MPLS レイヤ 3 VPN の設定

MPLS バーチャル プライベート ネットワーク（VPN）は、マルチプロトコル ラベル スイッチング（MPLS）プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1 つ以上のカスタマー エッジ（CE）デバイスが、1 つ以上のプロバイダー エッジ（PE）デバイスに接続されます。このモジュールでは、MPLS レイヤ 3 VPN の作成方法について説明します。

MPLS レイヤ 3 VPNs

MPLS バーチャル プライベート ネットワーク（VPN）は、マルチプロトコル ラベル スイッチング（MPLS）プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1 つ以上のカスタマー エッジ（CE）デバイスが、1 つ以上のプロバイダー エッジ（PE）デバイスに接続されます。この章では、MPLS VPN の作成方法について説明します。

MPLS バーチャル プライベート ネットワークの前提条件

- マルチプロトコル ラベル スイッチング（MPLS）、ラベル配布プロトコル（LDP）、および Cisco Express Forwarding がネットワークにインストールされていることを確認します。
- プロバイダー エッジ（PE）デバイスを含む、コア内のすべてのデバイスは、シスコ エクスプレス フォワーディングおよび MPLS 転送をサポートできる必要があります。「MPLS バーチャルプライベート ネットワーク カスタマーのニーズの評価」を参照してください。
- PE デバイスを含む、コア内のすべてのデバイスで Cisco Express Forwarding を有効にします。Cisco Express Forwarding がイネーブルになっているかどうかを確認する方法については、『*Cisco Express Forwarding Configuration Guide*』の「Configuring Basic Cisco Express Forwarding」の章を参照してください。
- デバイスをイネーブルにし、サービスの中断時に LDP バインディングおよび MPLS フォワーディングステートを保護するため、**mpls ldp graceful-restart** コマンドを設定する必要があります。スケール設定を使用した高可用性セットアップでの SSO 中のデバイス障害

を回避するために、（フォワーディングステートを保持しない場合でも）このコマンドを設定することを推奨します。

MPLS バーチャル プライベート ネットワークの制約事項

マルチプロトコル ラベル スイッチング（MPLS）または MPLS バーチャル プライベート ネットワーク（VPN）環境でスタティックルートを設定する場合は、**ip route** コマンドおよび **ip route vrf** コマンドの一部のバリエーションがサポートされません。スタティック ルートを設定するときは、次の注意事項に従ってください。

MPLS 環境でサポートされるスタティック ルート

MPLS 環境でスタティックルートを設定する場合、次の **ip route** コマンドがサポートされます。

- **ip route** *destination-prefix mask interface next-hop-address*

MPLS 環境でスタティックルートを設定し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを設定する場合、次の **ip route** コマンドがサポートされます。

- **ip route** *destination-prefix mask* **interface1 next-hop1**
- **ip route** *destination-prefix mask* **interface2 next-hop2**

TFIB を使用する MPLS 環境でサポートされないスタティック ルート

MPLS 環境でスタティックルートを設定する場合、次の **ip route** コマンドはサポートされません。

- **ip route** *destination-prefix mask next-hop-address*

MPLS 環境でスタティックルートを設定し、2 つのパスでネクストホップに到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route** *destination-prefix mask next-hop-address*

MPLS 環境でスタティックルートを設定し、2 つのネクストホップで宛先に到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route** *destination-prefix mask* **next-hop1**
- **ip route** *destination-prefix mask* **next-hop2**

スタティック ルートを指定する場合は、*interface* an *next-hop* 引数を使用します。

MPLS VPN 環境でサポートされるスタティック ルート

次の **ip route vrf** コマンドは、MPLS VPN 環境でスタティックルートを設定し、ネクストホップとインターフェイスが同じ VRF に存在する場合はサポートされません。

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*

- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**
- **ip route vrf** *vrf-name destination-prefix mask* **interface2 next-hop2**

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがグローバル ルーティング テーブルの MPLS クラウドのグローバルテーブルに存在する場合、次の **ip route vrf** コマンドがサポートされます。たとえば、ネクスト ホップがインターネット ゲートウェイを指している場合は、次のコマンドがサポートされます。

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*（このコマンドは、ネクストホップおよびインターフェイスがコアにある場合にサポートされます）。

MPLS VPN 環境でスタティックルートを設定し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを有効にする場合、次の **ip route** コマンドがサポートされます。

- **ip route** *destination-prefix mask* **interface1 next-hop1**
- **ip route** *destination-prefix mask* **interface2 next-hop2**

TFIB を使用する MPLS VPN 環境でサポートされないスタティック ルート

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがコア内の MPLS クラウドのグローバルテーブルに存在し、2 つのパスでネクストホップに到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route vrf** *destination-prefix mask next-hop-address* **global**

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがコア内の MPLS クラウドのグローバルテーブルに存在し、2 つのネクストホップで宛先に到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route vrf** *destination-prefix mask* **next-hop1 global**
- **ip route vrf** *destination-prefix mask* **next-hop2 global**

次の **ip route vrf** コマンドは、MPLS VPN 環境でスタティックルートを設定し、ネクストホップとインターフェイスが同じ VRF に存在する場合はサポートされません。

- **ip route vrf** *vrf-name destination-prefix mask* **next-hop1** *vrf-name destination-prefix mask* **next-hop1**
- **ip route vrf** *vrf-name destination-prefix mask* **next-hop2**

ネクスト ホップが CE デバイス上のグローバル テーブルに存在する MPLS VPN 環境でサポートされるスタティック ルート

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがカスタマーエッジ（CE）側のグローバルテーブルにある場合、次の **ip route vrf** コマンドがサポートされます。たとえ

ば、外部ボーダーゲートウェイプロトコル（EBGP）マルチホップの場合と同様に、宛先プレフィックスがCEデバイスのループバック アドレスである場合は、次のコマンドがサポートされます。

- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*

MPLS VPN 環境でスタティックルートを設定し、ネクストホップが CE 側のグローバルテーブルに存在し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを有効にする場合、次の **ip route** コマンドがサポートされます。

- **ip route** *destination-prefix mask* **interface1 nexthop1**
- **ip route** *destination-prefix mask* **interface2 nexthop2**

MPLS バーチャル プライベート ネットワークに関する情報

この項では、MPLS バーチャル プライベート ネットワークについて説明します。

MPLS バーチャル プライベート ネットワークの定義

マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク（MPLS VPN）を定義する前に、一般的な VPN を定義する必要があります。VPN の説明を次に示します。

- パブリック インフラストラクチャを介してプライベート ネットワーク サービスを提供する、IP ベースのネットワーク
- インターネットまたはその他のパブリックネットワークやプライベートネットワークを介してプライベートに相互通信できる一連のサイト

通常の VPN は、完全メッシュのトンネル、または相手先固定接続（PVC）を VPN 内のすべてのサイトに設定することで作成されます。このタイプの VPN は、新しいサイトを追加した場合に VPN 内の各エッジ デバイスを変更する必要があるため、維持または拡張が簡単ではありません。

MPLS ベースの VPN は、レイヤ 3 に作成され、ピア モデルに基づきます。ピア モデルによって、サービス プロバイダーおよびカスタマーは、レイヤ 3 のルーティング情報を交換できます。サービス プロバイダーは、カスタマー サイト間でデータをリレーします。このとき、カスタマー側では何をする必要もありません。

MPLS VPN の管理や拡張は、従来の VPN よりも簡単です。新しいサイトが MPLS VPN に追加された場合、更新する必要があるのは、カスタマー サイトにサービスを提供するサービス プロバイダーのエッジ デバイスだけです。

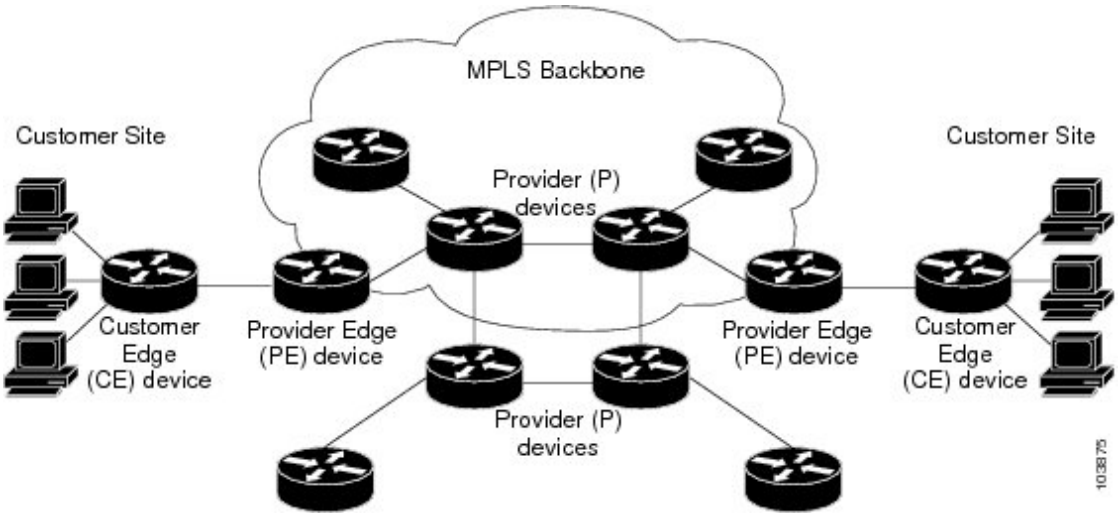
MPLS VPN のさまざまな部分について、次に説明します。

- プロバイダー（P）デバイス：プロバイダー ネットワークのコア内のデバイス。P デバイスは MPLS スイッチングを実行し、ルーティングされるパケットに VPN ラベルを付加しません。各ルートの MPLS ラベルは、プロバイダー エッジ（PE）デバイスによって割り当てられます。VPN ラベルは、データ パケットを正しい出力デバイスに誘導するために使用されます。

- PE デバイス：着信パケットが受信されるインターフェイスまたはサブインターフェイスに基づいて、着信パケットに VPN ラベルを付加するデバイス。PE デバイスは、カスタマー エッジ（CE）デバイスに直接接続されます。
- カスタマー（C）デバイス：ISP または企業ネットワークのデバイス。
- CE デバイス：ネットワーク上の PE デバイスに接続する、ISP のネットワーク上のエッジデバイス。CE デバイスは、PE デバイスとインターフェイスする必要があります。

次の図に、基本的な MPLS VPN を示します。

図 *1 :* 基本的 *MPLS VPN* 用語



MPLS バーチャル プライベート ネットワークの仕組み

マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク（MPLS VPN）機能は、MPLS ネットワークのエッジでイネーブルになっています。プロバイダーエッジ（PE）デバイスは、次の機能を実行します。

- カスタマー エッジ（CE）デバイスとルーティング アップデートを交換する。
- CE ルーティング情報を VPNv4 ルートに変換する。
- マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を介して、他の PE デバイスと VPNv4 ルートを交換する。

ここでは、MPLS VPN の機能について説明します。

MPLS バーチャル プライベート ネットワークの主要コンポーネント

マルチプロトコル ラベル スイッチング（MPLS）ベースのバーチャル プライベート ネットワーク（VPN）には、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN ルート ターゲット コミュニティは、VPN コミュニティのすべてのメンバのリストです。VPN ルート ターゲットは、各 VPN コミュニティ メンバに設定する必要があります。
- VPN コミュニティ プロバイダー エッジ（PE）デバイスのマルチプロトコル BGP（MP-BGP）ピアリング：MP-BGP は、VPN コミュニティのすべてのメンバーに Virtual Route Forwarding（VRF）到達可能性情報を伝播します。MP-BGP ピアリングは、VPN コミュニティのすべての PE デバイスで設定されている必要があります。
- MPLS 転送：MPLS は、VPN サービス プロバイダー ネットワーク上のすべての VPN コミュニティ メンバ間のすべてのトラフィックを転送します。

1 対 1 の関係は、カスタマー サイトと VPNs 間に必ずしも存在する必要はありません。1 つの指定されたサイトを複数の VPN のメンバにできます。ただし、サイトは、1 つの VRF とだけ関連付けることができます。カスタマー サイトの VRF には、そのサイトがメンバとなっている VPN からサイトへの、利用できるすべてのルートが含まれています。

MPLS バーチャル プライベート ネットワークの利点

マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク（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 を展開できます。また、次のような付加価値サービスを提供するための基盤を構築します。

コネクションレス型サービス

MPLS VPN の重要な技術的メリットとして、コネクションレスであることを挙げることができます。インターネットの成功には、TCP/IP という基礎的な技術が貢献しています。TCP/IP は、パケットを基礎とする、コネクションレス ネットワーク パラダイムに基づいて構築されています。これは、ホスト間の通信を確立するための事前のアクションが不要となり、2 者間の通信が簡単になることを意味します。現在の VPN ソリューションでは、コネクションレス型の IP 環境でプライバシーを確立するために、ネットワーク上でコネクション型ポイントツーポイントのオーバーレイを行っています。VPN がコネクションレス型ネットワーク上で動作しても、VPN では接続の容易さや、コネクションレス型ネットワークで利用できる多様なサービスを活用できません。コネクションレス VPN を作成すると、ネットワーク プライバシーのためのトンネルおよび暗号化が不要となり、その結果、複雑さが大幅に軽減されます。

集中型サービス

レイヤ 3 に VPN を構築すると、VPN に代表されるユーザー グループに目的のサービスを配布できます。VPN がサービス プロバイダーに提供する内容は、ユーザーがイントラネット サービスにプライベートに接続するためのメカニズムだけではありません。VPN では、付加価値サービスを対象のカスタマーに柔軟に提供する方法も提供する必要があります。ユーザーがそれぞれのイントラネットやエクストラネットでサービスをプライベートに使用できるようにするためには、拡張性が重要です。MPLS VPN は、プライベート イントラネットと見なされ、次のような新しい IP サービスを使用できます。

- マルチキャスト

- Quality Of Service（QoS）
- VPN でのテレフォニー サポート
- コンテンツや VPN への Web ホスティングを含む、集中型サービス

カスタマーごとに特化したサービスを、複数組み合わせてカスタマイズできます。たとえば、IP マルチキャストを低遅延のサービス クラスに組み合わせると、ビデオ会議をイントラネット内で実施できます。

拡張性

コネクション型ポイントツーポイントのオーバーレイ、フレーム リレー、または ATM 仮想接続（VC）を使用する VPN を作成する場合、その VPN では、主にスケーラビリティが問題となります。特に、カスタマー サイト間での完全メッシュ接続のないコネクション型 VPN は、最適ではありません。MPLS ベースの VPN では、スケーラビリティの高い VPN ソリューションを活用するために、代わりに、ピア モデルとレイヤ 3 コネクションレス型アーキテクチャを使用します。このピア モデルでは、カスタマー サイトがピアリングする必要があるのは、VPN のメンバであるその他のすべてのカスタマー エッジ（CE）デバイスではなく、1 つのプロバイダー エッジ（PE）デバイスだけとなります。コネクションレス型アーキテクチャによって、レイヤ 3 に VPN を作成することができ、トンネルまたは VC を行う必要がなくなります。

MPLS VPN のその他の拡張性の問題は、PE デバイス間の VPN ルートのパーティショニングに起因します。また、コア ネットワークでの PE デバイスとプロバイダー（P）デバイス間での VPN ルートおよび内部ゲートウェイ プロトコル（IGP）ルートのさらなるパーティショニングに起因します。

- PE デバイスは、メンバである VPN に対して VPN ルートを維持する必要があります。
- P デバイスでは、VPN ルートを一切維持する必要がありません。

これにより、プロバイダーのコアのスケーラビリティが高まり、いずれのデバイスもスケーラビリティのボトルネックとなりません。

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。1 つの VPN からのパケットが、間違って別の VPN に送信されることはありません。

セキュリティは、次の領域で提供されます。

- プロバイダーネットワークのエッジでは、お客様から受信したパケットが、正しい VPN に配置されることが保証されます。
- バックボーンでは、VPN トラフィックが常に分離されます。悪意のあるスプーフィング（PE デバイスへのアクセスを取得するための試行）は、ほぼ不可能です。これは、お客様から受信するパケットが IP パケットであるためです。これらの IP パケットは、VPN ラベルと一意に識別され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受信される必要があります。

作成の容易さ

VPN を最大限に活用するには、カスタマーは、新しい VPN とユーザー コミュニティを簡単に作成できる必要があります。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またはトポロジは必要ありません。イントラネットやエクストラネットにサイトを追加して、非公開ユーザー グループを形成できます。この方法で VPN を管理すると、指定された任意のサイトを複数の VPN のメンバにできるため、イントラネットやエクストラネットを構築する場合の柔軟性が最大限に高められます。

柔軟なアドレッシング

VPN サービスへのアクセスをより簡単にするために、サービスプロバイダーのお客様は、独自のアドレッシング計画を設計できます。このアドレッシング計画は、他のサービスプロバイダーのお客様のアドレッシング計画から独立させることができます。RFC 1918 に定義されているとおり、多くのお客様はプライベートアドレス空間を使用します。また、イントラネットの接続性を得るために時間と費用をかけてパブリック IP アドレスに変換することは望んでいません。MPLS VPN を使用すると、お客様は、アドレスのパブリックビューとプライベートビューを提供することで、ネットワークアドレス変換（NAT）を使用することなく現在のアドレス空間を引き続き使用できます。NAT は、重複するアドレス空間を持つ 2 つの VPN が通信する必要がある場合にだけ必要となります。これにより、カスタマーは、パブリック IP ネットワーク上で、独自の未登録プライベート アドレスを使用して自由に通信できます。

統合 QoS サポート

QoS は、多くの IP VPN カスタマーにとって重要な要件です。統合 QoS を使用すると、次の 2 つの基本的な VPN 要件に対処できます。

- 予測可能なパフォーマンスおよびポリシーの実装
- MPLS VPN における複数レベルのサービスのサポート

ネットワークトラフィックは、ネットワークのエッジで分類およびラベル付けされます。トラフィックはその後、加入者によって定義されたポリシーに従って集約され、プロバイダーによって実行されて、プロバイダーコア経由で転送されます。その後、破棄確率または遅延ごとに、ネットワークのエッジおよびコアでのトラフィックを異なるクラスに分けることができます。

直接的な移行

サービス プロバイダーは、VPN サービスを迅速に展開するために、直接的な移行パスを使用します。MPLS VPN の独自な特長として、IP、ATM、フレーム リレー、およびハイブリッド ネットワークを含む、複数のネットワーク アーキテクチャ上に構築できることを挙げることができます。

CE デバイス上で MPLS をサポートする必要がないため、エンドカスタマーの移行作業は簡単になります。お客様のイントラネットを変更する必要はありません。

MPLS バーチャル プライベート ネットワークの設定方法

次の項では、MPLS バーチャル プライベート ネットワークを設定する手順について説明します。

コア ネットワークの設定

次の項では、コアネットワークを設定する手順について説明します。

MPLS バーチャル プライベート ネットワーク カスタマーのニーズの評価

マルチプロトコル ラベル スイッチング仮想プライベート ネットワーク（MPLS VPN）を設定する前に、コア ネットワーク トポロジを識別して、MPLS VPN カスタマーに最適なサービスが提供されるようにする必要があります。コア ネットワーク トポロジを識別するには、次の作業を実行します。

手順の概要

1. ネットワークのサイズを識別します。
2. コアにおけるルーティング プロトコルを識別します。
3. MPLS VPN ハイ アベイラビリティのサポートが必要であるかどうかを判断します。
4. MPLS VPN コアで Border Gateway Protocol（BGP）ロード シェアリングおよび冗長パスが必要であるかどうかを決定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ネットワークのサイズを識別します。	必要となるデバイスとポートの数を決定するために、次の内容を識別します。 • サポートする必要があるカスタマーの数 • カスタマーごとに必要となる VPN の数 • 各 VPN に存在する、仮想ルーティングおよび転送インスタンスの数
ステップ 2	コアにおけるルーティング プロトコルを識別します。	コア ネットワークで必要なルーティング プロトコルを決定します。
ステップ 3	MPLS VPN ハイ アベイラビリティのサポートが必要であるかどうかを判断します。	MPLS VPN ノンストップ フォワーディングおよびグレースフル リスタートは、選択デバイスおよびCisco IOS ソフトウェア リリースでサポートされています。Cisco サポートに問い合わせて、正確な要件およびハードウェア サポートを確認してください。

	コマンドまたはアクション	目的
ステップ 4	MPLS VPN コアで Border Gateway Protocol（BGP）ロードシェアリングおよび冗長パスが必要であるかどうかを決定します。	設定手順については、『*MPLS Layer 3 VPNs Inter-AS and CSC Configuration Guide*』の「Load Sharing MPLS VPN Traffic」モジュールを参照してください。

コアにおける MPLS の設定

コアのすべてのデバイスでマルチプロトコル ラベル スイッチング（MPLS）をイネーブルにするには、ラベル配布プロトコルとして次のいずれかを設定する必要があります。

- MPLS ラベル配布プロトコル（LDP）。設定については、『*MPLS Label Distribution Protocol Configuration Guide*』の「MPLS Label Distribution Protocol (LDP)」モジュールを参照してください。

MPLS バーチャル プライベート ネットワーク カスタマーの接続

次の項では、MPLS バーチャル プライベート ネットワーク カスタマーの接続について説明します。

カスタマーの接続を可能にするための、PE デバイスでの VRF の定義

次の手順を使用して、IPv4 の仮想ルーティングおよび転送（VRF）設定を定義します。IPv4 と IPv6 の VRF を定義するには、MPLS レイヤ 3 VPN コンフィギュレーション ガイド [英語] の「IPv6 VPN over MPLS」モジュールの「Configuring a Virtual Routing and Forwarding Instance for IPv6」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** *ipv4* | *ipv6*
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit**

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	バーチャルプライベートネットワーク（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、Virtual Routing and Forwarding（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： `Device(config-vrf)# rd 100:1`	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* 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。ルート識別子（RD）は、次のいずれかの形式で入力できます。 • 16 ビットの AS 番号：32 ビットの番号。101:3 など。 • 32 ビットの IP アドレス：16 ビットの番号。10.0.0.1:1 など。
ステップ 5	**address-family** *ipv4* | *ipv6* 例： `Device(config-vrf)# address-family ipv6`	IPv4 または IPv6 アドレスファミリモードを開始します。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf-af)# route-target both 100:1`	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。 • **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。 • **both** キーワードを使用すると、ターゲット VPN 拡張コミュニティとの間でルーティング情報がインポートおよび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、インポートやエクスポートの route-target 拡張コミュニティの VRF リストに追加されます。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	（任意）終了して、グローバル コンフィギュレーション モードに戻ります。

各 VPN カスタマー用の PE デバイスでの VRF インターフェイスの設定

プロバイダー エッジ（PE）デバイス上のインターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送（VRF）インスタンスを関連付けるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル 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** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	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。 • *type* 引数で、設定するインターフェイスのタイプを指定します。 • *number* 引数には、ポート、コネクタ、またはインターフェイス カード番号を指定します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding vrf1`	指定したインターフェイスまたはサブインターフェイスに VRF を関連付けます。 • vrf-name 引数は、VRF に割り当てる名前です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）終了して、特権 EXEC モードに戻ります。

PE デバイスと CE デバイス間でのルーティング プロトコルの設定

カスタマー エッジ（CE）デバイスで使用されているのと同じルーティング プロトコルを使用して、プロバイダー エッジ（PE）デバイスを設定します。ボーダー ゲートウェイ プロトコル（BGP）、Routing Information Protocol バージョン 2（RIPv2）、EIGRP、Open Shortest Path First（OSPF）、または PE デバイスと CE デバイス間のスタティックルートを設定できます。

バーチャル プライベート ネットワークの設定の確認

ルート識別子は、Virtual Route Forwarding（VRF）インスタンス用に設定する必要があります。マルチプロトコル ラベル スイッチング（MPLS）は、VRF を伝送するインターフェイスで設定する必要があります。**show ip vrf** コマンドを使用して、VRF 用に設定されているルート識別子（RD）とインターフェイスを確認します。

手順の概要

1. **show ip vrf**

手順の詳細

show ip vrf

一連の定義済み VRF インスタンスおよび関連付けられているインターフェイスを表示します。また、この出力では、VRF インスタンスが設定済みルート識別子にマップされます。

MPLS バーチャル プライベート ネットワーク サイト間の接続の確認

ローカルおよびリモートのカスタマー エッジ（CE）デバイスがマルチプロトコル ラベル スイッチング（MPLS）コアを介して通信できることを確認するには、次の作業を実行します。

MPLS コアを介した CE デバイスから CE デバイスへの IP 接続の確認

手順の概要

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

ステップ 2 **ping** [*protocol*] {*host-name* | *system-address*}

AppleTalk、コネクションレス型モード ネットワーク サービス（CLNS）、IP、Novell、Apollo、Virtual Integrated Network Service（VINES）、DECnet、または Xerox Network Service（XNS）ネットワークでの基本的なネットワーク接続を診断します。**ping** コマンドを使用して、CE デバイス間の接続を確認します。

ステップ 3 **trace** [*protocol*] [*destination*]

パケットがその宛先に送信されるときに取るルートを検出します。**trace** コマンドは、2 つのデバイスが通信できない場合に問題の箇所を分離するのに役立ちます。

ステップ 4 **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

ルーティング テーブルの現在の状態を表示します。*ip-address* 引数を使用して、CE1 に CE2 へのルートが含まれていることを確認します。CE1 から学習したルートを確認します。CE2 へのルートがリストされていることを確認します。

ローカル CE デバイスとリモート CE デバイスが PE ルーティング テーブルに存在することの確認

手順の概要

1. **enable**
2. **show ip route vrf** *vrf-name* [*prefix*]
3. **show ip cef vrf** *vrf-name* [*ip-prefix*]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

ステップ 2 **show ip route vrf** *vrf-name* [*prefix*]

Virtual Route Forwarding（VRF）インスタンスに関連付けられている IP ルーティングテーブルを表示します。ローカル カスタマー エッジ（CE）デバイスとリモート カスタマー エッジ（CE）デバイスのループバック アドレスが、プロバイダー エッジ（PE）でデバイスのルーティング テーブルに存在することを確認します。

ステップ 3 **show ip cef vrf** *vrf-name* [*ip-prefix*]

VRF に関連付けられている Cisco Express Forwarding 転送テーブルを表示します。次のように、リモート CE デバイスのプレフィックスが、シスコ エクスプレス フォワーディング テーブルに存在することを確認します。

MPLS バーチャル プライベート ネットワーク（VPN）の設定例

次の項では、MPLS バーチャル プライベート ネットワークを設定する手順について説明します。

例：RIP を使用した MPLS バーチャル プライベート ネットワークの設定

PE の設定	CE の設定
vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface GigabitEthernet 1/0/1 vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable interface GigabitEthernet 1/0/1 ip address 192.0.2.2 255.255.255.0 mpls label protocol ldp mpls ip ! router rip version 2 timers basic 30 60 60 120 ! address-family ipv4 vrf vpn1 version 2 redistribute bgp 100 metric transparent network 192.0.2.0 distribute-list 20 in no auto-summary exit-address-family ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute rip no auto-summary no synchronization exit-address-family	ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface GigabitEthernet 1/0/1 ip address 192.0.2.1 255.255.255.0 no cdp enable router rip version 2 timers basic 30 60 60 120 redistribute connected network 10.0.0.0 network 192.0.2.0 no auto-summary

例：スタティック ルートを使用した MPLS バーチャル プライベート ネットワークの設定

PE の設定	CE の設定
vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface GigabitEthernet 1/0/1 vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable ! interface GigabitEthernet 1/0/1 ip address 192.168.0.1 255.255.0.0 mpls label protocol ldp mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 192.168.0.0 255.255.0.0 area 100 ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute static no auto-summary no synchronization exit-address-family ! ip route vrf vpn1 10.0.0.9 255.255.255.255 192.0.2.2 ip route vrf vpn1 192.0.2.0 255.255.0.0 192.0.2.2	ip cef ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface GigabitEthernet 1/0/1 ip address 192.0.2.2 255.255.0.0 no cdp enable ! ip route 10.0.0.9 255.255.255.255 192.0.2.3 3 ip route 198.51.100.0 255.255.255.0 192.0.2.3 3

例：BGP を使用した MPLS バーチャル プライベート ネットワークの設定

PE の設定	CE の設定
	router bgp 5000 bgp log-neighbor-changes neighbor 5.5.5.6 remote-as 5001 neighbor 5.5.5.6 ebgp-multihop 2 neighbor 5.5.5.6 update-source Loopback5 neighbor 35.2.2.2 remote-as 5001 neighbor 35.2.2.2 ebgp-multihop 2 neighbor 35.2.2.2 update-source Loopback1 neighbor 3500::1 remote-as 5001 neighbor 3500::1 ebgp-multihop 2 neighbor 3500::1 update-source Loopback1 ! address-family ipv4 redistribute connected neighbor 5.5.5.6 activate neighbor 35.2.2.2 activate no neighbor 3500::1 activate exit-address-family ! address-family ipv6 redistribute connected neighbor 3500::1 activate exit-address-family Device-RP(config)#

PE の設定	CE の設定

router bgp 5001
bgp log-neighbor-changes
bgp graceful-restart
bgp sso route-refresh-enable
bgp refresh max-eor-time 600
redistribute connected
neighbor 102.1.1.1 remote-as 5001
neighbor 102.1.1.1 update-source Loopback1
neighbor 105.1.1.1 remote-as 5001
neighbor 105.1.1.1 update-source Loopback10
neighbor 160.1.1.2 remote-as 5002
!
address-family vpnv4
  neighbor 102.1.1.1 activate
  neighbor 102.1.1.1 send-community both
  neighbor 105.1.1.1 activate
  neighbor 105.1.1.1 send-community extended
exit-address-family
!
address-family vpnv6
  neighbor 102.1.1.1 activate
  neighbor 102.1.1.1 send-community extended
 	
  neighbor 105.1.1.1 activate
  neighbor 105.1.1.1 send-community extended
exit-address-family
!
address-family ipv4 vrf full
  redistribute connected
  neighbor 20.1.1.1 remote-as 5000
  neighbor 20.1.1.1 ebgp-multihop 2
  neighbor 20.1.1.1 update-source Loopback2
  neighbor 20.1.1.1 activate
  neighbor 20.1.1.1 send-community both
exit-address-family
!
address-family ipv6 vrf full
  redistribute connected
  neighbor 2000::1 remote-as 5000
  neighbor 2000::1 ebgp-multihop 2
  neighbor 2000::1 update-source Loopback2
  neighbor 2000::1 activate
exit-address-family
!
address-family ipv4 vrf orange
  network 87.1.0.0 mask 255.255.252.0
  network 87.1.1.0 mask 255.255.255.0
  redistribute connected
  neighbor 40.1.1.1 remote-as 7000
  neighbor 40.1.1.1 ebgp-multihop 2
  neighbor 40.1.1.1 update-source Loopback3
  neighbor 40.1.1.1 activate
  neighbor 40.1.1.1 send-community extended
  neighbor 40.1.1.1 route-map orange-lp in
  maximum-paths eibgp 2
exit-address-family
!
address-family ipv6 vrf orange
  redistribute connected
  maximum-paths eibgp 2
  neighbor 4000::1 remote-as 7000
  neighbor 4000::1 ebgp-multihop 2	

PE の設定	CE の設定
neighbor 4000::1 update-source Loopback3 neighbor 4000::1 activate exit-address-family ! address-family ipv4 vrf sona redistribute connected neighbor 160.1.1.2 remote-as 5002 neighbor 160.1.1.2 activate neighbor 160.1.1.4 remote-as 5003 neighbor 160.1.1.4 activate exit-address-family	

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「MPLS コマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*
Cisco Express Forwarding の設定	『*Cisco Express Forwarding Configuration Guide*』の「Configuring Basic Cisco Express Forwarding」モジュール
LDP の設定	『*MPLS Label Distribution Protocol Configuration Guide*』の「MPLS Label Distribution Protocol (LDP)」モジュール

MPLS バーチャル プライベート ネットワークの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	MPLS バーチャル プライベート ネットワーク	MPLS バーチャル プライベート ネットワーク（VPN）は、マルチプロトコル ラベル スイッチング（MPLS）プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1 つ以上のカスタマーエッジ（CE）デバイスが、1 つ以上のプロバイダー エッジ（PE）デバイスに接続されます。
Cisco IOS XE Gibraltar 16.11.1	MPLS レイヤ 3 VPN の BGP PE-CE サポート	プロバイダーエッジ（PE）デバイスとカスタマーエッジ（CE）デバイス間のルーティングプロトコルとしての BGP のサポートが導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、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。