション レジスタ
　　起動時の設定　2-16
　　設定　2-15 ～ 2-18
システム イメージ
　フラッシュからのロード　2-18

ロードの必要性およびロード方法の決定　2-16
システムのハードウェア容量　55-5
実行コンフィギュレーションの確認　2-4
指定ルータのフラッディングに対する PIM スヌーピングのディセーブル化　34-6
自動保護スイッチング グループ内の Bridged Routed Encapsulation　14-8
ジャンボ フレーム　8-9
集約ラベル　26-2, 26-4
受信キュー
「QoS 受信キュー」を参照
出力レプリケーション パフォーマンスの改善　31-14
冗長構成（NSF）　5-1
設定
BGP　5-13
CEF　5-13
EIGRP　5-18
IS-IS　5-16
OSPF　5-15
マルチキャスト NSF with SSO の設定　5-12
冗長構成（RPR+）　7-1
redundancy コマンド　7-7
route processor redundancy plus　7-3
スーパーバイザ エンジンの設定　7-6
スーパーバイザ エンジンの設定の表示　7-8
設定　7-6
冗長構成（SSO）
redundancy コマンド　5-11
冗長性（NSF）
スーパーバイザ エンジンの設定　5-10
ルーティング プロトコル　5-4
ショート パイプ モード、設定　48-35
シリアル ID
説明　60-25
信頼しない
「QoS trust-cos」を参照
「QoS untrusted」を参照
信頼できないポートの DHCP Option 82 機能の許可　41-11
概要　41-3
設定　41-11

す

スイッチ TopN レポート
概要　57-1
実行　57-2
表示　57-2
フォアグラウンドの実行　57-2
スイッチド ポート アナライザ
「SPAN」を参照
スイッチ ファブリック機能　3-2, 4-7
設定　3-4, 4-8
モニタリング　3-5, 4-9
スイッチ プライオリティ
MSTP　20-45
スイッチポート
show interfaces　8-11, 8-12, 10-7, 10-12
スーパーバイザ エンジン
ROM モニタ　2-14
環境モニタリング　55-10
冗長構成　5-1, 7-1
冗長設定の表示　7-8
スタートアップ コンフィギュレーション　2-14
スタティック ルート　2-5
設定　2-1
設定の同期化　5-19, 7-7
デフォルト設定　2-1
スーパーバイザ エンジン 32　9-1
スーパーバイザ エンジンの冗長構成
設定　5-10, 7-6
スケジューリング
「QoS」を参照
スタティック ルート、設定　2-5
スタンバイ リンク　11-1
スティッキ ARP　40-43
スティッキ セキュア MAC アドレス　50-8, 50-9
スティッキ セキュア MAC アドレスによるポート セキュリティ　50-2

スティッキ セキュア MAC アドレスのイネーブル化　50-8
ストーム制御
　「トラフィック ストーム制御」を参照
スヌーピング
　「IGMP スヌーピング」を参照
　「MLDv2 スヌーピング」を参照
スロット番号、説明　8-1

せ

制御プレーン ポリシング
　「CoPP」の参照
セカンダリ VLAN　15-3
セキュア MAC アドレスのエージング タイプ　50-10
セキュリティ
　設定　35-1, 36-1, 40-1
セキュリティ ACL、加入者単位　24-4
セキュリティ、ポート　50-1
設定　45-65
　グローバル パラメータ
　　設定例　2-2
　コンフィギュレーション モードの使用　2-3 ～ 2-4
　レジスタ
　　起動時の設定　2-16
　　設定　2-15 ～ 2-18
　　設定の変更　2-17
設定例　2-4
　EoMPLS VLAN モード　26-26
　EoMPLS ポート モード　26-26, 26-29
専用アクセス レート（CAR）、サポート対象外　45-2

そ

送信キュー
　「QoS 送信キュー」を参照
送信元 ID
　call home イベントの形式　60-25
速度
　インターフェイスの設定　8-6
ソフトウェア
　ルータのアップグレード　6-9
ソフトウェア イメージ、Release 12.2SRB　C-1
ソフトウェア コンフィギュレーション レジスタの機能　2-15 ～ 2-18

た

ダイナミック ARP インスペクション
　ARP ACL と DHCP スヌーピング エントリのプライオリティ　42-5
　ARP キャッシュ ポイズニング　42-2
　ARP スプーフィング攻撃　42-2
　ARP パケットのレート制限
　　errdisable ステート　42-4
　　設定　42-10
　　説明　42-4
　ARP 要求、説明　42-1
　DHCP スヌーピング バインディング データベース　42-3
　DoS 攻撃、回避　42-10
　man-in-the middle 攻撃、説明　42-2
　インターフェイス信頼状態　42-3
　機能　42-2
　クリア
　　統計情報　42-16
　　ログ バッファ　42-17
　設定
　　着信 ARP パケットのレート制限　42-4, 42-10
　　ログ システム メッセージ　42-14
　　ログ バッファ　42-14, 42-15
　設定時の注意事項　42-6
　説明　42-1
　妥当性チェック、実行　42-12
　デフォルト設定　42-5
　統計情報
　　クリア　42-16
　　表示　42-16
　ドロップされたパケットのロギング、説明　42-5

ネットワーク セキュリティ問題とインターフェイス信頼状態 42-3
表示
ARP ACL 42-16
信頼状態およびレート制限 42-16
設定および動作状態 42-16
統計情報 42-16
ログ バッファ 42-17
レート制限を超過した場合の errdisable ステート 42-4
ログ システム メッセージ
設定 42-14
ログ バッファ
クリア 42-17
設定 42-14, 42-15
表示 42-17
脱退処理、IGMP
イネーブル化 33-13
脱退処理、MLDv2
イネーブル化 32-13
単一方向イーサネット
「UDE」を参照
設定例 25-5
単一方向リンク検出プロトコル
「UDLD」を参照

て

手順
グローバル パラメータの設定 2-2
コンフィギュレーション モードの使用 2-3 ～ 2-4
デバイス ID
call home の形式 60-25
デフォルト設定
802.1X 49-6
Flex Link 11-2
IP MMLS 31-7
LLDP 17-10
MSTP 20-38
UDLD 51-3
VTP 13-6
音声 VLAN 16-4
スーパーバイザ エンジン 2-1
ダイナミック ARP インスペクション 42-5
デフォルトの VLAN 10-10
デュアルプライオリティ キュー
IP 加入者 24-5, 24-26
デュプレックス モード
インターフェイスの設定 8-6
電源管理
概要 55-1
システムの所要電力、9 スロット シャーシ 55-5
冗長構成のイネーブル化またはディセーブル化 55-2
モジュールの電源投入または切断 55-3
電源の冗長性をイネーブルまたはディセーブルにするコマンド 55-2
電子メール アドレス
call home の割り当て 60-3
電子メール通知
Call Home 60-1
転送遅延時間
MSTP 20-47
転送遅延時間、MSTP 20-47
転送遅延時間、STP 20-36

と

統計情報
802.1X 49-17
独立 VLAN 15-3
独立ポート 15-3
特権
終了 2-12
設定
特権レベル 2-12
複数のレベル 2-11
デフォルトの変更 2-12

ログイン 2-12
トラストポイント 60-3
トラフィック ストーム制御
コマンド
ブロードキャスト 43-4
しきい値 43-1
説明 43-1
モニタリング 43-6
トラフィック フラッディングのブロック 44-1
トラフィック抑制
「トラフィック ストーム制御」を参照
トランク 10-3
802.1Q の制約事項 10-5
DTP をサポートしないデバイス 10-4
VLAN 1 の最小化 10-11
インターフェイスのデフォルト設定 10-7
カプセル化 10-3
許可された VLAN 10-11
異なる VTP ドメイン 10-3
設定 10-8
デフォルトの VLAN 10-10
ネイティブ VLAN 10-10
トランクでサポートされるポート セキュリティ 50-4, 50-5, 50-8, 50-9
トランスレーショナル ブリッジ番号（デフォルト） 14-6
トンネリング 48-4, 48-31
トンネリング、802.1Q の
「802.1Q」を参照 17-1

に

入力ブリッジド IP トラフィックに対する NetFlow および NDE 52-26
認証
「ポートベースの認証」も参照
認証、許可、アカウンティング
「AAA」を参照
認証、許可、アカウンティング（AAA） 40-1

ね

ネイティブ VLAN 10-10

は

バージョン 8（NDE） 52-11
ハードウェア レイヤ 3 スイッチング、注意事項 29-4
バインディング データベース、DHCP スヌーピング
「DHCP スヌーピング バインディング データベース」を参照
パケット
マルチキャスト 37-3
パケット キャプチャ 62-1
パケット再循環 45-12
パケットの書き換え
CEF 29-2
IP MMLS 31-3
パケット バースト 40-17
パス コスト
MSTP 20-44
パスワード
暗号化 2-11
（注意） 2-11
イネーブル パスワードを忘れた場合の回復方法 2-13
設定
TACACS+ 2-10
TACACS+（注意） 2-10
イネーブル シークレット 2-9
イネーブル パスワード 2-9
回線パスワード 2-9
スタティック イネーブル パスワード 2-8
パスワードに関する注意
TACACS+ 2-10
暗号化 2-11
バックアップ インターフェイス
「Flex Link」を参照

ひ

非 RPF マルチキャスト 31-5
光ファイバ、単一方向リンクの検出 51-1
非集約ラベル 26-2, 26-4
標準範囲 VLAN
「VLAN」を参照

ふ

ファブリック スイッチング モード
「SFM」を参照
ファブリック スイッチングモードでは、Supervisor Engine 720 で dcef-only コマンドを許可 5-2, 7-4
フィルタ、NDE
宛先 TCP/UDP ポート、設定 52-29
宛先ホスト フィルタ、指定 52-29
概要 52-8
送信元ホストおよび宛先 TCP/UDP ポート 52-29
プロトコル 52-30
フォールバック ブリッジング 22-2
不揮発性ランダムアクセス メモリ
「NVRAM」を参照
複数パスの RPF チェック 35-2
プライオリティ
CoS の上書き 16-7, 16-8
プライオリティ レート伝播、IP 加入者 24-5, 24-26, 24-27
プライベート VLAN 15-1
IP アドレス指定 15-4
SVI 15-6
エンド ステーション アクセス 15-4
コミュニティ VLAN 15-3
サブドメイン 15-2
セカンダリ VLAN 15-3
設定 15-11
セカンダリ VLAN とプライマリ VLAN 15-13
セカンダリ VLAN 入力トラフィックのルーティング 15-14
プライベートとしての VLAN 15-12
ホスト ポート 15-15
無差別ポート 15-16
設定時の注意事項 15-7, 15-9, 15-11
独立 VLAN 15-3
トラフィック 15-6
複数のスイッチ間 15-5
プライマリ VLAN 15-3
ポート
コミュニティ 15-3
設定時の注意事項 15-9
独立 15-3
無差別 15-3
モニタリング 15-17
利点 15-2
プライマリ VLAN 15-3
プライマリ リンク 11-1
フラッシュ メモリ
書き込み保護 2-19
システム イメージのロード 2-18
セキュリティ上の注意事項 2-19
設定プロセス 2-19
ルータの起動元としての設定 2-19
フラッシュ メモリ カードに関するセキュリティ上の注意事項 2-19
フラッディングのブロック 44-1
ブリッジ ID
「STP ブリッジ ID」を参照
ブリッジ グループ 22-2
ブリッジ プライオリティ、STP 20-34
ブリッジ プロトコル データ ユニット
「BPDU」を参照
ブリッジング 22-1
ブリッジングのスパニングツリー プロトコル 22-2
プルーニング、VTP
「VTP」を参照、プルーニング
フレーム配信
「EtherChannel ロード バランシング」を参照
フロー
IP MMLS

部分的および完全スイッチング 31-4
フロー制御 8-12
ブロードキャスト ストーム
「トラフィック ストーム制御」を参照
フローマスク
IP MLS
destination-ip 52-3
destination-source-ip 52-3
interface-destination-source-ip 52-3
ip-full 52-3
ip-interface-full 52-3
NetFlow（Release 12.2SRA） 52-3
NetFlow（Release 12.2SRB） 52-3, 52-4
概要 52-3
最小限 52-21
ブロッキング ステート、STP 20-7
プロトコル トンネリング
「レイヤ 2 プロトコル トンネリング」を参照 18-1
分散型シスコ エクスプレス フォワーディング
「dCEF」を参照
分類（QoS） 45-112

ほ

ポイントツーポイント GRE トンネル上の IPv4 マルチキャスト 1-4
ポート
デバウンス タイマーの設定 8-13
ポート コスト、STP 20-33
ポート集約プロトコル
「PAgP」を参照
ポート セキュリティ
違反 50-2
エージング 50-10, 50-11
スティッキ セキュア MAC アドレスのイネーブル化 50-8
設定 50-4
説明 50-1
デフォルト設定 50-3
表示 50-11
ポート セキュリティの MAC 移動 50-2
ポートチャネル
「EtherChannel」を参照
switchport trunk encapsulation dot1q 12-6
ポート デバウンス タイマー 8-13
ポート ネゴシエーション 8-7
ポート プライオリティ
MSTP 20-43
ポート プライオリティ、STP 20-31
ポートベース ACL（PACL）。「Private Hosts 機能」を参照
ポートベース認証
EAPOL-Start フレーム 49-3
EAP-Request/Identity フレーム 49-3
EAP-Response/Identity フレーム 49-3
イネーブル化
802.1x 認証 49-8, 49-9
定期的な再認証 49-11
開始およびメッセージ交換 49-3
カプセル化 49-2
クライアント、定義 49-2
スイッチ
RADIUS クライアント 49-2
プロキシとして 49-2
設定
RADIUS サーバ 49-11
クライアントの手動での再認証 49-12
クライアントの認証の初期化 49-12
スイッチからクライアントへの再送信時間 49-13
スイッチ上の RADIUS サーバ パラメータ 49-9
スイッチとクライアント間のフレーム再送信回数 49-15
待機時間 49-13
設定時の注意事項 49-7
説明 49-1
デバイスの役割 49-2
デフォルト値へのリセット 49-17
デフォルト設定 49-6

統計情報の表示 49-17
認証サーバ
RADIUS サーバ 49-2
定義 49-2
方式リスト 49-8
ポート
許可および無許可 49-4
許可ステートおよび dot1x port-control コマンド 49-4
ポート ベースの QoS 機能
「QoS」を参照
ポートベースの認証
設定
スイッチとクライアント間の EAP-Request フレーム再送信時間 49-14
スイッチと認証サーバ間の再送信時間 49-15
トポロジ、サポート対象 49-5
ポート モード 26-25
ホスト ポート 15-3
ポリシー 45-57
ポリシーベース ルーティング
「PBR」を参照
ポリシー マップ 45-65
インターフェイスへの対応付け 45-72
ポリシング
「QoS ポリシング」を参照
ポリシング、QoS（定義） 45-113

ま

マークダウン
「QoS マークダウン」を参照
マイクロフロー ポリシング ルール
「QoS ポリシング」を参照
マクロ、インターフェイス レンジ 8-4
マニュアル、関連資料 liv
マニュアルの構成 li
マルチキャスト
IGMP スヌーピング 33-10
MLDv2 スヌーピング 32-10
NetFlow 統計情報 52-15
PIM スヌーピング 34-4
概要 33-1
非 RPF 31-5
マルチキャスト RPF 31-2
マルチキャスト VPN 28-1
マルチキャスト グループ
加入 33-2
脱退 32-6, 33-4
マルチキャスト グループ、IPv6
加入 32-4
マルチキャスト ストーム
「トラフィック ストーム制御」を参照
マルチキャストの強化 - 出力レプリケーション パフォーマンスの改善 31-14
マルチキャストの強化 - レプリケーション モード検出 31-12
マルチキャスト フラッディングのブロック 44-1
マルチキャスト マルチレイヤ スイッチング
「IPv4 MMLS」を参照
マルチキャスト、ルーティング テーブルの表示 31-21
マルチキャスト レプリケーション モード検出の強化 31-12
マルチレイヤ スイッチ フィーチャ カード
「MSFC」を参照

み

ミニ プロトコル アナライザ 62-1

む

無差別ポート 15-3

も

モニタリング
Flex Link 11-4

プライベート VLAN **15-17**

ゆ

ユーザ ベースのレート制限 **45-19, 45-70**
ユニキャスト RPF **35-2**
ユニキャストおよびマルチキャスト フラッディングのブロック **44-1**
ユニキャスト ストーム
「トラフィック ストーム制御」を参照
ユニキャスト フラッディングのブロック **44-1**
ユニフォーム モード
設定 **48-40**

よ

予約範囲 VLAN
「VLAN」を参照

ら

ラベル エッジ ルータ **26-2**
ラベル スイッチド パス **26-25**
ラベル スイッチング ルータ **26-2, 26-4**

り

略語、リスト **A-1, B-1**
リンク障害、単一方向の検出 **20-25**
リンク冗長性
「Flex Link」を参照
リンク ネゴシエーション **8-7**

る

ルーティング テーブル、マルチキャスト **31-21**
ルート ガード
「STP ルート ガード」を参照
ルート スイッチ
MSTP **20-41**
ルート ブリッジ、STP **20-29**
ループ ガード
「STP ループ ガード」を参照

れ

例
ソフトウェア コンフィギュレーション レジスタ **2-15 ～ 2-18**
レイヤ 2
show interfaces **8-11, 8-12, 10-7, 10-12**
VLAN インターフェイスの割り当て **14-13**
インターフェイスの設定 **10-6**
アクセス ポート **10-13**
トランク **10-8**
インターフェイス モード **10-4**
スイッチング **10-1**
デフォルト **10-5**
トランク **10-3**
レイヤ 2 Traceroute **59-1**
レイヤ 2 traceroute
1 ポートに複数のデバイス **59-2**
ARP **59-2**
CDP **59-1**
IP アドレスおよびサブネット **59-2**
MAC アドレスおよび VLAN **59-2**
使用上の注意事項 **59-1**
説明 **59-1**
マルチキャスト トラフィック **59-2**
ユニキャスト トラフィック **59-1**
レイヤ 2 インターフェイス、設定 **10-1**
レイヤ 2 の再マーキング **45-15**
レイヤ 2 プロトコル トンネリング
概要 **18-1**
レイヤ 2 トンネルの設定 **18-2**
レイヤ 3
IP MMLS および MLS キャッシュ **31-2**
レイヤ 3 スイッチド パケットの書き換え

CEF 29-2
レイヤ 3 スイッチング
CEF 29-2
レイヤ 4 ポート演算（ACL） 36-6
レプリケーション モード検出 31-12
レポート、MLD 32-4
連絡先情報
call home の割り当て 60-3

ろ

ローカル出力レプリケーション 31-14
ロード バランシング 26-8

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/