CHAPTER 37

MPLS および EoMPLS の設定

この章では、Catalyst 3750 Metro スイッチに Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）および Ethernet over MPLS（EoMPLS）を設定する方法について説明します。MPLS は、リンク レイヤ（レイヤ 2）スイッチングとネットワーク レイヤ（レイヤ 3）ルーティングを統合するパケットスイッチング テクノロジーです。MPLS がイネーブルの場合、データは任意のレイヤ 3 プロトコルを使用し、複数のレイヤ 2 テクノロジーを任意に組み合わせて転送されるため、スケーラビリティが高まります。MPLS は、ルータベース インターネット バックボーンを介して送信元と宛先を接続する複数のルートをサポートします。

EoMPLS は、MPLS ネットワークを介してレイヤ 2 イーサネット フレームを転送するトンネリング メカニズムです。ブリッジ、ルータ、またはスイッチを配置しなくても、離れた位置にある 2 つのレイヤ 2 ネットワークを接続することができます。MPLS バックボーンをイネーブルにして、レイヤ 2 トラフィックを受信できるようにするには、MPLS バックボーンの両端にある Label Edge Router（LER; ラベル エッジ ルータ）を設定します。

MPLS 機能がサポートされるのは Enhanced-Services（ES）ポート上のみです。EoMPLS は標準ポートおよび ES ポート上でサポートされます。

（注） MPLS の詳細については、『*Cisco IOS Switching Services Configuration Guide*』Release 12.2 の「Multiprotocol Label Switching」を参照してください。この章で使用する MPLS コマンドの構文および使用方法の詳細については、『*Cisco IOS Switching Services Command Reference*』Release 12.2 を参照してください。
EoMPLS コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

Cisco IOS Release 12.2(25)SED 以降のリリースでは、スイッチで Hierarchical Virtual Private LAN Service（H-VPLS; 階層構造の仮想プライベート LAN サービス）アーキテクチャがサポートされ、MPLS ネットワーク上の LAN サービスがシミュレーションされます。スイッチは、IEEE 802.1Q トンネリングまたは EoMPLS を使用して H-VPLS をサポートします。詳細については、次のソフトウェア マニュアルを参照してください。

- EoMPLS の詳細については、「EoMPLS の概要」（p.37-15）を参照してください。
- EoMPLS の設定の詳細については、「EoMPLS のイネーブル化」（p.37-18）、および「MPLS および EoMPLS QoS の設定」（p.37-21）を参照してください。
- 802.1Q トンネリングの詳細については、「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」の章を参照してください。
- Cisco 7600 ルータでの H-VPLS の設定の詳細については、次の URL にある『*OSM Configuration Note*』12.2SX の「Configuring Multiprotocol Label Switching on the Optical Services Modules」を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00801e5c06.html

MPLS サービスの概要

従来のレイヤ 3 転送では、パケットがネットワークを通過するときに、各ルータでレイヤ 3 ヘッダーからパケット転送情報を抽出します。この情報をインデックスに使用して、ルーティング テーブル検索を実行し、パケットのネクスト ホップを判別します。通常はヘッダー内の宛先アドレス フィールドのみが関連しますが、他のヘッダー フィールドが関連することもあります。このため、パケットが通過する各ルータではパケット ヘッダーを分析する必要があります。

MPLS を使用すると、レイヤ 3 ヘッダーは 1 回のみ分析され、構造化されていない固定長の値（*ラベル*）にマッピングされます。複数の異なるヘッダーで同じネクスト ホップが選択される場合は、これらのヘッダーを同じラベルにマッピングすることができます。実際は、ラベルは*転送同等クラス*を表します。つまり、外見が異なるにもかかわらず、転送機能に関して区別できない一連のパケットを表します。

最初のラベル選択は、レイヤ 3 ヘッダーの内容のみを基準として行うことができます。また、ポリシーを基準とすることにより、後続ホップでの転送判断をポリシーベースで行うこともできます。ラベルが選択されると、レイヤ 3 パケットの前に短いラベル ヘッダーが付加され、パケットの一部としてネットワーク内で伝達されます。ネットワーク内の各 MPLS ルータを経由する後続ホップでは、ラベルが交換されます。ルータはラベルに関する MPLS 転送テーブル検索を実行して、転送判断を行います。パケット ヘッダーを再び分析する必要はありません。ラベルは構造化されていない固定長の値であるため、MPLS 転送テーブル検索プロセスは簡単かつ高速です。

ネットワーク内の各 Label Switching Router（LSR; ラベル スイッチング ルータ）は、転送同等クラスを表すために使用されるラベル値に関して、独立したローカルな判断を行います。この対応関係は、*ラベル バインディング*といいます。各 LSR は、自身が行ったラベル バインディングをネイバに通知します。ラベルの付いたパケットが LSR A から近接する LSR B に送信されると、パケットで伝達されるラベル値は、パケットの転送同等クラスを表すために B が割り当てたラベル値になります。このため、IP パケットがネットワークを通過するにつれて、ラベル値は変更されます。

（注）　Catalyst 3750 Metro スイッチはサービスプロバイダー コア ルータとしてでなく、サービスプロバイダー エッジの顧客配置機器（PE-CLE）として使用されるため、LSR として正常に動作しません。スイッチがラベル スイッチングを実行するのは、ES ポートを介して 2 つの異なるプロバイダー コア ルータに接続されて、冗長パスを実現している場合のみです。この場合、スイッチは Quality of Service（QoS）ポリシーを使用して出力側で MPLS パケットを分類し、ラベル スイッチングを行います。

ラベルは転送同等クラスを表しますが、ネットワーク内の特定のパスは表しません。一般に、ネットワーク内のパスは Open Shortest Path First（OSPF）、Enhanced Interior Gateway Protocol（EIGRP）、Intermediate-System-to-Intermediate-System（IS-IS）、Border Gateway Protocol（BGP）など、既存のレイヤ 3 ルーティング プロトコルによって常に選択されます。各ホップでラベルを検索する場合、ネクスト ホップはダイナミック ルーティング アルゴリズムによって決定されます。

MPLS VPN の概要

MPLS Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を使用すると、ビジネス カスタマー向けのスケーラブルなレイヤ 3 VPN バックボーン サービスの導入や管理を行うことができます。VPN は、1 つまたは複数の物理ネットワーク上でリソースを共有するセキュアな IP ベース ネットワークです。VPN に含まれる地理的に離れたサイトでは、共有バックボーンを介して安全に通信することができます。

VPN ルートは Multiprotocol BGP（MP-BGP）を使用して、MPLS ネットワークを介して配信されます。MP-BGP は各 VPN ルートに対応付けられたラベルも配信します。MPLS VPN は VPN Routing/Forwarding（VRF）サポートを使用して、ルーティング ドメインを相互に隔離します。MPLS VPN を介してルートが取得された場合、スイッチは新しいルートを標準 VRF ルートとして学習します。ただし、ネクスト ホップの宛先 MAC（メディア アクセス制御）アドレスは実際のアドレスでなく、ルートに割り当てられた ID を含む特殊な形式のアドレスです。MPLS-VPN パケットがポートに着信すると、スイッチはルーティング テーブル内でラベルを検索し、パケットの処理内容を決定します。

各 VPN は 1 つまたは複数の VPN VRF インスタンスに対応付けられます。VRF にはルーティング テーブル、転送テーブル、および Customer Edge（CE; カスタマー エッジ）デバイスに接続されたカスタマー デバイスの VPN メンバーシップを定義する規則が格納されています。カスタマー サイトは複数の VPN に属することができますが、1 つのサイトに対応付けることができる VRF は 1 つのみです。VRF には次の要素があります。

- IP ルーティング テーブル
- Cisco Express Forwarding（CEF）テーブル
- CEF 転送テーブルを使用するインターフェイスのセット
- ルーティング テーブル内の情報を制御する規則およびルーティング プロトコル パラメータのセット

カスタマーサイト VRF には、そのサイトで使用可能な、そのサイトが属する VPN のすべてのルートが格納されます。VPN ルーティング情報は、各 VRF の IP ルーティング テーブルおよび CEF テーブルに格納されます。各テーブル セットは VRF ごとに維持されます。これにより、情報が VPN 外部に転送されたり、VPN 外部のパケットが VPN 内のルータに転送されることがなくなります。パケットは VRF IP ルーティング テーブルおよび VRF CEF テーブルに格納されたルーティング情報に基づいて、宛先に転送されます。

PE ルータは CE デバイスから取得された各カスタマー プレフィクスにラベルをバインドし、他の PE ルータにアドバタイズされるプレフィクスのネットワーク到達可能性情報にラベルを追加します。プロバイダー ネットワークを介して CE デバイスから着信したパケットが PE ルータによって転送されると、そのパケットには宛先 PE ルータから取得されたラベルが付加されます。宛先 PE ルータは、ラベルの付いたパケットを受信すると、ラベルを調べて、正しい CE デバイスにパケットを転送するために使用します。バックボーンを通過するカスタマー データパケットが伝達するラベルには、2 つのレベルがあります。

- 上位ラベルは正しい PE ルータにパケットを転送します。
- 2 番めのラベルは、PE ルータが CE デバイスにパケットを転送する方法を定義します。

VPN の利点

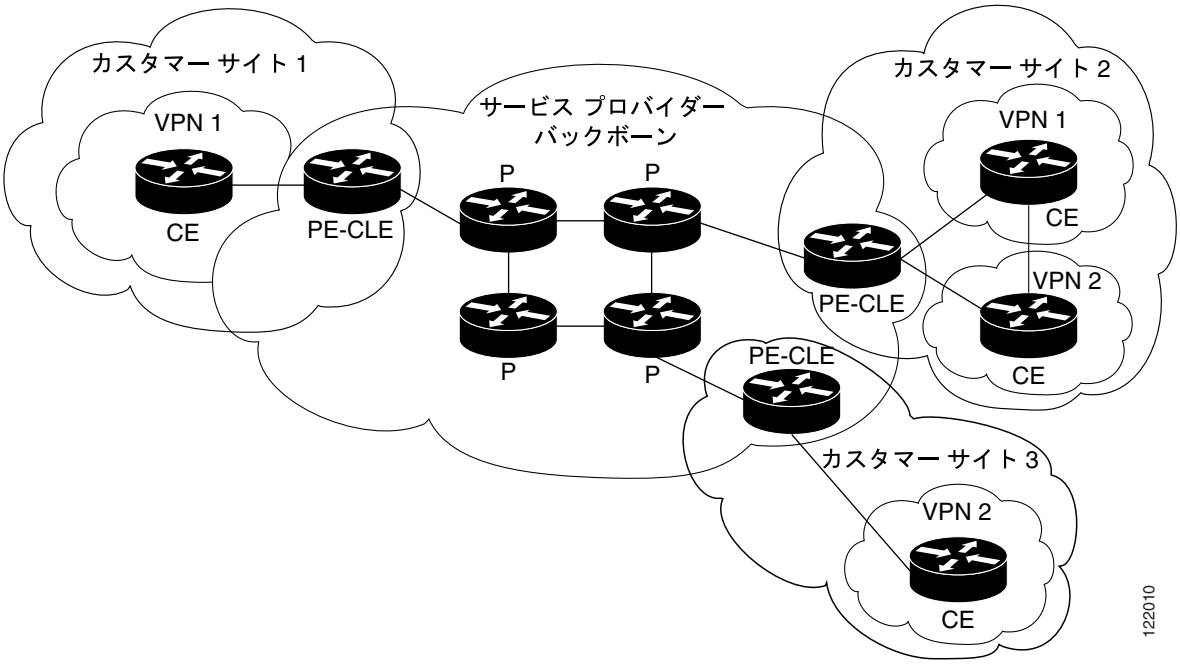
MPLS VPN を使用すると、サービス プロバイダーはスケーラブルな VPN を導入したり、次のような付加価値のあるサービスを提供するための基礎を構築することができます。

- コネクションレス サービス — MPLS VPN はコネクションレスです。つまり、ホスト間の通信を確立する場合に、事前の処理が不要です。コネクションレス VPN では、トンネルおよび暗号化を使用してネットワークのプライバシーを確保する必要がありません。

- 中央集中型サービス — MPLS VPN はプライベート イントラネットとして使用されます。プライベート イントラネットでは、VPN で表されるユーザ グループに目的の IP サービスを提供することができます。
- スケーラビリティ — MPLS ベース VPN ではピア モデルおよびレイヤ 3 コネクションレス アーキテクチャを使用して、スケーラビリティの高いソリューションを利用することができます。ピア モデルでは、カスタマー サイトは 1 つの PE ルータに対するピアとして機能する必要があります。これは、VPN に属する他のすべてのカスタマー PE デバイスまたは CE デバイスと異なります。PE ルータには、メンバーである VPN の VPN ルートが保持されます。コア ネットワーク内のルータには、VPN ルートは保持されません。
- セキュリティ — MPLS VPN はコネクション型 VPN と同じレベルのセキュリティを提供します。特定の VPN からのパケットが、誤って別の VPN に送信されることはありません。プロバイダー ネットワークのエッジに実装されたセキュリティにより、カスタマーから着信したパケットは正しい VPN に送信されます。バックボーンに実装されたセキュリティにより、VPN トラフィックは互いに分離されます。
- 作成が容易 — MPLS VPN はコネクションレスであるため、特定のポイントツーポイント接続マップやトポロジは不要です。サイトをイントラネットおよびエクストラネットに追加して、閉じたユーザ グループを形成することができます。
- 柔軟なアドレス指定 — Network Address Translation（NAT; ネットワーク アドレス変換）を使用しなくても、カスタマーは引き続き現在のアドレス スペースを使用することができます。MPLS VPN によって、パブリック アドレスとプライベート アドレスが対応付けられるためです。NAT が必要となるのは、アドレス スペースが重複する 2 つの VPN が通信する場合のみです。
- 移行が容易 — 複数のネットワーク アーキテクチャ上に MPLS VPN を構築することができます。MPLS をサポートするために CE ルータを配置したり、カスタマーのイントラネットを変更する必要がないため、エンド カスタマーは簡単に移行することができます。
- MPLS VPN を導入すると、BGP の機能も拡張されます。

図 37-1 に、サービスプロバイダー バックボーン ネットワーク、PE-CLE ルータ、および CE デバイスを含む VPN の例を示します。

図 37-1　VPN およびサービス プロバイダー バックボーン



各 VPN には、CE デバイスに接続されたカスタマー デバイスが含まれています。カスタマー デバイスは VPN を使用してデバイス間で情報を交換します。プロバイダー ルータ（P）は VPN を認識しません。

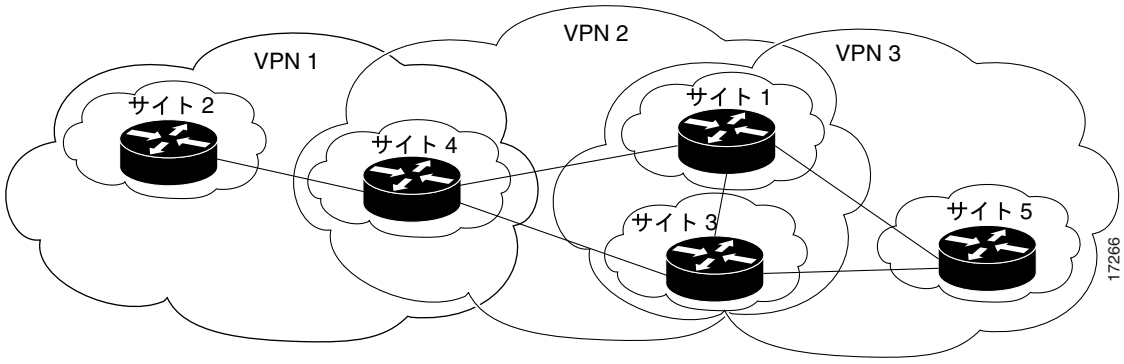
図 37-2 に、3 つの VPN 内で通信を行う 5 つのカスタマー サイトを示します。VPN は次のサイトと通信することができます。

VPN1：サイト 2 および 4

VPN2：サイト 1、3、および 4

VPN3：サイト 1、3、および 5

図 37-2　カスタマー サイトおよび VPN



VPN ルーティング情報の配信

VPN ルーティング情報の配信を制御するには、BGP 拡張コミュニティによって実装される VPN ルート ターゲット コミュニティを使用します。VPN ルーティング情報は、次の方法で配信されます。

- CE デバイスから取得された VPN ルートが BGP プロセスに追加されると、VPN ルート ターゲット拡張コミュニティ アトリビュートのリストが VPN ルートに対応付けられます。アトリビュート値は、ルート取得元の VRF に対応付けられたルート ターゲットのエクスポート リストから取得されます。
- 各 VRF には、ルート ターゲット拡張コミュニティのインポート リストも対応付けられます。インポート リストは、ルートを VRF にインポートする場合にルータに格納されていなければならないルート ターゲット拡張コミュニティ アトリビュートを定義します。たとえば、特定の VRF のインポート リストにルート ターゲット コミュニティ A、B、および C が含まれている場合、これらのルート ターゲット拡張コミュニティ（A、B、または C）のいずれかを伝達するすべての VPN ルートが、この VRF にインポートされます。

PE ルータはスタティックな設定を使用して CE デバイスから IP プレフィクスを取得することができます。そのためには、CE デバイスとの BGP セッション、または CE ルータとの Routing Information Protocol（RIP）交換を使用します。IP プレフィクスは IPv4 アドレス ファミリーのメンバーです。IP プレフィクスを取得すると、PE ルータは IP プレフィクスと 8 バイトの Route Distinguisher（RD）を組み合わせて、IP プレフィクスを VPN-IPv4 プレフィクスに変換します。生成されたプレフィクスは VPN-IPv4 アドレス ファミリーのメンバーです。カスタマー サイトがグローバルに一意でない（未登録のプライベート）IP アドレスを使用している場合でも、カスタマー アドレスを一意に識別します。

BGP は、VPN ごとに VPN-IPv4 プレフィクスの到達可能性情報を配信します。BGP 通信は、IP ドメイン内（別名 Autonomous System [AS; 自律システム]）（Internal BGP [IBGP]）および AS 間（External BGP [EBGP]）の 2 つのレベルで実行されます。PE/PE セッションは IBGP セッションです。PE/CE セッションは EBGP セッションです。

BGP は、IPv4 以外のアドレス ファミリーのサポートを定義する BGP マルチプロトコル拡張機能を使用して、PE ルータ間で VPN-IPv4 プレフィクスの到達可能性情報を伝播します。この方法では、指定された VPN のルートは、この VPN の他のメンバーによってのみ学習されるため、VPN のメンバー間で相互に通信できます。

MPLS VPN の設定

ここでは、PE ルータとして使用される Catalyst 3750 Metro スイッチに MPLS VPN を設定する方法について説明します。

- MPLS のデフォルト設定（p.37-8）
- MPLS VPN 設定時の注意事項（p.37-8）

ここでは、必要な作業について説明します。

- MPLS のイネーブル化（p.37-9）
- VPN の定義（p.37-10）
- BGP ルーティング セッションの設定（p.37-11）
- PE/PE ルーティング セッションの設定（p.37-11）

PE/CE ルーティング セッションも設定する必要があります。ここでは、設定例を示します。

- BGP PE/CE ルーティング セッションの設定（p.37-12）
- RIP PE/CE ルーティング セッションの設定（p.37-12）
- スタティック ルート PE/CE ルーティング セッションの設定（p.37-13）

MPLS VPN 内のパケット フローの例については、「MPLS VPN 内のパケットフロー」（p.37-14）を参照してください。

MPLS のデフォルト設定

通常のルーテッド パスでの IPv4 パケットのラベル スイッチングは、デフォルトでグローバルにイネーブル化されています。インターフェイスでの IPv4 パケットの MPLS 転送は、デフォルトでディセーブルです。

mpls label protocol グローバル コンフィギュレーション コマンドで配信プロトコルが明示的に設定されていない場合は、Tag Distribution Protocol（TDP）がスイッチのデフォルトのラベル配信プロトコルになります。MPLS を使用する場合は、Label Distribution Protocol（LDP）を設定することを推奨します。

インターフェイスにプロトコルが明示的に設定されていない場合は、スイッチのデフォルトのラベル配信プロトコルが使用されます。デフォルトでは、すべての宛先のラベルがすべての LDP ネイバにアドバタイズされます。

VRF は未定義です。インターフェイスのデフォルト ルーティング テーブルは、グローバル ルーティング テーブルです。

MPLS VPN 設定時の注意事項

MPLS を使用するには、スイッチ上で CEF をイネーブルにする必要があります。CEF はデフォルトでイネーブルに設定されています。CEF の詳細については、「CEF の設定」（p.34-90）を参照してください。

スイッチは ES ポートを介して MPLS ネットワークと接続する必要があります。MPLS 設定がサポートされるのは、ES ポートのみです。

MPLS が設定されているインターフェイスには、VLAN（仮想 LAN）マッピングを設定しないでください。

スイッチは合計 26 の VRF および VPN をサポートします。

VRF には PBR テンプレートとの互換性はありません。**sdm prefer routing-pbr** コマンドを入力して PBR テンプレートを設定した場合は、コンフィギュレーションから設定済み VRF がすべて削除されます。PBR および VRF を同じスイッチ上で機能させることはできません。

MPLS のイネーブル化

図 37-1 のようなネットワーク内で MPLS を使用する場合は、MPLS をグローバルにイネーブル化し、PE-CLE ルータ上で明示的に設定する必要があります。

すべての宛先プレフィクスへのパケットに対してラベルスイッチングを行う場合に、ネットワークを介して MPLS を追加導入するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip cef**	デバイス上で CEF がディセーブルの場合は、イネーブルにします。
ステップ 3	**mpls ip**	通常のルーテッド パスで IPv4 パケットの MPLS 転送がディセーブルの場合は、イネーブルにします。
ステップ 4	**mpls label protocol ldp**	スイッチのラベル プロトコルを LDP に設定します。デフォルト プロトコルは TDP です。
ステップ 5	**mpls ldp advertise-labels** [**for** *prefix-access-list* [**to** *peer-access-list*]]	スイッチ上で MPLS ラベル アドバタイズをイネーブルにします。キーワードを指定しない場合は、アドバタイズされるラベルに制限は課せられません。 • （任意）**for** *prefix-access-list* — ラベルをアドバタイズする必要がある宛先を指定します。 • （任意）**to** *peer-access-list* — ラベル アドバタイズを受信する必要がある LDP ネイバを指定します。LSR は、6 バイトの LDP ID の最初の 4 バイトからなるルータ ID によって識別されます。
ステップ 6	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、MPLS ネットワークに接続されているレイヤ 3 ES インターフェイスを指定します。
ステップ 7	**mpls ip**	インターフェイスの通常のルーテッド パスで IPv4 パケットの MPLS 転送をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mpls forwarding table** **show mpls interfaces**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ネットワーク内のすべての PE-CLE ルータおよび該当するインターフェイスに対して上記ステップを繰り返し、すべてのルータおよび接続先インターフェイスを MPLS に対してイネーブルに設定します。

スイッチ上で MPLS をディセーブルにするには、**no mpls ip** グローバル コンフィギュレーション コマンドを使用します。デフォルト TDP に戻すには、**no mpls label protocol ldp** グローバル コンフィギュレーション コマンドを使用します。

VPN の定義

PE-CLE ルータ上で VPN ルーティング インスタンスを定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合にのみ必須）。
ステップ 3	**ip vrf** *vrf-name*	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てて VPN ルーティング インスタンスを定義します。
ステップ 4	**rd** *route-distinguisher*	RD を指定して、VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	指定された VRF のインポート、エクスポート、またはインポート / エクスポート ルート ターゲット コミュニティのリストを作成します。AS 番号と任意の番号（xxx:y）、または IP アドレスと任意の番号（A.B.C.D:y）を入力します。*route-target-ext-community* に、ステップ 4 で入力した *route-distinguisher* と同じ値を設定する必要があります。
ステップ 6	**import map** *route-map*	（任意）VRF に、指定されたインポート ルート マップを関連付けます。
ステップ 7	**export map** *route-map*	（任意）VRF に、指定されたエクスポート ルート マップを関連付けます。
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	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けるレイヤ 3 ES または VLAN インターフェイスを指定します。
ステップ 10	**ip vrf forwarding** *vrf-name*	VRF にレイヤ 3 インターフェイスを関連付けます。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip vrf**	定義された VRF およびインターフェイスを表示します。
ステップ 13	**show ip route vrf** **show ip cef vrf** *vrf-name*	VRF の IP ルーティング テーブルを表示します。 VRF に関連付けられた CEF 転送テーブルを表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VRF を削除し、VRF からすべてのインターフェイスを削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。VRF から特定のインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

BGP ルーティング セッションの設定

プロバイダー ネットワークに BGP ルーティング セッションを設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing**	IP ルーティングをイネーブルにします（IP ルーティングがディセーブルになっている場合にのみ必須）。
ステップ 3	**router bgp** *autonomous-system-number*	BGP ルーティング プロセスをイネーブルにし、他の BGP ルータに渡された AS 番号を割り当てて、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ～ 65535 です。64512 ～ 65535 は、プライベート AS 番号専用です。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*	ローカル AS に対して識別されるネイバ IP アドレスまたは BGP ピア グループを指定します。指定できる AS 番号の範囲は 1 ～ 65535 です。
ステップ 5	**neighbor** *ip-address* **activate**	IPv4 アドレス ファミリーのアドバタイズをアクティブにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp neighbor**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング セッションを削除するには、**no router bgp** *autonomous-system* グローバル コンフィギュレーション コマンドを使用します。

PE/PE ルーティング セッションの設定

IBGP を使用するプロバイダー ネットワークに PE/PE ルーティング セッションを設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コ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 bgp** *autonomous-system-number*	ルータ 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	**address-family vpnv4** [**unicast**]	アドレス ファミリー コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィクスを使用するルーティング セッションを設定します。 （任意）**unicast —** VPNv4 ユニキャスト アドレス プレフィクスを指定します。
ステップ 4	**neighbor** *ip-address* **remote-as** ***as-number***	PE ルータ間の IBGP セッションを定義します。
ステップ 5	**neighbor** *ip-address* **activate**	IPv4 アドレス ファミリーのアドバタイズをアクティブにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** [**ipv4**] [**neighbors**] [**vpnv4**]	BGP の設定を確認します。すべての BGP IPv4 プレフィクスの情報を表示します。
ステップ 8	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング セッションを削除するには、**no router bgp** *autonomous-system* グローバル コンフィギュレーション コマンドを使用します。

BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コ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 bgp** *autonomous-system-number*	BGP ルーティング プロセスに、他の BGP ルータに渡された AS 番号を設定して、ルータ 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	**address-family ipv4** [**unicast**] **vrf** *vrf-name*	PE/CE ルーティング セッション用の EBGP パラメータを定義して、VRF アドレスファミリー コンフィギュレーション モードを開始します。 （注） VRF アドレスファミリー コンフィギュレーション モードでの自動サマリーおよび同期については、デフォルトは *off* です。
ステップ 4	**neighbor** *address* **remote-as** *as-number*	PE および CE ルータ間の EBGP セッションを定義します。
ステップ 5	**neighbor** *address* **activate**	IPv4 アドレス ファミリーのアドバタイズをアクティブにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip bgp** [**ipv4**] [**neighbors**]	BGP の設定を確認します。すべての BGP IPv4 プレフィクスの情報を表示します。
ステップ 8	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング セッションを削除するには、**no router bgp** *as-number* グローバル コンフィギュレーション コマンドを使用します。

RIP PE/CE ルーティング セッションの設定

（注） PE/CE ルーティング セッションには、OSPF ルーティング プロトコルも使用できます。

RIP PE/CE ルーティングを設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コ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 rip**	RIP ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンド	説明
ステップ 3	**address-family ipv4** [**unicast**] **vrf** *-name*	PE/CE ルーティング セッション用の RIP パラメータを定義して、VRF アドレスファミリー コンフィギュレーション モードを開始します。 （注）　VRF　アドレスファミリー　コンフィギュレーション モードでの自動サマリーおよび同期については、デフォルトは *off* です。
ステップ 4	**network** *prefix*	PE/CE リンク上で RIP をイネーブルに設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip rip database** [*network-prefix*]	設定を確認します。
ステップ 7	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティングをディセーブルにするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

スタティック ルート PE/CE ルーティング セッションの設定

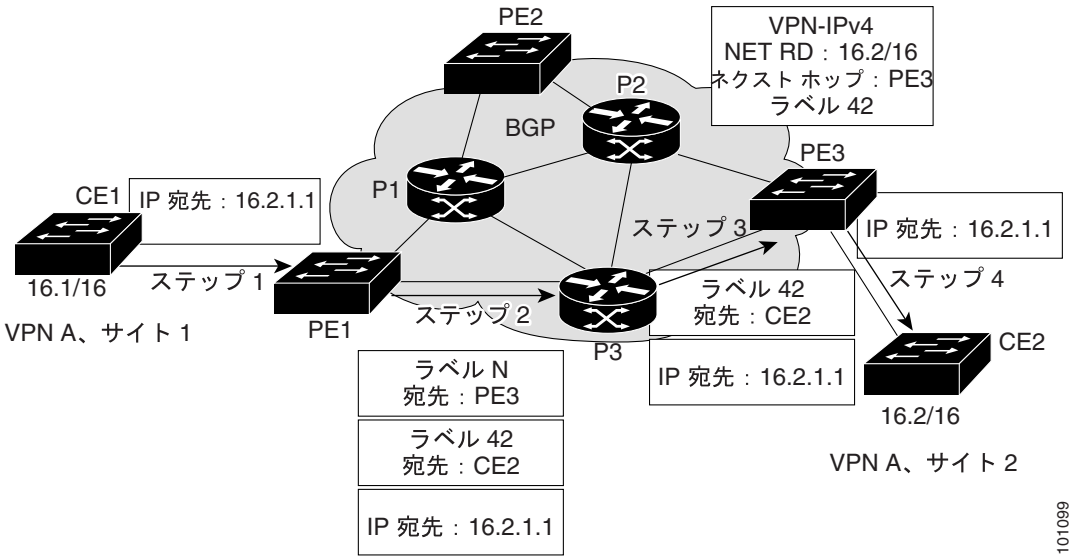
スタティック ルーティングを設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route vrf** *vrf-name prefix mask*	PE/CE セッションに使用する VRF スタティック ルーティング テーブルを定義します。
ステップ 3	**router bgp** *autonomous-system-number*	BGP ルーティング プロセス AS 番号を入力し、ルータ 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	**address-family ipv4** [**unicast**] **vrf** *vrf-name*	PE/CE ルーティング セッションごとにスタティック ルート パラメータを定義して、VRF アドレスファミリー コンフィギュレーション モードを開始します。 （注）　VRF　アドレスファミリー　コンフィギュレーション モードでの自動サマリーおよび同期については、デフォルトは *off* です。
ステップ 5	**redistribute static**	VRF スタティック ルートを VRF BGP テーブルに再配信します。
ステップ 6	**redistribute connected**	直接接続されたネットワークを VRF BGP テーブルに再配信します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip bgp** [**ipv4**]	設定を確認します。
ステップ 9	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

MPLS VPN 内のパケットフロー

図 37-3 に、MPLS VPN ネットワークの 2 つのカスタマー サイト間のパケット フローの例を示します。

図 37-3　MPLS VPN パケット フローの例



スイッチ PE1 のカスタマー（ファスト イーサネット）ポートは、VPN でのルーテッド動作用に設定されています。このポートではスタティック ルーティングまたはルーティング プロトコル（RIP、OSPF、EIGRP、または BGP）を使用して、パケットを転送します。カスタマーの VPN に関連付けられた RD を持つ PE1 スイッチの ES ポートには、MP-BGP が設定されています。MP-BGP は、この RD を使用している ES ポートを介して、ルートおよび関連付けられた VPN ラベルを再配信するように設定されています。

パケット フローに関する手順は、次のとおりです。

ステップ 1　PE スイッチ PE1（Catalyst 3750 Metro スイッチなど）は、サイト 1 のカスタマー スイッチからパケットを受信します。スイッチは検索テーブルから、VRF が MPLS を実行している VLAN であることを判別し、MPLS 検索テーブルを使用して、パケットの処理内容を判別します。MPLS 検索テーブルには、宛先 MAC アドレスとしてピア LSR、および送信元 MAC アドレスとしてローカル インターフェイスが格納されています。

ステップ 2　PE1 は適切なネクスト ホップおよびラベルが設定された BGP ルートを検出し、パケットに適切なラベルを追加して、ES ポートからネクスト ホップ ルータ（P3）にパケットを転送します。

ステップ 3　P3 ルータはこのパケットを受信し、パケットの上位ラベル（Interior Gateway Protocol [IGP; 内部ゲートウェイ プロトコル]）に基づいて MPLS-VPN ネットワークを介してパケットを転送してから、上位ラベルを削除します。

ステップ 4　PE3 はパケットを受信し、MPLS カプセル化を解除して、パケットを転送します。転送する場合は、宛先として CE スイッチ CE2 が設定されたパケット内の VPN ラベルに関連付けられた VRF インターフェイスを使用します。

EoMPLS の概要

Any Transport over MPLS（AToM）は MPLS ネットワーク上でレイヤ 2 パケットを転送するためのソリューションです。サービス プロバイダーは MPLS ネットワークを使用して、既存のレイヤ 2 ネットワークが設定されたカスタマー サイト間を接続することができます。サービス プロバイダーは、ネットワーク管理環境によってネットワークを分離しなくても、MPLS ネットワークを使用して、各カスタマーにすべてのタイプのトラフィックを転送することができます。Catalyst 3750 Metro スイッチは、トンネリング メカニズムを使用してレイヤ 2 イーサネット トラフィックを搬送する AToM のサブセットである EoMPLS をサポートしています。

EoMPLS は、MPLS パケットをイーサネット フレームにカプセル化し、MPLS ネットワーク上で転送します。各フレームは単一のパケットとして転送されます。バックボーンに接続された PE ルータは、必要に応じてパケット カプセル化用ラベルを追加したり、削除したりします。

- 入力 PE ルータはイーサネット フレームを受信し、プリアンブル、Start of Frame Delimiter（SFD）、および Frame Check Sequence（FCS）を削除して、パケットをカプセル化します。それ以外のパケット ヘッダーは変更されません。
- 入力 PE ルータはポイントツーポイント Virtual Connection（VC）ラベルおよび Label Switched Path（LSP; ラベル スイッチド パス）トンネル ラベルを追加して、MPLS バックボーンを介して通常の MPLS ルーティングを行います。
- ネットワーク コア ルータは LSP トンネル ラベルを使用して、MPLS バックボーンを介してパケットを送信します。MPLS バックボーンでは、イーサネット トラフィックと他のタイプのパケットを区別しません。
- MPLS バックボーンの反対側では、出力 PE ルータがパケットを受信し、LSP トンネル ラベルが付加されている場合はこれを削除して、パケットのカプセル化を解除します。PE ルータは、パケットから VC ラベルも削除します。
- PE ルータは必要に応じてヘッダーを更新し、該当するインターフェイスから宛先スイッチにパケットを送信します。

MPLS バックボーンはトンネル ラベルを使用して、PE ルータ間でパケットを転送します。出力 PE ルータは VC ラベルを使用して、イーサネット パケットの発信インターフェイスを選択します。EoMPLS トンネルは単一方向です。双方向の EoMPLS を実現するには、各方向にトンネルを 1 つずつ設定する必要があります。

ポイントツーポイント VC を使用するには、2 つの PE ルータに VC エンドポイントを設定する必要があります。レイヤ 2 トラフィックの転送専用 VC に関する情報を取得するのは、MPLS バックボーンの入口および出口にある PE ルータのみです。その他のルータには、これらの VC のテーブル エントリは格納されません。

ここでは、次の内容について説明します。

- 他の機能との相互作用（p.37-15）
- EoMPLS の制限（p.37-17）

他の機能との相互作用

ここでは、EoMPLS と他の機能との相互作用について説明します。具体的な内容は次のとおりです。

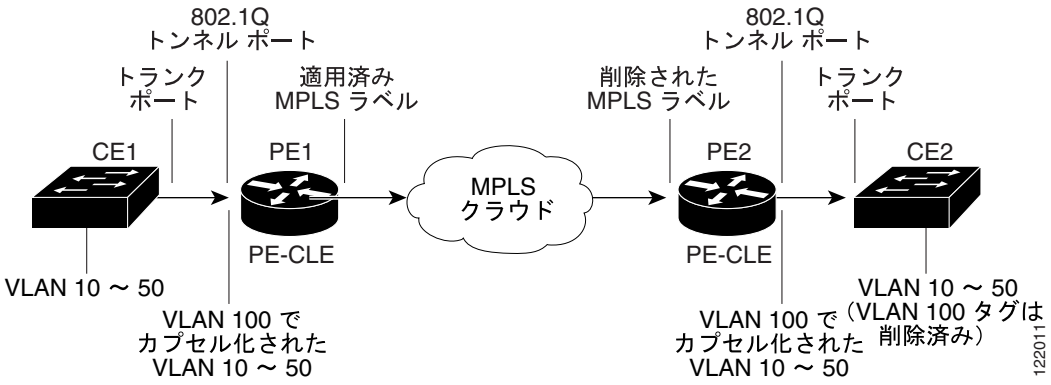
- EoMPLS および 802.1Q トンネリング（p.37-16）
- EoMPLS およびレイヤ 2 トンネリング（p.37-16）
- EoMPLS および QoS（p.37-17）

EoMPLS および 802.1Q トンネリング

IEEE 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することができます。この際に、カスタマーの VLAN ID は保護され、複数の VLAN のトラフィックが集約されます。802.1Q トンネリングの詳細については、第 16 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

図 37-4 に、MPLS ネットワーク上で EoMPLS を使用して、802.1Q トンネリング トラフィックを転送する設定の例を示します。PE-CLE として機能するスイッチを介してレイヤ 2 デバイスが MPLS ネットワークに接続されているトポロジ内で、802.1Q トンネリングをサポートするには、802.1Q トンネリング カプセル化トラフィック（PE1）を受信する PE-CLE の入力 LAN ポートを、VLAN 100 トラフィックを受信するトンネル ポートとして設定します。PE1 のインターフェイスはポートベース EoMPLS 転送用に、PE2 のインターフェイスは宛先 IP アドレスとして設定されます。CE1 から着信した VLAN 10 ～ 50 のパケットは、VLAN 100 でカプセル化されて、MPLS ネットワークに接続された PE1 出力ポートに送信されます。出力ポートでは、MPLS タグがフレーム ヘッダーに追加されたあと、VC にマッピングされ、次の MPLS PE-CLE（PE2）に転送されます。

図 37-4　EoMPLS の例



VLAN ベース EoMPLS の場合は VLAN に、ポートベース EoMPLS の場合はイーサネット ポートに **mpls l2transport route** または **xconnect** 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、カスタマー VLAN またはイーサネット ポートに基づいてトラフィックを転送するように、EoMPLS トンネルを設定することができます。

- MPLS コアを介して、MPLS ネットワークの反対側の特定の受信側に、802.1Q トンネルによってカプセル化されたトラフィックを転送するには、ポートベース EoMPLS を設定します。
- 802.1Q トンネルによってカプセル化されたトラフィックをアクセス デバイスから PE ルータに転送するには、VLAN ベース EoMPLS を設定します。

EoMPLS およびレイヤ 2 トンネリング

EoMPLS リンクを介してレイヤ 2 プロトコル トンネリングを行うと、CDP、STP、および VTP Protocol Data Unit（PDU; プロトコル データ ユニット）を MPLS ネットワークを介してトンネリングすることができます。レイヤ 2 デバイスが PE として機能するスイッチを介して MPLS ネットワークに接続されている場合に、レイヤ 2 プロトコル トンネリングをサポートするには、レイヤ 2 プロトコル トラフィックを受信する PE の入力ポートをトンネル ポートとして設定します。レイヤ 2 プロトコル トラフィックがカプセル化されてから、MPLS ネットワークを介して転送されます。レイヤ 2 プロトコル トンネリングの詳細については、第 16 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

EoMPLS および QoS

EoMPLS はラベル内の 3 つの EXP（試験）ビットを使用してパケットのプライオリティを判別することにより、QoS をサポートします。LER 間で QoS をサポートするには、VC とトンネル ラベルの両方に EXP ビットを設定します。EoMPLS QoS 分類は入力側で実行されます。照合できるのはレイヤ 3 パラメータ（IP や DSCP など）のみであり、レイヤ 2 パラメータ（CoS［サービス クラス］）は照合されません。EoMPLS および QoS の詳細については、「MPLS および EoMPLS QoS の設定」（p.37-21）を参照してください。

EoMPLS の制限

EoMPLS に適用される制限事項は、次とのとおりです。

- EoMPLS を使用するには、MPLS 用として少なくとも 1 つの ES ポートを設定する必要があります。したがって、ES ポートで EoMPLS を稼働させる場合に、EoMPLS を設定できるのは、MPLS が設定されていない ES ポート上のみです。
- MTU（最大伝送ユニット）— EoMPLS はパケットの分割および再組み立てをサポートしていません。したがって、受信された最大のレイヤ 2 VLAN 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 MTU を設定する必要があります。入力および出力 PE ルータには、同じ MTU 値を設定する必要があります。
- アドレス形式 — MPLS 転送を適切に動作させるには、PE ルータのすべてのループバック アドレスに 32 ビット マスクを設定する必要があります。OSPF では、ループバック アドレスを使用する必要があります。
- パケット形式 — 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。PE および CE ルータ間では、ISL（スイッチ間リンク）カプセル化はサポートされません。
- スイッチ上で EoMPLS を使用する VLAN の最大数は 1005 です。
- レイヤ 2 接続に関する制限：
  - EoMPLS を使用する場合は、PE ルータ間を直接レイヤ 2 で接続することはできません。
  - MPLS バックボーンを介してイーサネット VLAN を転送するようにルータが設定されている場合は、これらのルータ間に複数のレイヤ 2 接続を設定することはできません。別のレイヤ 2 接続を追加すると、ピア ルータ上でスパニングツリーがディセーブルの場合、スパニングツリー ステートが頻繁に切り替わります。
- EoMPLS およびトランキングに関する制限：
  - EoMPLS バックボーンでイーサネット スパニングツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）をサポートするには、EoMPLS VLAN の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 の伝達経路がカスタマー スイッチへのトランクに限定されます。
  - トランクのネイティブ VLAN を EoMPLS VLAN にすることはできません。
- 802.1Q インターフェイス上で EoMPLS をイネーブルにするには、**mpls l2transport route** または **xconnect** インターフェイス コンフィギュレーション コマンドを使用します。
- EoMPLS が設定されているインターフェイスには、VLAN マッピングを設定しないでください。
- プライベート VLAN インターフェイスで EoMPLS を設定しないでください。

EoMPLS のイネーブル化

ここでは、PE ルータとして使用されるスイッチに EoMPLS を設定する方法について説明します。

EoMPLS のデフォルト設定

デフォルトで、EoMPLS は設定されていません。

mpls ldp router-id コマンドはディセーブルです。VC は設定されていません。

EoMPLS 設定時の注意事項

EoMPLS を設定する場合は、次の注意事項を考慮してください。

- EoMPLS を使用するには、MPLS 用として少なくとも 1 つの ES ポートを設定する必要があります。したがって、ES ポートで EoMPLS を稼働させる場合に、EoMPLS を設定できるのは、MPLS が設定されていない ES ポート上のみです。
- EoMPLS をイネーブルにする前に、インポジション LER とディスポジション LER の間のすべてのパスに対して **mpls ip** インターフェイス コンフィギュレーション コマンドを使用して、ダイナミック MPLS ラベリングをイネーブルにする必要があります。デフォルトで、MPLS はグローバルにイネーブルに設定されています。
- VLAN ベース EoMPLS の場合は、スイッチに VLAN を設定する必要があります。
- 2 つの PE ルータ間で EoMPLS を稼働させるには、ルータ間の LDP セッションが必要です。各ルータで LDP ルータ ID として使用される IP アドレスは、他のルータから IP 到達可能でなければなりません。IP アドレスを使用する必要があるインターフェイスを指定して、LDP ルータ ID の選択を制御するには、任意の **mpls ldp router-id** グローバル コンフィギュレーション コマンドを使用します。
  - 指定されたインターフェイスが起動していて、IP アドレスが設定されている場合は、このコマンドを使用するときに任意の **force** キーワードを省略できます。ルータ ID を選択する場合は、この IP アドレスがルータ ID として選択されます。
  - 指定されたインターフェイスが起動していないか、または IP アドレスが設定されていない場合に、指定されたインターフェイスの IP アドレスがインターフェイスの起動時に使用されるように設定するには、**force** キーワードを指定してこのコマンドを使用します。
- 両方の PE ルータに、ルータ間の VC を作成する場合に使用できるループバック アドレスを設定する必要があります。OSPF を IGP として使用する場合に、PE ルータ間で MPLS 転送を適切に稼働させるには、PE ルータのすべてのループバック アドレスに 32 ビット マスクを設定する必要があります。
- VLAN マッピングが設定されているインターフェイスには、EoMPLS を設定しないでください。

EoMPLS の設定

VLAN インターフェイスには、VLAN ベース EoMPLS を設定します。VLAN ベース EoMPLS がイネーブルの場合、スイッチは VLAN ID に基づいてトンネルと VC ラベルを関連付けます。ES インターフェイス上でポートベース EoMPLS をイネーブルにする場合は、同じコマンドを使用します。

2 つのエンドポイント間でレイヤ 2 パケットを転送するように EoMPLS を設定するには、PE-CLE ルータ上で特権 EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mpls label protocol ldp**	すべてのインターフェイスで LDP をイネーブルにします。デフォルトで、TDP はイネーブルに設定されます。このコマンドを使用すると、すべてのインターフェイスが LDP を使用するように設定されます。
ステップ 3	**interface loopback0**	ループバック インターフェイスに対して、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	**ip address** *ip-address subnet mask*	ループバック インターフェイスに IP アドレスを割り当てます。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**mpls ldp router-id loopback0 force**	（任意）ループバック インターフェイス 0 の IP アドレスをルータ ID として使用するように強制的に設定します。
ステップ 7	**interface** *interface-id*	レイヤ 3 VLAN（VLAN ベース EoMPLS の場合）または ES ポートのインターフェイス ID（ポートベース EoMPLS の場合）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。
ステップ 8	**mpls l2transport route** *destination vc-id* または **xconnect** *destination vc-id* **encapsulation mpls**	MPLS を介してレイヤ 2 VLAN パケットを転送するようにインターフェイスを設定します。 • *destination* ― VC の反対側にある PE ルータの IP アドレス • *vc-id* ― VC に定義された一意の値。vc-id は VC のエンドポイントに関連付けられます。この値は、VC の両端で同じでなければなりません。指定できる範囲は 1 ～ 4294967295 です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show mpls l2transport vc**	設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EoMPLS トンネルを削除するには、**no mpls l2transport route** *destination vc-id* または **no xconnect** *destination vc-id* **encapsulation mpls** インターフェイス コマンドを使用します。

次に、スイッチ PE1 の VLAN 3 インターフェイスと PE2 の VLAN 4 インターフェイス間に EoMPLS トンネルを設定する例を示します。

PE1 の IP アドレスは 10.0.0.1/32、PE2 の IP アドレスは 20.0.0.1/32 です。両方の PE ルータに、MPLS コアとの MPLS 接続が設定されています。VC ID は 123 です。

PE1 スイッチに、次のコマンドを入力します。

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 10.10.10.10 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface vlan 3
Switch(config-if)# mpls l2transport route 20.0.0.1 123
```

PE2 スイッチに、次のコマンドを入力します。

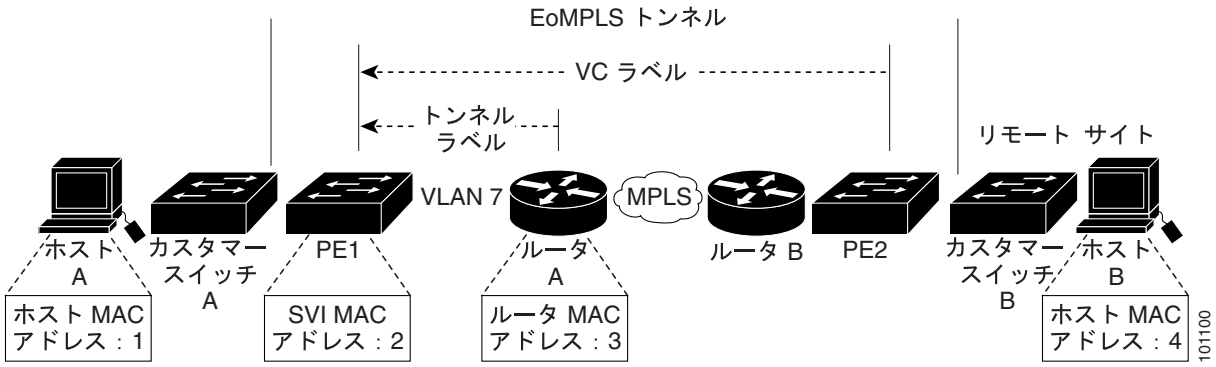
```
Switch(config)# interface loopback0
Switch(config-if)# ip address 20.20.20.20 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface vlan 4
Switch(config-if)# mpls l2transport route 10.0.0.1 123
```

EoMPLS ネットワークのパケット フロー

図 37-5 に、EoMPLS ネットワークのパケット フローの例を示します。PE1 のカスタマー ポートは、PE2 のリモート カスタマー ポートへのポート単位 EoMPLS トンネル用に設定されています。この設定により、これらのポートに接続された、物理的に離れている 2 つのカスタマー スイッチ（A および B）は、同じ物理 LAN 上で直接接続されているかのように認識されます。

EoMPLS トンネルにはスイッチ B の IP アドレス、およびリモート カスタマー ポートに関連付けられた VC ID が設定されています。PE1 は、ルータ A（PE1 の ES ポートに接続）から LDP によってアドバタイズするラベルを使用して、PE2 とのトンネル LSP を確立します。次に、PE1 は PE2 とのターゲット LDP セッションを確立して、VC ID に関連付けられた VC ラベルをアドバタイズします。PE2 に EoMPLS トンネルが設定されている場合、PE2 もターゲット LDP セッションを確立して、VC ID に関連付けられた VC ラベルをアドバタイズします。これにより、スイッチ PE1 とスイッチ PE2 の 2 つの ES ポート間に、EoMPLS トンネルが確立されます。

図 37-5　EoMPLS パケット フローの例



ホスト A が VLAN 3 上のカスタマー スイッチに接続されていて、この VLAN 3 のトランク ポートが 802.1Q タギング用に設定された PE1 に接続されているとします。ホスト A は、MAC アドレス、ラベル、および VLAN の特定の値を使用して（図を参照）、パケットをホスト B に送信します。カスタマー スイッチはホスト パケットにタグを付加し、トランク ポートを介して PE1 に転送します。

タグ付きパケットは、ポート単位 EoMPLS トンネリング用に設定された CE ポートに着信します。PE1 スイッチはパケット ヘッダーを調べて、スイッチに格納されたテーブルを検索し、パケットの処理内容を判別します。ポートにはポート単位 EoMPLS トンネリングが設定されているため、スイッチはパケット内の VLAN タグを削除しないで、内部 VLAN にパケットを割り当てます。カスタマー ポートおよび ES ポートにのみ、内部 VLAN が設定されています。したがって、PE1 ES ポートがパケットの唯一の宛先となります。

ES ポートはトンネル ラベルおよび VC ラベルを含めてパケット ヘッダーをカプセル化し、パケットをネクスト ホップ（この場合はルータ A）に転送し、そこから MPLS ネットワークにパケットを送信します。

ルータはパケットを受信し、MPLS ネットワークを介してリモート PE2 スイッチに転送します。PE2 は MPLS カプセル化を解除し、VC ラベルに関連付けられたポートからパケットを送信します。カスタマー スイッチ B は最終的な VLAN タグを削除し、パケットをリモート ホスト B に転送します。

VLAN ベース EoMPLS パケット フローは、基本的にポートベース EoMPLS と同じです。ただし、内部 VLAN でなく、カスタマー VLAN が使用されます。PE1 スイッチはカスタマー VLAN ID を検索して、パケットを ES ポートに転送するかを判別します。ここで、パケットは再び調べられ、該当する VLAN の EoMPLS に基づいて、トンネル ラベルおよび VC ラベルとともにカプセル化されます。

MPLS および EoMPLS QoS の設定

MPLS および EoMPLS で QoS を使用すると、ネットワーク管理者は MPLS ネットワーク上で異なる Type of Service（ToS; サービス タイプ）を提供することができます。各パケットは、パケット QoS によって指定された特定の種類のサービスを受信できます。QoS IP precedence ビットを保護するには、QoS をグローバルにディセーブルにする必要があります。

QoS をイネーブルにしたあとで、Differentiated Services Code Point（DSCP）または IP precedence ビットを保護するには、インターフェイス レベルの信頼設定を使用します。詳細については、「ポートの信頼状態による入力分類の設定」（p.32-53）を参照してください。ただし、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自動的に上書きされます。たとえば、DSCP ビットが保護されている場合、IP precedence および CoS ビットは DSCP ビットの値によって上書きされます。また、MPLS ラベル内の 3 つの EXP ビットを使用してパケットのプライオリティを判別することにより、MPLS および EoMPLS QoS プライオリティを設定することもできます。

（注）　スイッチでサポートされるのは、MPLS および EoMPLS の DSCP および IP precedence 分類のみです。

ここでは、次の情報について説明します。

MPLS QoS の概要

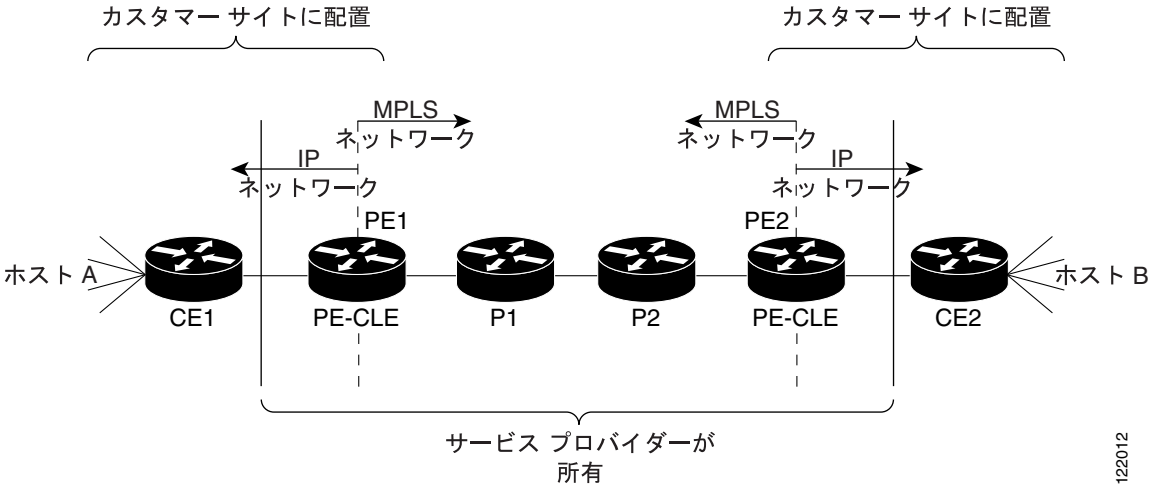
MPLS ネットワークでは、サービスを複数の方法で指定することができます。たとえば、IP パケット内の IP precedence ビット設定を使用します。サイト間で IP パケットを送信する場合は、IP precedence フィールド（IP パケットのヘッダー内の DSCP フィールドの最初の 3 ビット）によって QoS が指定されます。IP precedence のマーキングに基づいて、遅延や帯域幅などの目的の処理がパケットに設定されます。ネットワークが MPLS ネットワークの場合、IP precedence ビットはネットワーク エッジの MPLS EXP フィールドにコピーされます。

サービス プロバイダーは MPLS パケットの QoS 値を別の値に設定することもできます。サービス プロバイダーはカスタマーに属する IP precedence フィールドの値を上書きしないで、MPLS EXP フィールドを設定することができます。カスタマーは引き続き IP ヘッダーを使用することができます。パケットが MPLS ネットワークを通過するときに、IP パケットの QoS は変化しません。

MPLS EXP フィールドに別の値を選択することにより、レートやタイプなどの特性に基づいてパケットにマーキングすることができます。これにより、輻輳期間中に必要となるプライオリティをパケットに設定することができます。

図 37-6 に、カスタマーに属する IP ネットワークの 2 つのサイトを接続する MPLS ネットワークを示します。

図 37-6　2 つのカスタマー サイトを接続する MPLS ネットワーク



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配置された顧客配置ルータであり、入力および出力 PE デバイスです。CE1 および CE2 は CE デバイスです。P1 および P2 は、サービスプロバイダー ネットワークの中心にあるサービス プロバイダー ルータです。

パケットは PE1（入力 PE-CLE ルータ）に IP パケットとして着信します。PE1 は着信したパケットを MPLS パケットとして MPLS ネットワークに送信します。サービスプロバイダー ネットワーク内では、パケットは MPLS パケットであるため、キューイング メカニズムが検索する IP precedence フィールドは存在しません。パケットは PE2（出力 PE-CLE ルータ）に着信するまで、MPLS パケットのままです。PE2 は各パケットからラベルを削除し、パケットを IP パケットとして転送します。

サービス プロバイダーは MPLS QoS を使用することにより、タイプ、入力インターフェイス、およびその他の要素に従ってパケットを分類できます。その場合には、IP precedence または DSCP フィールドを変更しないで、MPLS EXP フィールド内に各パケットを設定（マーキング）します。IP precedence または DSCP ビットを使用すると、IP パケットに対して QoS を指定できます。MPLS EXP ビットを使用すると、MPLS パケットに対して QoS を指定できます。MPLS ネットワーク内の MPLS パケットに QoS 値を設定するには、PE1（入力ルータ）で MPLS EXP フィールド値を設定します

パケットに正しいプライオリティを割り当てることが重要です。パケットのプライオリティは、輻輳期間中のパケットの処理方法に影響します。たとえば、サービス プロバイダーとカスタマーとの間に、サービス プロバイダーが提供するトラフィック量を指定するサービスレベル契約が交わされているとします。契約に準拠するには、カスタマーは合意したレートを超えるレートで送信しないようにする必要があります。パケットはレートに適合するか、または適合しないかのどちらかです。ネットワークに輻輳が発生した場合は、レートに適合しないパケットをより積極的に廃棄することができます。

MPLS および EoMPLS QoS のイネーブル化

ここでは、入力 PE ルータに MPLS QoS を設定する方法について説明します。具体的な内容は次のとおりです。

- MPLS および EoMPLS QoS のデフォルト設定（p.37-23）
- EXP ビットによるパケットのプライオリティの設定（p.37-23）

QoS の詳細については、第 32 章「QoS の設定」を参照してください。

MPLS および EoMPLS QoS のデフォルト設定

QoS はディセーブルに設定されています。パケットは変更されません。また、パケット内の CoS、DSCP、および IP precedence 値も変更されません。トラフィックはパススルー モードでスイッチングされます（パケットは書き換えられずにスイッチングされ、ポリシングを伴わないベストエフォート型として分類されます）。

VLAN ベース EoMPLS パケットのデフォルトの動作では、802.1p ビットが VC およびトンネル ラベルの EXP ビットにリレーされます。ポートベース EoMPLS パケットのデフォルトの動作では、VC およびトンネル ラベルの EXP ビットに値 0 が使用されます。階層型 QoS ポリシーを ES ポートに適用すれば、VLAN ベースまたはポートベースの EoMPLS のデフォルト動作を変更できます。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP は 0 に設定されます）。ポリシー マップは設定されていません。

（注） MPLS および EoMPLS QoS の場合、照合できるのはレイヤ 3 パラメータ（IP または DSCP 値）のみです。レイヤ 2 パラメータ（CoS 値）は照合されません。

EXP ビットによるパケットのプライオリティの設定

MPLS および EoMPLS を使用すると、ラベル内の 3 つの EXP ビットを使用してパケットのプライオリティを判別し、入力ルータで QoS を実行することができます。LER 間で QoS をサポートするには、VC とトンネル ラベルの両方に EXP ビットを設定します。EXP ビットに値を割り当てない場合は、802.1Q ヘッダー タグ制御情報フィールドのプライオリティ ビットが EXP ビット フィールドに書き込まれます。

このプロセスでは、入力ルータで次の作業を行います。

- DSCP または IP precedence 分類に従って IP パケットを分類するように、クラス マップを設定します。

  （注） スイッチでサポートされるのは、MPLS および EoMPLS の DSCP および IP precedence 分類のみです。

- MPLS パケットをマーキングするように（分類情報を MPLS EXP フィールドに書き込むように）、ポリシー マップを設定します。
- サービス ポリシーを付加するように、入力インターフェイスを設定します。

EoMPLS または MPLS QoS 用に EXP ビットを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。 デフォルト設定における QoS の動作については、第 32 章「QoS の設定」を参照してください。
ステップ 3	**class-map** *class-map-name*	トラフィック クラスの名前を指定し、クラスマップ コンフィギュレーション モードを開始します。

	コマンド	説明
ステップ 4	**match** {**ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	802.1Q パケットの一致条件を指定します。 • **ip dscp** *dscp-list* — 着信パケットと比較する最大 8 つの IP DSCP 値。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* — 着信パケットと比較する最大 8 つの IP precedence 値。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。 （注）　MPLS および EoMPLS に対して、**cos** および **vlan** キーワードはサポートされません。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map** *policy-map-name*	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class** *class-name*	**class-map** コマンドを使用して事前に設定されたトラフィック クラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**set mpls experimental** *exp-number*	指定されたポリシー マップとパケットが一致する場合に、MPLS ビットに設定する値を指定します。指定できる範囲は 0 ～ 7 です。
ステップ 9	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *interface-id*	インターフェイス ID を入力し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは入力ルータの ES 出力ポートでなければなりません。
ステップ 12	**service-policy output** *policy-map-name*	指定されたポリシー マップを出力インターフェイスに付加します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show policy-map** [***policy-map-name*** [**class** *class-map-name*]] **show policy-map interface** *interface-id*	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラスを削除するには、**no class** *class-name* ポリシーマップ コンフィギュレーション コマンドを使用します。

次に、クラスおよびポリシー マップを使用して、MPLS QoS の DSCP および IP precedence 用に異なる各 EXP ビットを設定する例を示します。

```
Switch(config)# class-map match-all gold-class
Switch(config-cmap)# match ip dscp 1
Switch(config-cmap)# exit
Switch(config)# class-map match-all silver-class
Switch(config-cmap)# match ip precedence 2
Switch(config-cmap)# exit

Switch(config)# policy-map out-policy
Switch(config-pmap)# class gold-class
Switch(config-pmap-c)# set mpls experimental 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# set mpls experimental 4
Switch(config-pmap-c)# exit

Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# end
```

MPLS および EoMPLS のモニタおよびメンテナンス

MPLS カウンタを消去したり、MPLS および EoMPLS 情報を表示したりするには、表 37-1 に記載された特権 EXEC コマンドを使用します。

表 37-1　MPLS および EoMPLS 情報表示用のコマンド

コマンド	説明
clear mpls counters	MPLS 転送カウンタをクリアします。
show mpls forwarding-table	MPLS Label Forwarding Information Base（LFIB）の内容を表示します。
show mpls interfaces	ラベル スイッチング用に設定されたインターフェイスの情報を表示します。
show mpls ip binding	LDP によって取得されたラベル バインディングに関する指定された情報を表示します。
show mpls l2transport vc [**detail**] [**summary**]	PE デバイスでレイヤ 2 パケットをルーティングするためにイネーブル化された EoMPLS VC に関する詳細情報、またはサマリー情報を表示します。
show mpls l2transport vc [*vc-id*] [*vc-id-min - vc-id-max*]	指定された VC または VC 範囲に関する情報を表示します。指定できる範囲は 1 ～ 4294967295 です。
show mpls label range	パケット インターフェイスで使用可能なローカル ラベルの範囲を表示します。
show mpls ldp bindings	Label Information Base（LIB）の内容を表示します。
show mpls ldp discovery	LDP 検出プロセスのステータスを表示します。
show mpls ldp neighbor	LDP セッションのステータスを表示します。
show mpls ldp parameters	現在の LDP パラメータを表示します。
show mpls prefix-map	標準 IP アクセス リストを照合するネットワーク プレフィクスに QoS マップを割り当てるためのプレフィクス マップを表示します。
show mpls ldp backoff	設定済みのセッション設定バックオフ パラメータ、およびセッション設定をスロットリングするときに使用される任意の LDP ピアに関する情報を表示します。