MPLS レイヤ 3 VPN Inter-AS および CSC コンフィギュレーション ガイド

初版：2012 年 11 月 05 日

最終更新：2013 年 03 月 29 日

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/

【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。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

強力な Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースは、コンバージド リリース バージョンとして Cisco IOS XE 16 にマージされました。Cisco IOS XE 16 は、スイッチングおよびルーティング ポートフォリオの幅広いアクセス範囲とエッジ製品を網羅する単一のリリースとなります。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディングページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS

自律システム境界ルータ（ASBR）で VPN-IPv4 アドレスを交換するマルチプロトコル ラベル スイッチング（MPLS）VPN Inter-AS 機能により、MPLS VPN はサービス プロバイダーと自律システムにまたがることができます。このモジュールでは、ASBR が外部 Border Gateway Protocol（EBGP）を使用して IPv4 ネットワーク層到達可能性情報（NLRI）を VPN-IPv4 アドレスの形式で交換できるようにします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の前提条件

- マルチプロトコル ラベル スイッチング（MPLS）VPN 内の自律システムまたはサブ自律システム間に外部 Border Gateway Protocol（EBGP）ルーティングを設定する前に、すべての MPLS VPN ルーティング インスタンスおよびセッションを適切に設定しておく必要があります。この項で説明する設定作業は、次の設定作業からなります。「Configuring MPLS Layer 3 VPNs」モジュールの説明に従って次の作業を実行します。
  - VPN ルーティング インスタンスの定義
  - MPLS コアにおける BGP ルーティング セッションの設定
  - MPLS コアにおけるプロバイダー エッジ間（PE-to-PE）ルーティング セッションの設定
  - BGP のプロバイダー エッジからカスタマー エッジ（PE-to-CE）へのルーティング セッションの設定
  - 直接接続された自律システム境界ルータ（ASBR）間の VPN-IPv4 EBGP セッションの設定

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の制約事項

マルチホップ VPN-IPv4 外部 Border Gateway Protocol（EBGP）はサポートされていません。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS に関する情報

MPLS VPN Inter-AS の概要

自律システムとは、共通のシステム管理グループによって管理され、単一の明確に定義されたルーティング プロトコルを使用する、単一のネットワークまたはネットワークのグループのことです。

VPN が大規模になるにつれて、その要件も多くなります。場合によっては、VPN が異なる地理的エリアの異なる自律システムに存在する必要があります。また、一部の VPN は、複数のサービス プロバイダーにまたがって設定する必要があります（オーバーラッピング VPN）。VPN がどのよ

うに複雑で、どのような場所にあっても、自律システム間の接続はカスタマーに対してシームレスである必要があります。

MPLS VPN Inter-AS の利点

マルチプロトコル ラベル スイッチング（MPLS）VPN Inter-AS には次の利点があります。

- VPN が複数のサービス プロバイダー バックボーンをカバーできる：異なる自律システムを実行する複数のサービス プロバイダーが、共同で同じカスタマーに MPLS VPN サービスを提供できます。あるカスタマー サイトから開始し、さまざまな VPN サービス プロバイダー バックボーンを通過して、同じカスタマーの別のサイトに到達するように VPN を設定できます。以前は、MPLS VPN は、単一の Border Gateway Protocol（BGP）自律システム サービス プロバイダー バックボーンのみを通過できました。この機能により、複数の自律システムが、サービスプロバイダーのカスタマー サイト間に連続性がありシームレスなネットワークを形成できます。

- VPN を異なるエリアに作成できる：サービス プロバイダーは、異なる地理的エリアに VPN を作成できます。すべての VPN トラフィック フローを（エリア間で）1 箇所のポイントを通過させるようにすると、エリア間のネットワーク トラフィックのレートをより適切に制御できます。

- 連合により内部ボーダー ゲートウェイ プロトコル（IBGP）メッシングを最適化できる：自律システム内の内部ボーダー ゲートウェイ プロトコル（iBGP）メッシングがより整理され、管理しやすくなります。自律システムを複数の異なるサブ自律システムに分割して、それらを単一の連合に分類できます（ただし、VPN バックボーン全体は単一の自律システムと見なされます）。連合を形成するサブ自律システム間でのラベル付き VPN-IPv4 ネットワーク層到達可能性情報（NLRI）の交換がサポートされているため、サービス プロバイダーはこの機能を使用して、連合全体で MPLS VPN を提供できます。

ASBR で VPN-IPv4 アドレスを交換する Inter-AS の使用

異なるサービス プロバイダーの異なる自律システムは、VPN-IPv4 アドレスの形式で IPv4 ネットワーク層到達可能性情報（NLRI）を交換することによって通信できます。自律システム境界ルータ（ASBR）はネットワーク到達可能性情報を交換するために外部 Border Gateway Protocol（EBGP）を使用します。その後、Interior Gateway Protocol（IGP）によって、各 VPN および各自律システム全体に、VPN-IPv4 プレフィックスのネットワーク層情報が配布されます。ルーティング情報では、次のプロトコルが使用されます。

- 自律システム内では、ルーティング情報は IGP を使用して共有されます。
- 自律システム間では、ルーティング情報は EBGP を使用して共有されます。EBGP を使用して、サービス プロバイダーは別個の自律システム間でルーティング情報をループ フリーで交換することを保証するドメイン間ルーティング システムを設定することができます。

EBGP の主な機能は、自律システムのルートのリストに関する情報を含む、自律システム間のネットワーク到達可能性情報を交換することです。自律システムは、EBGP ボーダー エッジ デバイスを使用してラベル スイッチング情報を含むルートを配布します。各ボーダー エッジ デバイスでは、ネクスト ホップおよびラベルが書き換えられます。詳細については、ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS における情報交換, （6 ページ）を参照してください。

MPLS VPN でサポートされている相互自律システム設定は次のとおりです。

- **プロバイダー間 VPN**：異なるボーダー エッジ デバイスによって接続された、2 つ以上の自律システムを含む MPLS VPN。各自律システムは、EBGP を使用してルートを交換します。自律システム間では、IGP 情報（ルーティング情報）は交換されません。
- **BGP 連合**：単一の自律システムを複数のサブ自律システムに分割してから、指定された単一の連合として分類した MPLS VPN。ネットワークでは、連合は単一の自律システムとして認識されます。異なる自律システム内のピアは、EBGP セッションを介して通信しますが、これらのピアは IBGP ピアである場合と同様にルート情報を交換できます。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS における情報交換

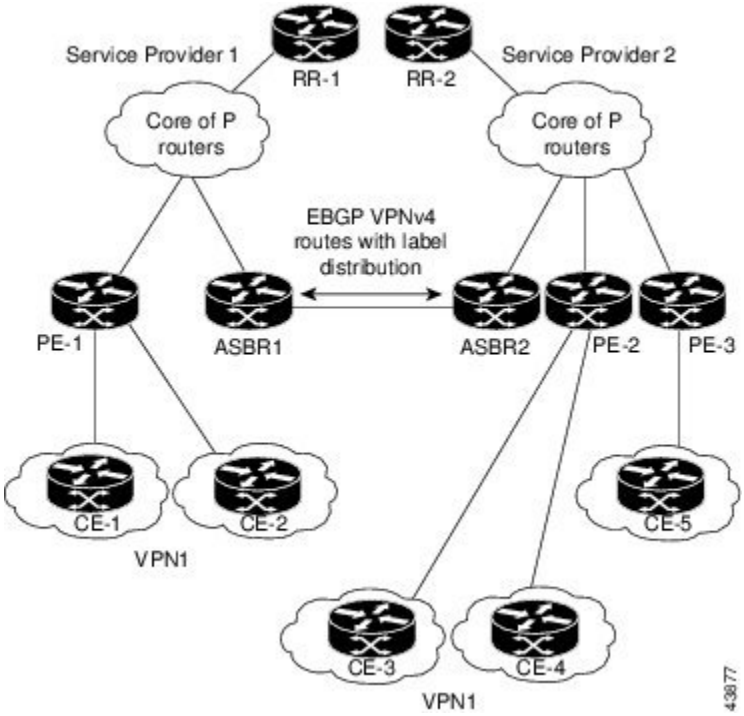
ここでは、次の内容について説明します。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS における情報の伝送

次の図に、2 つの異なる自律システムから構成された 1 つのマルチプロトコル ラベル スイッチング（MPLS）VPN を示します。各自律システムは異なる管理制御下で運用され、異なる内部ゲートウェイ プロトコル（IGP）が実行されています。サービス プロバイダーは、外部 Border Gateway

Protocol（EBGP）ボーダーエッジデバイス（ASBR1、ASBR2）を経由してルーティング情報を交換します。

図 *1*：*ASBR* で *VPN-IPv4* アドレスを交換する *2* つの *MPLS VPN Inter-AS* システム間の *EBGP* 接続



この設定では、次のプロセスによって情報が送信されます。

手順の概要

1. プロバイダー エッジ デバイス（PE-1）では、ルートを配布する前に、そのルートに対してラベルが割り当てられます。PE デバイスは、ボーダー ゲートウェイ プロトコル（BGP）のマルチプロトコル拡張を使用して、ラベルマッピング情報を送信します。PEデバイスは、VPN-IPv4 アドレスとしてルートを配布します。アドレス ラベルおよび VPN 識別子は、IPv4 ネットワーク層到達可能性情報（NLRI）の一部として符号化されます。
2. 2 つのルート リフレクタ（RR-1 と RR-2）には、自律システム内の VPN-IPv4 内部ルートが反映されます。自律システムのボーダー エッジ デバイス（ASBR1 と ASBR2）は、VPN-IPv4 外部ルートをアドバタイズします。
3. EBGP ボーダー エッジ デバイス（ASBR1）によって、次の自律システム（ASBR2）にルートが再配布されます。ASBR1 は、EBGP のネクストホップ属性の値として自身のアドレスを指定し、新しいラベルを割り当てます。このアドレスでは、次のことが保証されます。
4. EBGP ボーダー エッジ デバイス（ASBR2）では、設定に応じて、次のいずれかの方法でルートが再配布されます。

手順の詳細

ステップ 1 プロバイダー エッジ デバイス（PE-1）では、ルートを配布する前に、そのルートに対してラベルが割り当てられます。PE デバイスは、ボーダー ゲートウェイ プロトコル（BGP）のマルチプロトコル拡張を使用して、ラベルマッピング情報を送信します。PE デバイスは、VPN-IPv4 アドレスとしてルートを配布します。アドレス ラベルおよび VPN 識別子は、IPv4 ネットワーク層到達可能性情報（NLRI）の一部として符号化されます。

ステップ 2 2 つのルート リフレクタ（RR-1 と RR-2）には、自律システム内の VPN-IPv4 内部ルートが反映されます。自律システムのボーダー エッジ デバイス（ASBR1 と ASBR2）は、VPN-IPv4 外部ルートをアドバタイズします。

ステップ 3 EBGP ボーダー エッジ デバイス（ASBR1）によって、次の自律システム（ASBR2）にルートが再配布されます。ASBR1 は、EBGP のネクストホップ属性の値として自身のアドレスを指定し、新しいラベルを割り当てます。このアドレスでは、次のことが保証されます。

- ネクストホップ デバイスが、サービス プロバイダー（P）バックボーン ネットワーク内で常に到達可能であること。
- 配布元デバイスによって割り当てられたラベルが適切に解釈されること。（ルートに関連付けられるラベルは、対応するネクストホップ デバイスによって割り当てられる必要があります）。

ステップ 4 EBGP ボーダー エッジ デバイス（ASBR2）では、設定に応じて、次のいずれかの方法でルートが再配布されます。

- IBGP ネイバーが **neighbor next-hop-self** コマンドを使用して設定されている場合、ASBR2 は、EBGP ピアから受信したアップデートのネクストホップ アドレスを変更して転送します。
- IBGP ネイバーが **neighbor next-hop-self** コマンドを使用して設定されていない場合、ネクストホップ アドレスは変更されません。ASBR2 は、EBGP ピアのホスト ルートを IGP 経由で伝播する必要があります。EBGP VPN-IPv4 ネイバー ホスト ルートを伝播するには、**redistribute connected subnets** コマンドを使用します。EBGP VPN-IPv4 ネイバー ホスト ルートは、ネイバーがアップ状態になったときにルーティング テーブルに自動的にインストールされます。このことは、異なる自律システム内の PE デバイス間でラベル スイッチド パスを確立するために重要です。

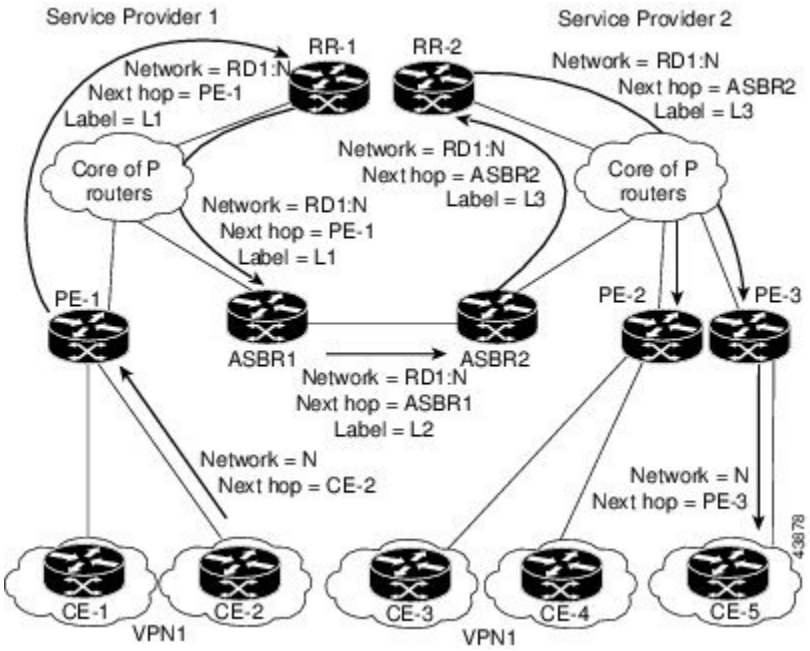
ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS における VPN ルーティング情報の交換

自律システムは、接続を確立するために VPN ルーティング情報（ルートとラベル）を交換します。自律システム間の接続を制御するために、プロバイダー エッジ（PE）デバイスおよび外部 Border Gateway Protocol（EBGP）ボーダー エッジ デバイスはラベル転送情報ベース（LFIB）を保持します。LFIB では、VPN 情報の交換中に PE デバイスおよび EBGP ボーダー エッジ デバイスが受信するラベルとルートが管理されます。

次の図に、自律システム間におけるVPNのルートおよびラベル情報の交換について示します。自律システムでは、VPN ルーティング情報を交換する場合に次の条件が使用されます。

- ルーティング情報に次の内容が含まれています。
  - 宛先ネットワーク（N）
  - 配布元デバイスに関連付けられたネクストホップ フィールド
  - ローカル MPLS ラベル（L）
- RD1: ルート識別子が宛先ネットワーク アドレスの一部として含まれています。ルート識別子によって、VPN-IPv4 ルートが VPN サービス プロバイダー環境内でグローバルに一意となります。
- 自律システム境界ルータ（ASBR）は、内部ボーダー ゲートウェイ プロトコル（IBGP）ネイバーに VPN-IPv4 ネットワーク層到達可能性情報（NLRI）を送信する場合に、ネクストホップ（next-hop-self）を変更するように設定されています。したがって、ASBR では、IBGP ネイバーに NLRI を転送する場合に新しいラベルを割り当てる必要があります。

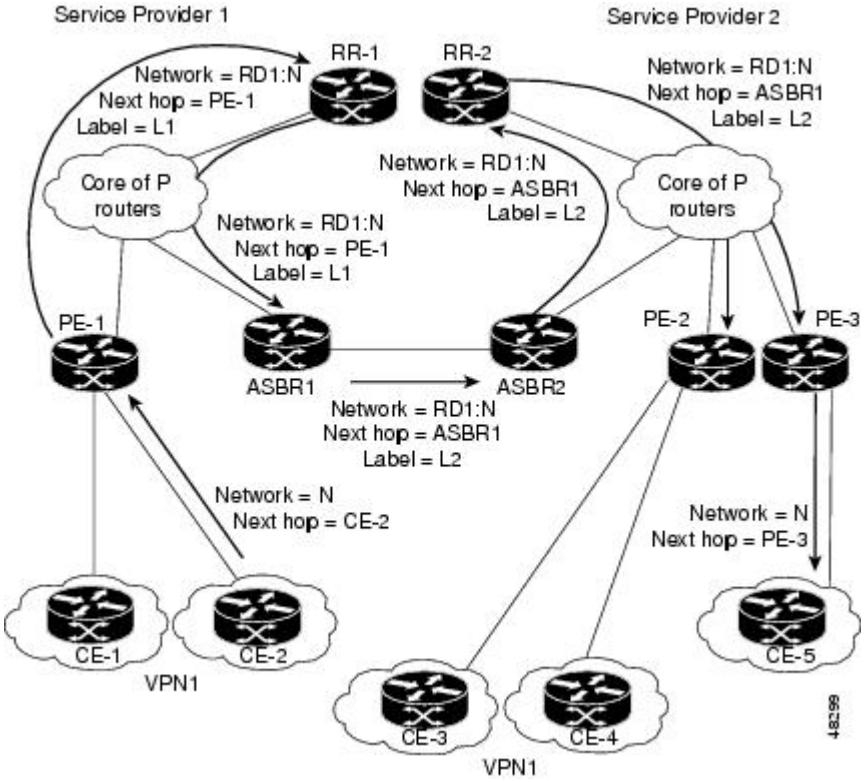
図 *2*：*ASBR* で *VPN-IPv4* アドレスを交換する *MPLS VPN Inter-AS* システム間でのルートとラベルの交換



次の図に、自律システム間におけるVPNのルートおよびラベル情報の交換について示します。唯一の違いは、ASBR2 が **redistribute connected** コマンドを使用して設定されていることです。これ

により、ホスト ルートがすべての PE に伝播されます。ASBR2 はネクストホップ アドレスを変更するように設定されていないため、**redistribute connected** コマンドが必要となります。

図 *3* : ***ASBR*** で ***VPN-IPv4*** アドレスを交換する ***MPLS VPN Inter-AS*** における、***redistribute connected*** コマンドを使用したルートとラベルの交換



ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS システム間のパケット転送

次の図に、プロバイダー間ネットワークにおいて、次のパケット転送方法を使用して自律システム間でパケットが転送されるようすを示します。

パケットは、マルチプロトコル ラベル スイッチング（MPLS）によって宛先に転送されます。パケットでは、各プロバイダー エッジ（PE）デバイスおよび外部 Border Gateway Protocol（EBGP）ボーダーエッジデバイスのラベル転送情報ベース（LFIB）に格納されているルーティング情報が使用されます。

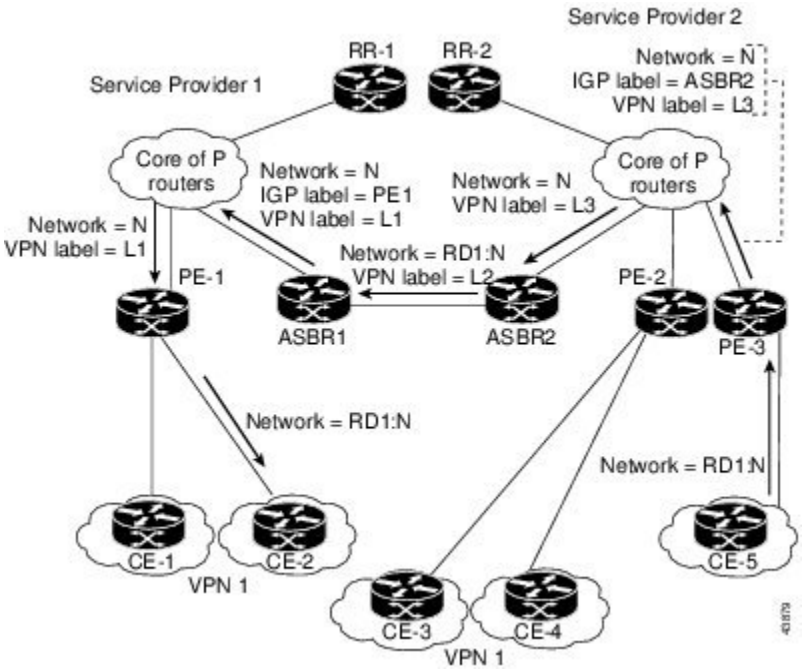
サービス プロバイダー VPN バックボーンはラベルを転送するためにダイナミック ラベル スイッチングを使用します。

各自律システムでは、標準的なマルチレベル ラベリングを使用して、自律システム デバイスのエッジ間（CE-5 から PE-3 など）でパケットが転送されます。自律システム間では、アドバタイズされたルートに対応する単一レベルのラベリングのみが使用されます。

データ パケットが VPN バックボーンを通過する場合、2 つのレベルのラベルが伝送されます。

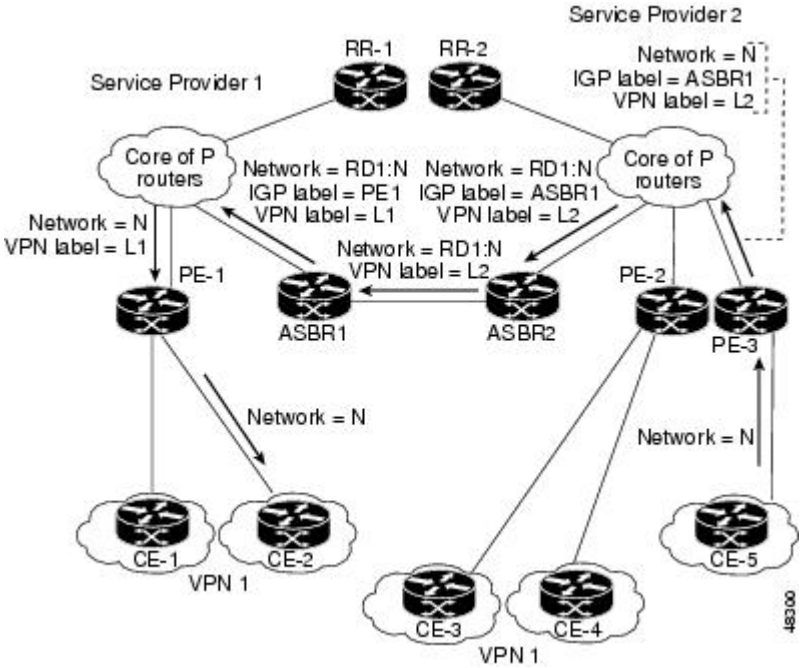
- 最初のラベル（IGP ルート ラベル）によって、パケットが正しい PE デバイスまたは EBGP ボーダー エッジ デバイスに転送されます（たとえば、ASBR2 の内部ゲートウェイ プロトコル（IGP）ラベルは ASBR2 ボーダー エッジ デバイスを指します）。
- 2 番目のラベル（VPN ルート ラベル）によって、パケットが適切な PE デバイスまたは EBGP ボーダー エッジ デバイスに転送されます。

図 *4*：*ASBR* で *VPN-IPv4* アドレスを交換する *MPLS VPN Inter-AS* システム間のパケット転送



次の図に、上記の図と同じパケット転送方法を示します。ただし、今回は、EBGP デバイス（ASBR1）で新しいラベルが再割り当てされずにパケットが転送されます。

図 *5*：*ASBR* で *VPN-IPv4* アドレスを交換する *MPLS VPN Inter-AS* システム間での新しいラベルを割り当てないパケット転送



ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS における連合の使用

連合とは、複数のサブ自律システムをグループ化したものです。連合を使用することによって、自律システム内のピア デバイスの合計数を減らすことができます。連合では、自律システムが複数のサブ自律システムに分割され、自律システムに連合識別子が割り当てられます。VPN は、異なる自律システムまたは連合を形成する複数のサブ自律システムで実行される、複数のサービス プロバイダーにまたがることができます。

連合において、各サブ自律システムと他のサブ自律システムとの関係は、フル メッシュになっています。サブ自律システム間の通信は、Open Shortest Path First（OSPF）や Intermediate System-to-Intermediate System（IS-IS）などの内部ゲートウェイ プロトコル（IGP）を使用して行われます。また、各サブ自律システムには、他のサブ自律システムへの外部 Border Gateway Protocol（EBGP）接続もあります。連合 EBGP（CEBGP）ボーダー エッジ デバイスは、指定されたサブ自律システム間で next-hop-self アドレスを転送します。next-hop-self アドレスによって、Border Gateway Protocol（BGP）では、プロトコルでネクスト ホップを選択するのではなく、ネクスト ホップとして指定されたアドレスを使用することが強制されます。

次の 2 つの方法のいずれかを使用して、異なるサブ自律システムに連合を設定できます。

- next-hop-self アドレスが CEBGP ボーダー エッジ デバイス間でのみ転送されるようにデバイスを設定できます（双方向）。サブ自律システム ボーダーのサブ自律システム（IBGP ピア）

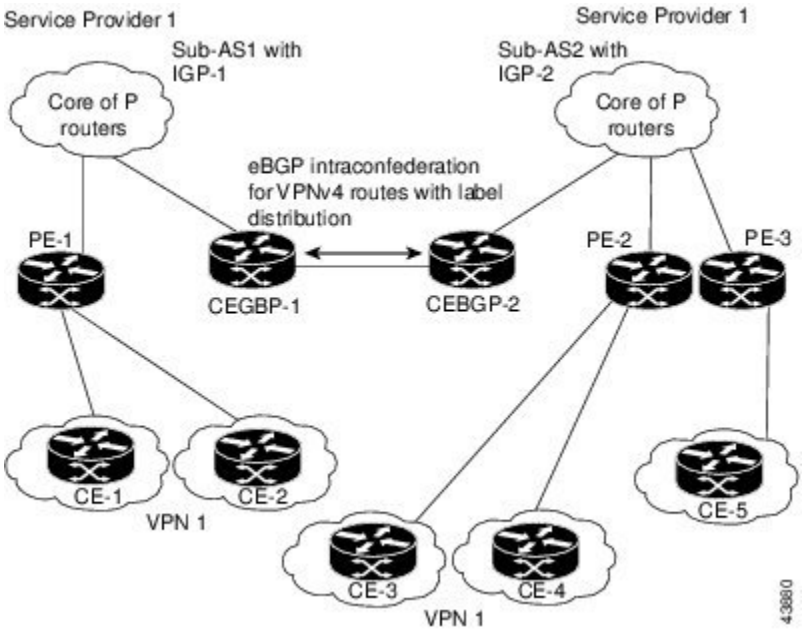
では、next-hop-self アドレスは転送されません。各サブ自律システムは、単一の IGP ドメインとして実行されます。ただし、CEBGP ボーダー エッジ デバイス アドレスは、IGP ドメイン内で認識されます。

- next-hop-self アドレスが CEBGP ボーダー エッジ デバイス間（双方向）、およびサブ自律システム ボーダーの IBGP ピア内で転送されるようにデバイスを設定できます。各サブ自律システムは、単一の IGP ドメインとして実行されますが、ドメイン内の PE デバイス間で next-hop-self アドレスの転送もします。CEBGP ボーダー エッジ デバイス アドレスは、IGP ドメイン内で認識されます。

次の図に、一般的な MPLS VPN 連合設定を示します。この連合設定の特徴は次のとおりです。

- 2 つの CEBGP ボーダー エッジ デバイスは、2 つのサブ自律システム間で VPN-IPv4 アドレスおよびラベルを交換します。
- 配布元デバイスはネクスト ホップ アドレスおよびラベルを変更して、next-hop-self アドレスを使用します。
- IGP-1 および IGP-2 では、CEBGP-1 と CEBGP-2 のアドレスが認識されます。

図 *6*：連合内の *2* つのサブ自律システム間の *EBGP* 接続



この連合設定の特徴は次のとおりです。

- CEBGP ボーダー エッジ デバイスは、サブ自律システム間の隣接ピアとして機能します。サブ自律システムは、EBGP を使用してルート情報を交換します。
- 各 CEBGP ボーダーエッジデバイス（CEBGP-1、CEBGP-2）は、ルートを次のサブ自律システムに配布する前に、ルートのラベルを割り当てます。CEBGP ボーダーエッジデバイスは、BGP のマルチプロトコル拡張を使用して、VPN-IPv4 アドレスとしてルートを配布します。

ラベルおよび VPN 識別子は、IPv4 ネットワーク層到達可能性情報（NLRI）の一部として符号化されます。

- 各プロバイダー エッジ（PE）および CEBGP ボーダー エッジ デバイスは、ルートを再配布する前に、各 VPN-IPv4 アドレス プレフィックスに独自のラベルを割り当てます。CEBGP ボーダー エッジ デバイスは、ラベル付きの VPN-IPv4 アドレスを交換します。ラベルには、（EBGP ネクストホップ属性の値として）next-hop-self アドレスが含まれています。サブ自律システム内では、CEBGP ボーダー エッジ デバイス アドレスが IBGP ネイバー全体に配布され、2 つの CEBGP ボーダー エッジ デバイスが両方の連合で認識されます。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の設定方法

VPN-IPv4 アドレスを交換するように ASBR を設定する

他の自律システムと VPN-IPv4 ルートを交換するように外部ボーダー ゲートウェイ プロトコル（EBGP）自律システム境界ルータ（ASBR）を設定するには、次の作業を実行します。

（注） VPN-IPv4 EBGP ネイバーのホスト ルートを他のデバイスおよびプロバイダー エッジ デバイスに伝播するには、デバイスの内部ゲートウェイ プロトコル（IGP）設定部分で **redistribute connected subnets** コマンドを発行します。内部ボーダー ゲートウェイ プロトコル（IBGP）ネイバーを設定するときに next-hop-self アドレスを指定することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **no bgp default route-target filter**
5. **address-family vpnv4** [**unicast**]
6. **neighbor***peer-group-name***remote-as***as-number*
7. **neighbor***peer-group-name***activate**
8. **exit-address-family**
9. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 1`	EBGP ルーティング プロセスを作成して、それに自律システム番号を割り当てます。 • 自律システム番号は、他の自律システムの EBGP デバイスでデバイスを識別できるようにするために渡されます。
ステップ 4	**no bgp default route-target filter** 例： `Device(config)# no bgp default route-target filter`	BGP の route-target フィルタリングを無効にし、デバイスでコンフィギュレーション モードを開始します。 • 受信したすべての BGP VPN-IPv4 ルートがデバイスによって受け入れられます。
ステップ 5	**address-family vpnv4** [**unicast**] 例： `Device(config-router)# address-family vpnv4`	VPN バックボーン全体で VPNv4 アドレスを伝送するルーティング セッションを設定し、デバイスをアドレス ファミリ コンフィギュレーション モードに設定します。 • 8 バイトのルート識別子（RD）を追加することによって、各アドレスはグローバルに一意になります。 • unicast キーワードによって、ユニキャスト プレフィックスが指定されます。
ステップ 6	**neighbor***peer-group-name***remote-as***as-number* 例： `Device(config-router-af)# neighbor 1 remote-as 2`	アドレス ファミリ コンフィギュレーション モードを開始して、隣接 EBGP ピア グループを指定します。 • この EBGP ピア グループは、指定した自律システムに属すると見なされます。

	コマンドまたはアクション	目的
ステップ 7	**neighbor***peer-group-name***activate** 例： `Device(config-router-af)# neighbor 1 activate`	ネイバー EBGP デバイスへの VPNv4 アドレス ファミリのアドバタイズメントをアクティブにします。
ステップ 8	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	ルータ コンフィギュレーション モードのアドレス ファミリ サブモードを終了します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

連合内のサブ自律システム間で VPN ルートを交換する EBGP ルーティングの設定

連合内のサブ自律システム間で VPN ルートを交換する EBGP ルーティングを設定するには、次の作業を実行します。

（注） VPN-IPv4 EBGP ネイバーのホストルートが（IGP によって）他のデバイスおよびプロバイダーエッジデバイスに伝播されるようにするには、CEBGP デバイスの IGP 設定部分で **redistribute connected** コマンドを指定します。OSPF を使用している場合は、「redistribute connected」サブネットが存在する CEBGP インターフェイスで OSPF プロセスがイネーブルにならないようにする必要があります。

（注） この連合では、サブ自律システムの IGP ドメインで CEBGP-1 および CEBGP-2 のアドレスが認識されている必要があります。ルータ設定の一部として next-hop-self アドレスを指定しない場合は、CEBGP-1 および CEBGP-2 のアドレスだけでなく、サブ自律システム内のすべての PE デバイスのアドレスがネットワーク全体に配布されるようにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***sub-autonomous-system*
4. **bgp confederation identifier***as-number*
5. **bgp conferderation peers***sub-autonomous-system*
6. **no bgp default route-target filter**
7. **address-family vpnv4** [**unicast**]
8. **neighbor***peer-group-name***remote-as***as-number*
9. **neighbor***peer-group-name***next-hop-self**
10. **neighbor***peer-group-name***activate**
11. **exit-address-family**
12. **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 モードをイネーブルにします。 • 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	**router bgp***sub-autonomous-system* 例： `Device(config)# router bgp 2`	EBGP ルーティング プロセスを作成し、それに自律システム番号を割り当てて、デバイスでコンフィギュレーション モードを開始します。 • サブ自律システム番号は、他のサブ自律システムの EBGP デバイスでデバイスを識別できるようにするために渡されます。
ステップ 4	**bgp confederation identifier***as-number* 例： `Device(config-router)# bgp confederation identifier 100`	各サブ自律システムに関連付けられる連合識別子を指定することによって、EBGP 連合を定義します。 • サブ自律システムは、単一の自律システムと見なされます。

	コマンドまたはアクション	目的
ステップ 5	**bgp conferderation peers***sub-autonomous-system* 例： `Device(config-router)# bgp confederation peers 1`	連合に属するサブ自律システムを指定します（連合内の他のサブ自律システムのネイバーを特殊な EBGP ピアとして指定します）。
ステップ 6	**no bgp default route-target filter** 例： `Device(config-router)# no bgp default route-target filter`	BGP の route-target コミュニティ フィルタリングをディセーブルにします。受信したすべての BGP VPN-IPv4 ルートがデバイスによって受け入れられます。
ステップ 7	**address-family vpnv4** [**unicast**] 例： `Device(config-router)# address-family vpnv4`	VPN バックボーン全体で VPNv4 アドレスを伝送するルーティング セッションを設定します。8 バイトの RD を追加することによって、各アドレスはグローバルに一意になります。アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードによって、ユニキャスト プレフィックスが指定されます。
ステップ 8	**neighbor***peer-group-name***remote-as***as-number* 例： `Device(config-router-af)# neighbor 1 remote-as 1`	アドレス ファミリ コンフィギュレーション モードを開始して、隣接 EBGP ピア グループを指定します。 • この EBGP ピア グループは、指定したサブ自律システムに属すると見なされます。
ステップ 9	**neighbor***peer-group-name***next-hop-self** 例： `Device(config-router-af)# neighbor 1 next-hop-self`	デバイスを指定したネイバーのネクスト ホップとしてアドバタイズします。 • next-hop-self アドレスがルータ設定の一部として指定されている場合は、**redistribute connected** コマンドを使用する必要はありません。
ステップ 10	**neighbor***peer-group-name***activate** 例： `Device(config-router-af)# neighbor R activate`	指定したサブ自律システムのネイバー PE デバイスへの VPNv4 アドレス ファミリのアドバタイズメントをアクティブにします。

	コマンドまたはアクション	目的
ステップ 11	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	ルータ コンフィギュレーション モードのアドレス ファミリ サブモードを終了します。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ASBR で VPN-IPv4 アドレスを交換する Inter-AS の確認

VPN-IPv4 ラベル転送情報ベース（LFIB）エントリを表示するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**]
3. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**]
4. **disable**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**] 例： `Device# show ip bgp vpnv4 all labels`	VPN アドレス情報を BGP テーブルから表示します。 • すべての VPNv4 ラベルについての情報を表示するには、**all** キーワードおよび **labels** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**] 例： `Device# show mpls forwarding-table`	MPLS LFIB の内容（ルートの VPNv4 プレフィックスや長さ、BGP ネクストホップ宛先など）を表示します。
ステップ 4	**disable** 例： `Device# disable`	ユーザ EXEC モードに戻ります。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の設定例

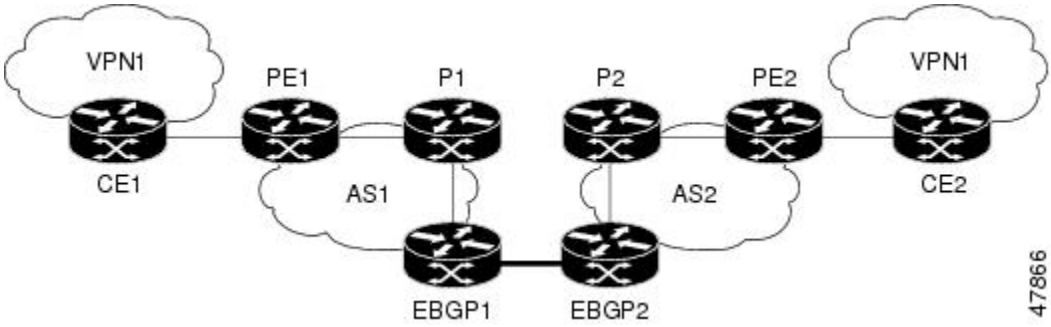
例：ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の設定

次の図のネットワーク トポロジは、次のように設定された 2 つの自律システムを示しています。

- 自律システム 1（AS1）には、プロバイダー エッジ 1（PE1）、P1、外部 Border Gateway Protocol 1（EBGP1）が含まれています。内部ゲートウェイ プロトコル（IGP）は Open Shortest Path First（OSPF）です。
- 自律システム 2（AS2）には、PE2、P2、および EBGP2 が含まれています。IGP は、Intermediate System to Intermediate System（IS-IS）です。
- カスタマー エッジ 1（CE1）および CE2 は、VPN1 という同じ VPN に属しています。
- P デバイスはルート リフレクタです。
- EBGP1 は、**redistribute connected subnets** コマンドを使用して設定されています。

- EBGP2 は、**neighbor next-hop-self** コマンドを使用して設定されています。

図 *7*：*2* つの自律システムの設定



例：自律システム 1 CE1 の設定

次の例は、2 つの自律システムがあるトポロジにおける VPN1 の CE1 の設定方法を示しています。

```
interface Loopback1
 ip address 10.1.0.4 255.0.0.0
!
interface GigabitEthernet0/0/0
   no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface GigabitEthernet0/5/3 point-to-point
  ip address 10.1.0.2 255.0.0.0
 frame-relay interface-dlci 22
!
router ospf 1
 network 192.168.3.0 255.255.0.0 area 0
```

例：自律システム 1 PE1 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS1 の PE1 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 1:105
 route-target export 1:100
 route-target import 1:100
!
interface GigabitEthernet0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/0.3 point-to-point
 ip vrf forwarding V1
 ip address 192.168.2.4 255.255.0.0
 frame-relay interface-dlci 22
!
interface GigabitEthernet0/5/3
 ip address 192.168.3.5 255.255.0.0
```

```
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 192.168.41.0 255.255.0.0 area 0
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 1 metric 100 subnets
 network 192.168.41.0 255.255.0.0 area 0
!
router bgp 1
 no synchronization
 neighbor 1 peer-group
 neighbor 1 remote-as 1
 neighbor 1 update-source Loopback0
 neighbor 192.168.11.10 peer-group R
 no auto-summary
 !
 address-family ipv4 vrf V1
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor R activate
  neighbor R send-community extended
  neighbor 192.168.11.10 peer-group R
  no auto-summary
  exit-address-family
```

例：自律システム 1 P1 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS1 の P1 の設定方法を示しています。

```
ip cef
!
interface Loopback0
 ip address 10.1.2.1 255.0.0.0
!
interface GigabitEthernet0/4/7
 ip address 10.1.0.4 255.0.0.0
 tag-switching ip
!
interface GigabitEthernet0/5/3
 ip address 10.2.0.3 255.0.0.0
 duplex auto
 speed auto
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.0.2 255.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor 192.168.3.4 peer-group R
 neighbor 192.168.3.5 peer-group R
 !
 address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
```

```
 neighbor R send-community extended
 neighbor 192.168.3.4 peer-group R
 neighbor 192.168.3.5 peer-group R
 exit-address-family
```

例：自律システム 1 EBGP1 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS1 の EBGP1 の設定方法を示しています。

```
ip cef
!
interface Loopback0
 ip address 10.2.2.1 255.0.0.0
!
!
ip cef
!
interface Loopback0
 ip address 10.2.2.1 255.0.0.0
!
interface GigabitEthernetEthernet0/5/3
 ip address 10.1.0.5 255.0.0.0
 tag-switching ip
!
interface GigabitEthernet0/0/0
!
interface GigabitEthernet0/0/0.1 point-to-point
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network 10.1.0.5 255.0.0.0 area 0
!
router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor 10.1.0.2 remote-as 2
 neighbor 10.1.0.2 peer-group R
 no auto-summary
 !
 address-family vpnv4
  neighbor R activate
  neighbor R send-community extended
  neighbor 10.1.0.2 activate
  neighbor 10.1.0.2 send-community extended
  neighbor 10.1.0.2 peer-group R
  no auto-summary
  exit-address-family
```

例：自律システム 2 EBGP2 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS2 の EBGP2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:103
 route-target export 1:100
 route-target import 1:100
!
```

```
interface Loopback0
 ip address 10.1.1.2 255.0.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 10.1.1.2 255.0.0.0
!
interface GigabitEthernet0/4/7
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/3 point-to-point
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
interface GigabitEthernet0/0/4
 no ip address
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface GigabitEthernet0/0/4.1 point-to-point
 ip address 10.1.0.5 255.0.0.0
 pvc 1/100
!
router isis
 net 49.0002.0000.0000.0003.00
!
router bgp 2
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor 10.1.0.1 remote-as 1
 neighbor 10.1.1.2 remote-as 2
 neighbor 10.1.1.2 update-source Loopback0
 neighbor 10.1.1.2 next-hop-self
!
 address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor 10.1.0.1 activate
  neighbor 10.1.0.1 send-community extended
  neighbor 10.1.1.2 activate
  neighbor 10.1.1.2 next-hop-self
  neighbor 10.1.1.2 send-community extended
  exit-address-family
```

例：自律システム 2 P2 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS2 の P2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:108
 route-target export 1:100
 route-target import 1:100
!
```

```
interface Loopback0
 ip address 10.1.0.2 255.0.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 10.1.0.2 255.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.2.1.4 255.0.0.0
 ip router isis
 tag-switching ip
!
interface GigabitEthernet0/0/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface GigabitEthernet0/0/3.1 point-to-point
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
router isis
 net aa.0002.0000.0000.0008.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 2
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor 10.1.2.1 peer-group R
 neighbor 10.0.1.2 peer-group R
 !
 address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 10.1.2.1 peer-group R
  neighbor 10.0.1.2 peer-group R
  exit-address-family
```

例：自律システム 2 PE2 の設定

次の例は、2 つの自律システムがあるトポロジにおける AS2 の PE2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:109
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 192.168.11.10 255.255.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 192.168.11.10 255.255.0.0
```

```
!
interface GigabitEthernet0/5/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/5/3.1 point-to-point
 ip vrf forwarding V1
 ip unnumbered Loopback1
 frame-relay interface-dlci 24
!
interface GigabitEthernet0/0/0
 ip address 192.168.2.10 255.255.0.0
 ip router isis
 tag-switching ip
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 2 subnets
 network 192.168.2.2 255.255.0.0 area 0
!
router isis
 net 49.0002.0000.0000.0009.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.3.2 remote-as 2
 neighbor 192.168.3.2 update-source Loopback0
 !
 address-family ipv4 vrf V1
  redistribute connected
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 send-community extended
  exit-address-family v
```

例：自律システム 2 CE2 の設定

次の例は、2 つの自律システムがあるトポロジにおける VPN1 の CE2 の設定方法を示しています。

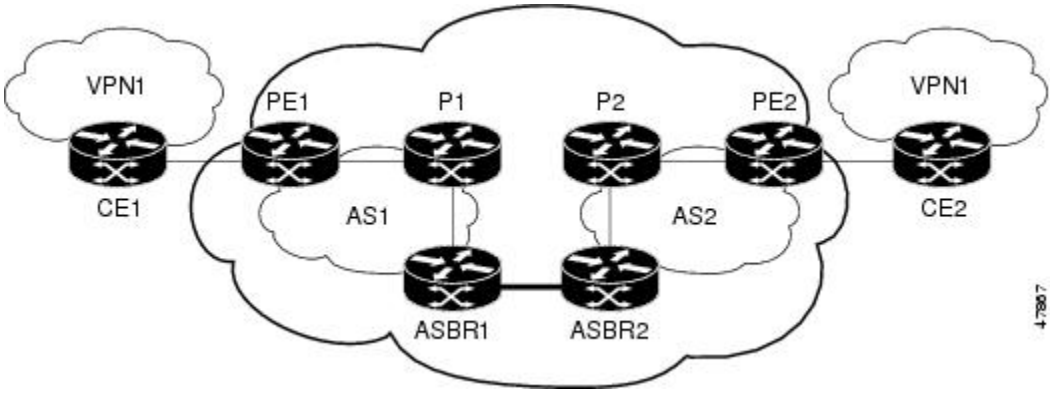
```
interface Loopback0
 ip address 192.168.2.2 255.255.0.0
!
interface GigabitEthernet0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/0.1 point-to-point
 ip unnumbered Loopback0
 frame-relay interface-dlci 24
!
router ospf 1
 network 192.168.4.6 255.255.0.0 area 0
```

例：連合において ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の設定

次の図のネットワーク トポロジは、バックボーンを連合でパーティション化した、単一のインターネット サービス プロバイダーを示しています。プロバイダーの自律システム番号は 100 です。2 つの自律システムでは独自の IGP が実行されており、次のように設定されています。

- 自律システム 1（AS1）には、プロバイダーエッジ 1（PE1）、P1、自律システム境界ルータ 1（ASBR1）が含まれています。内部ゲートウェイ プロトコル（IGP）は Open Shortest Path First（OSPF）です。
- 自律システム 2（AS2）には、PE2、P2、ASBR2 が含まれています。IGP は、Intermediate System to Intermediate System（IS-IS）です。
- カスタマー エッジ 1（CE1）および CE2 は、VPN1 という同じ VPN に属しています。
- P デバイスはルート リフレクタです。
- ASBR1 は、**redistribute connected subnets** コマンドを使用して設定されています。
- ASBR2 は、**neighbor next-hop-self** コマンドを使用して設定されています。

図 *8*：連合内の *2* つの自律システムの設定



例：自律システム 1 CE1 の設定

次の例は、連合トポロジにおける VPN1 の CE1 の設定方法を示しています。

```
interface Loopback1
 ip address 192.168.3.4 255.255.255.255
!
interface GigabitEthernet0/4/7
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface GigabitEthernet0/4/7.1 point-to-point
 ip address 192.168.1.3 255.255.0.0
```

```
 frame-relay interface-dlci 22
!
router ospf 1
 network 192.168.0.1 255.255.0.0 area 0
```

例：自律システム 1 PE1 の設定

次の例は、連合トポロジにおける AS1 の PE1 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 1:105
 route-target export 1:100
 route-target import 1:100
!
interface GigabitEthernet0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/0.3 point-to-point
 ip vrf forwarding V1
 ip address 10.0.2.4 255.0.0.0
 frame-relay interface-dlci 22
!
interface GigabitEthernet0/4/7
 ip address 10.1.2.6 255.0.0.0
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.8.4 255.0.0.0 area 0
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 1 metric 100 subnets
 network 10.1.8.4 255.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp confederation identifier 100
 bgp confederation identifier 100
 neighbor 1 peer-group
 neighbor 1 remote-as 1
 neighbor 1 update-source Loopback0
 neighbor 10.2.1.2 peer-group R
 no auto-summary
 !
 address-family ipv4 vrf V1
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor R activate
  neighbor R send-community extended
  neighbor 10.2.1.2 peer-group R
  no auto-summary
  exit-address-family
```

例：自律システム 1 P1 の設定

次の例は、連合トポロジにおける AS1 の P1 の設定方法を示しています。

```
ip cef
!
interface Loopback0
 ip address 10.0.0.2 255.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.2.1.1 255.0.0.0
 tag-switching ip
!
interface GigabitEthernet0/4/7
 ip address 10.2.2.1 255.0.0.0
 duplex auto
 speed auto
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.2.2 255.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor 10.0.0.4 peer-group R
 neighbor 10.0.0.5 peer-group R
 !
 address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 10.1.0.4 peer-group R
  neighbor 10.1.0.5 peer-group R
  exit-address-family
```

例：自律システム 1 ASBR1 の設定

次の例は、連合トポロジにおける AS1 の ASBR1 の設定方法を示しています。

```
ip cef
!
interface Loopback0
 ip address 10.0.0.4 255.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.2.1.40 255.255.255.0
 tag-switching ip
!
interface GigabitEthernet0/5/3
 no ip address
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface GigabitEthernet0/5/3.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 pvc 1/100
!
router ospf 1
 log-adjacency-changes
```

```
 redistribute connected subnets
 network 10.0.0.3 255.0.0.0 area 0
!
router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp confederation identifier 100
 bgp confederation peers 1
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor 10.0.0.2 remote-as 2
 neighbor 10.0.0.2 next-hop-self
 neighbor 10.0.0.2 peer-group R
 no auto-summary
 !
 address-family vpnv4
  neighbor R activate
  neighbor R send-community extended
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 next-hop-self
  neighbor 10.0.0.2 send-community extended
  neighbor 10.0.0.2 peer-group R
  no auto-summary
  exit-address-family
```

例：自律システム 2 ASBR2 の設定

次の例は、連合トポロジにおける AS2 の ASBR2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:103
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 10.0.0.3 255.0.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 10.0.0.3 255.0.0.0
!
interface GigabitEthernet0/4/7
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/4/7.2 point-to-point
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
interface GigabitEthernet0/5/3
 no ip address
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface GigabitEthernet0/5/3.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 pvc 1/100
!
```

```
router isis
 net aa.0002.0000.0000.0003.00
!
router bgp 2
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp confederation identifier 100
 bgp confederation peers 1
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 next-hop-self
 neighbor 10.0.0.8 remote-as 2
 neighbor 10.0.0.8 update-source Loopback0
 neighbor 10.0.0.8 next-hop-self
 !
 address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 next-hop-self
  neighbor 10.0.0.1 send-community extended
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 next-hop-self
  neighbor 10.0.0.8 send-community extended
  exit-address-family
```

例：自律システム 2 P2 の設定

次の例は、連合トポロジにおける AS2 の P2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:108
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 10.0.0.8 255.0.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 10.0.0.8 255.0.0.0
!
interface GigabitEthernet0/0/0
 ip address 10.9.1.2 255.0.0.0
 ip router isis
 tag-switching ip
!
interface GigabitEthernet0/5/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface GigabitEthernet0/5/3.1 point-to-point
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
router isis
 net aa.0002.0000.0000.0008.00
!
router bgp 2
```

```
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor R peer-group
 neighbor R remote-as 2
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor 10.0.0.3 peer-group R
 neighbor 10.0.0.9 peer-group R
 !
 address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 10.0.0.3 peer-group R
  neighbor 10.0.0.9 peer-group R
  exit-address-family
```

例：自律システム 2 PE2 の設定

次の例は、連合トポロジにおける AS2 の PE2 の設定方法を示しています。

```
ip cef
!
ip vrf V1
 rd 2:109
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 10.0.0.9 255.0.0.0
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 10.0.0.9 255.0.0.0
!
interface GigabitEthernet0/0/4
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/4.1 point-to-point
 description Bethel
 ip vrf forwarding V1
 ip unnumbered Loopback1
 frame-relay interface-dlci 24
!
interface GigabitEthernet0/4/7
 ip address 10.9.1.1 255.0.0.0
 ip router isis
 tag-switching ip
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 2 subnets
 network 10.0.0.2 255.0.0.0 area 0
!
router isis
 net aa.0002.0000.0000.0009.00
!
```

```
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor 10.0.0.8 remote-as 2
 neighbor 10.0.0.8 update-source Loopback0
 !
 address-family ipv4 vrf V1
  redistribute connected
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-community extended
  exit-address-family
```

例：自律システム 2 CE2 の設定

次の例は、連合トポロジにおける VPN1 の CE2 の設定方法を示しています。

```
interface Loopback0
 ip address 10.0.0.11 255.0.0.0
!
interface GigabitEthernet0/0/7
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface GigabitEthernet0/0/7.1 point-to-point
ip unnumbered Loopback0
 frame-relay interface-dlci 24
!
router ospf 1
 network 10.0.1.2 255.0.0.0 area 0
```

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
MPLS	『MPLS Product Literature』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1700	『*Assigned Numbers*』
RFC 1966	『*BGP Route Reflection: An Alternative to Full Mesh IBGP*』
RFC 2842	『*Capabilities Advertisement with BGP-4*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3107	『*Carrying Label Information in BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*ASBR* で *VPN-IPv4* アドレスを交換する *MPLS VPN Inter-AS* の機能情報

機能名	リリース	機能情報
MPLS VPN 相互自律システムのサポート	Cisco IOS XE Release 3.7S	MPLS VPN 相互自律システムのサポート機能を使用すると、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。この機能は、ASBR を使用して VPN-IPv4 アドレスを交換するように Inter-AS を設定する方法について説明します。 Cisco IOS XE Release 3.7S では、Cisco ASR 903 ルータのサポートが追加されました。 この機能で使用される新しいコマンドまたは変更されたコマンドはありません。

第 3 章

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS 機能を使用すると、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）がサービス プロバイダーおよび自律システムにまたがることができます。この章では、自律システム境界ルータ（ASBR）がプロバイダーエッジ（PE）ルータの MPLS ラベル付きの IPv4 ルートを交換できるように MPLS VPN Inter-AS ネットワークを設定する方法について説明します。ルート リフレクタ（RR）は、マルチホップ マルチプロトコル外部ボーダー ゲートウェイ プロトコル（eBGP）を使用して VPN-IPv4 ルートを交換します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の前提条件

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS を設定する前に、ネットワークで MPLS VPN 動作が適切に設定されている必要があります。

次の表に、Cisco IOS S リリースにおける Cisco 12000 シリーズ ラインカードのサポートを示します。

表 2 : *Cisco IOS S* リリースにおける *Cisco 12000* シリーズ ラインカードのサポート

タイプ	ラインカード	サポートされる Cisco IOS リリース
ATM	4 ポート OC-3 ATM 1 ポートOC-12 ATM 4□ OC-12 ATM 8 ポート OC-3 ATM	12.0(22)S 12.0(23)S 12.0(27)S
チャネライズド インターフェイス	2 ポート CHOC-3 6 ポート Ch T3 (DS1) 1 ポート CHOC-12 (DS3) 1 ポート CHOC-12 (OC-3) 4 ポート CHOC-12 ISE 1 ポート CHOC-48 ISE	12.0(22)S 12.0(23)S 12.0(27)S

タイプ	ラインカード	サポートされる Cisco IOS リリース
電気インターフェイス	6 ポート DS3 12 ポート DS3 6 ポート E3 12 ポート E3	12.0(22)S 12.0(23)S 12.0(27)S
イーサネット	3 ポート GbE	12.0(23)S 12.0(27)S
Packet Over Sonet（POS）	4 ポート OC-3 POS 8 ポート OC-3 POS 16 ポート OC-3 POS 1 ポート OC-12 POS 4 ポート OC-12 POS 1 ポート OC-48 POS 4 ポートOC-3 POS ISE 8 ポートOC-3 POS ISE 16 ポートOC-3 POS ISE 4 ポートOC-12 POS ISE 1 ポートOC-48 POS ISE	12.0(22)S 12.0(23)S 12.0(27)S

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の制約事項

- eBGP マルチホップが設定されたネットワークでは、非隣接ルータ間にラベル スイッチド パス（LSP）を設定する必要があります。
- 複数の BGP スピーカーを接続する物理インターフェイスは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングと MPLS をサポートしている必要があります。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS に関する情報

MPLS VPN Inter-AS の概要

自律システムとは、共通のシステム管理グループによって管理され、単一の明確に定義されたルーティング プロトコルを使用する、単一のネットワークまたはネットワークのグループのことです。

VPNが大規模になるにつれて、その要件も多くなります。場合によっては、VPNが異なる地理的エリアの異なる自律システムに存在する必要があります。また、一部のVPNは、複数のサービスプロバイダーにまたがって設定する必要があります（オーバーラッピングVPN）。VPNがどのように複雑で、どのような場所にあっても、自律システム間の接続はカスタマーに対してシームレスである必要があります。

MPLS VPN Inter-AS の利点

マルチプロトコル ラベル スイッチング（MPLS）VPN Inter-AS には次の利点があります。

- VPN が複数のサービス プロバイダー バックボーンをカバーできる：異なる自律システムを実行する複数のサービス プロバイダーが、共同で同じカスタマーに MPLS VPN サービスを提供できます。あるカスタマー サイトから開始し、さまざまな VPN サービス プロバイダー バックボーンを通過して、同じカスタマーの別のサイトに到達するように VPN を設定できます。以前は、MPLS VPN は、単一の Border Gateway Protocol（BGP）自律システム サービス プロバイダー バックボーンのみを通過できました。この機能により、複数の自律システムが、サービスプロバイダーのカスタマー サイト間に連続性がありシームレスなネットワークを形成できます。

- VPN を異なるエリアに作成できる：サービス プロバイダーは、異なる地理的エリアに VPN を作成できます。すべての VPN トラフィック フローを（エリア間で）1 箇所のポイントを通過させるようにすると、エリア間のネットワーク トラフィックのレートをより適切に制御できます。

- 連合により内部ボーダー ゲートウェイ プロトコル（IBGP）メッシングを最適化できる：自律システム内の内部ボーダー ゲートウェイ プロトコル（iBGP）メッシングがより整理され、管理しやすくなります。自律システムを複数の異なるサブ自律システムに分割して、それらを単一の連合に分類できます（ただし、VPNバックボーン全体は単一の自律システムと見なされます）。連合を形成するサブ自律システム間でのラベル付き VPN-IPv4 ネットワーク層到達可能性情報（NLRI）の交換がサポートされているため、サービス プロバイダーはこの機能を使用して、連合全体で MPLS VPN を提供できます。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の使用に関する情報

この機能では、ASBR が PE ルータの MPLS ラベル付きの IPv4 ルートを交換できるように MPLS VPN Inter-AS ネットワークを設定できます。RR は、マルチホップ マルチプロトコル外部ボーダーゲートウェイ プロトコル（eBGP）を使用して VPN-IPv4 ルートを交換します。このように Inter-AS システムを設定する方法は、多くの場合 MPLS VPN Inter-AS--IPv4 BGP ラベル配布と呼ばれます。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の利点

Inter-AS システムを設定して、ASBR で MPLS ラベル付きの IPv4 ルートが交換できるようにすることには、次のような利点があります。

- ASBR にすべての VPN-IPv4 ルートを格納する必要がなくなります。ルート リフレクタを使用して VPN-IPv4 ルートを格納し、PE ルータに転送すると、ASBR がすべての VPN-IPv4 ルートを保持し、VPN-IPv4 ラベルに基づいてルートを転送する設定と比較して、改善されたスケーラビリティが得られます。
- ルート リフレクタに VPN-IPv4 ルートを保持することによって、ネットワークの境界における設定が簡易化されます。
- 非 VPN コア ネットワークが、VPN トラフィックの中継ネットワークとして動作できます。MPLS ラベルの付いた IPv4 ルートを非 MPLS VPN サービス プロバイダー経由で送信できます。
- 隣接 LSR 間で他のラベル配布プロトコルが必要なくなります。隣接する 2 つのラベル スイッチング ルータ（LSR）が BGP ピアでもある場合、BGP で MPLS ラベルの配布を実行できます。これら 2 つの LSR 間で、他のラベル配布プロトコルは必要ありません。

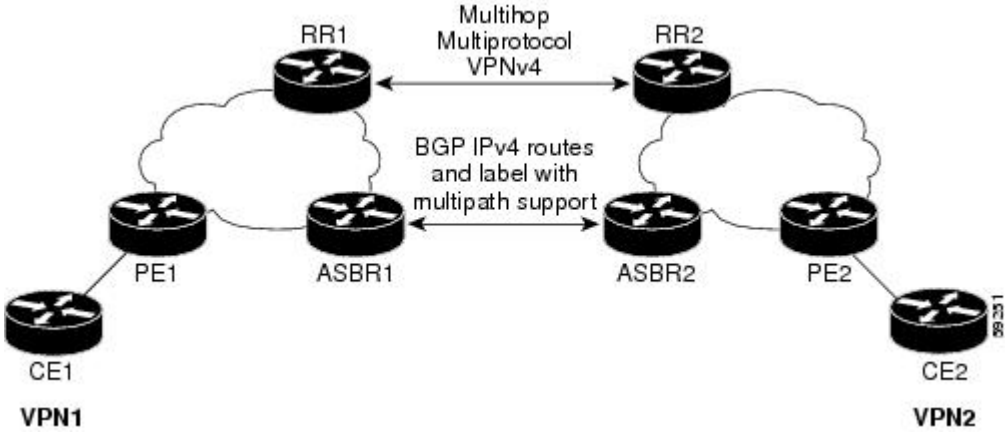
ASBR が MPLS ラベル付きの IPv4 ルートを交換する場合の Inter-AS の動作

MPLS ラベル付きの IPv4 ルートを交換する VPN サービス プロバイダー ネットワークを設定できます。VPN サービス プロバイダー ネットワークは次のように設定できます。

- ルート リフレクタは、マルチホップ マルチプロトコル eBGP を使用して VPN-IPv4 ルートを交換します。この設定では、自律システムをまたがってネクストホップ情報および VPN ラベルが維持されます。
- ローカル PE ルータ（たとえば次の図の PE1）は、リモート PE ルータ（PE2）のルートおよびラベル情報を把握する必要があります。この情報は、次のいずれかの方法で PE ルータおよび ASBR 間で交換できます。

- 内部ゲートウェイ プロトコル（IGP）とラベル配布プロトコル（LDP）：ASBR は、eBGP から学習した IPv4 ルートおよび MPLS ラベルを IGP および LDP に再配布できます。その逆も可能です。
- 内部ボーダー ゲートウェイ プロトコル（iBGP）IPv4 ラベル配布：ASBR および PE ルータは、直接 iBGP セッションを使用して、VPN-IPv4 と IPv4 ルートおよび MPLS ラベルを交換できます。

または、ルート リフレクタが、ASBR から学習した IPv4 ルートおよび MPLS ラベルを VPN の PE ルータに反映できます。これは、ASBR がルート リフレクタと IPv4 ルートおよび MPLS ラベルを交換することによって実現されます。ルート リフレクタは、VPN-IPv4 ルートも VPN の PE ルータに反映します。たとえば、次の図の VPN1 で、RR1 は、学習した VPN-IPv4 ルート、および ASBR1 から学習した IPv4 ルートと MPLS ラベルを PE1 に反映します。ルート リフレクタを使用して VPN-IPv4 ルートを格納し、それらを PE ルータおよび ASBR 経由で転送することによって、スケーラブルな設定が可能となります。



BGP ルーティング情報

BGP ルーティング情報には、次の項目が含まれています。

- 宛先の IP アドレスであるネットワーク番号（プレフィックス）。
- ルートがローカル ルータに到達するために通過する他の自律システムのリストである自律システム パス。リスト内の最初の自律システムはローカル ルータに最も近いシステムです。リスト内の最後の自律システムはローカル ルータから最も遠いシステムであり、通常、ルートの始点となる自律システムです。
- ネクスト ホップなどの、自律システム パスについての他の情報を提供するパス属性。

BGP メッセージのタイプと MPLS ラベル

MPLS ラベルは、ルータが送信するアップデート メッセージに含まれています。ルータ間では、次のタイプの BGP メッセージが交換されます。

- キープアライブ メッセージ：ルータ間では、隣接ルータがルーティング情報を交換可能であるかどうかを判断するためにキープアライブ メッセージが交換されます。ルータは、定期的にこれらのメッセージを送信します（シスコ ルータのデフォルトは 60 秒です。）キープアライブ メッセージには、ルーティング データは含まれていません。メッセージ ヘッダーのみが含まれています。
- 通知メッセージ：ルータでエラーが検出されると、通知メッセージが送信されます。
- オープン メッセージ：ルータが隣接ルータとの間で TCP 接続を確立すると、ルータ間でオープン メッセージが交換されます。このメッセージには、ルータが属する自律システムの数とメッセージを送信したルータの IP アドレスが含まれています。
- アップデート メッセージ：ルータのルートが新規作成、変更、または切断された場合、ルータは隣接ルータにアップデート メッセージを送信します。このメッセージには、使用可能なルートの IP アドレスのリストを含む NLRI が含まれます。アップデート メッセージには、使用できなくなったすべてのルートが含まれています。また、アップデート メッセージには、使用可能なパスと使用できないパスの両方のパス属性と長さも含まれています。アップデート メッセージでは、VPN-IPv4 ルートのラベルは RFC 2858 の規定に従って符号化されます。また、アップデート メッセージでは、IPv4 ルートのラベルは RFC 3107 の規定に従って符号化されます。

BGP においてルートとともに MPLS ラベルが送信される方法

BGP（eBGP および iBGP）でルートを配布するときに、そのルートにマッピングされている MPLS ラベルも配布できます。ルートの MPLS ラベル マッピング情報は、ルートについての情報を含む BGP 更新メッセージによって伝送されます。ネクスト ホップが変わらない場合は、ラベルも維持されます。

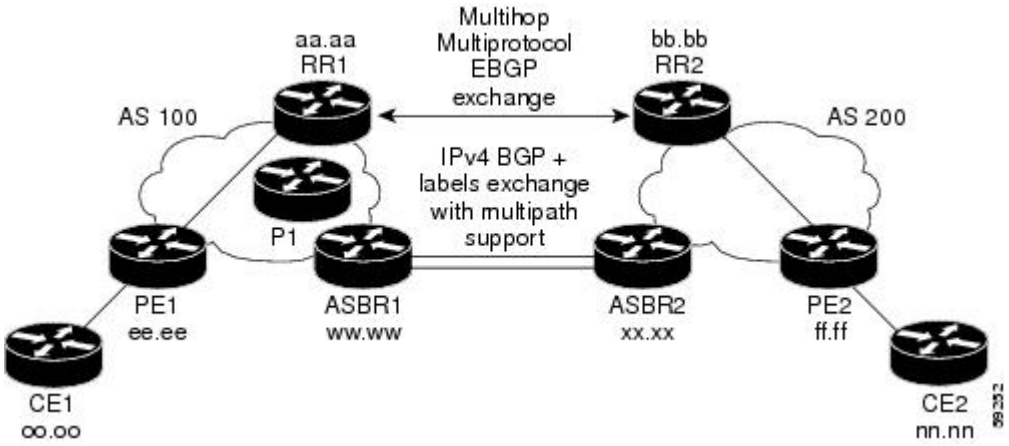
両方の BGP ルータで **neighbor send-label** コマンドを発行すると、それらのルータでルートとともに MPLS ラベルを送信できるという内容がルータ間で相互にアドバタイズされます。ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の設定方法

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS を設定するには、次の各項で説明する作業を実行します。

次の図に次の設定例を示します。

- この設定は、2 つの VPN で構成されています。
- ASBR は、MPLS ラベル付きの IPv4 ルートを交換します。
- ルートリフレクタは、マルチホップ MPLS eBGP を使用して VPN-IPv4 ルートを交換します。
- ルートリフレクタは、自律システム内の他のルータに IPv4 ルートおよび VPN-IPv4 ルートを反映します。



IPv4 ルートおよび MPLS ラベルを交換する ASBR の設定

IPv4 ルートおよび MPLS ラベルを交換する ASBR を設定するには、次の作業を実行します。この設定手順では、例として ASBR1 を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **mdt** | **vrf***vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor***ip-address***send-label**
8. **exit-address-family**
9. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータでルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor hh.0.0.1 remote-as 200`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **mdt** | **vrf***vrf-name*] 例： `Router(config-router)# address-family ipv4`	標準 IPv4 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **mdt** キーワードでは、IPv4 マルチキャスト配布ツリー（MDT）アドレス ファミリ セッションを指定します。

	コマンドまたはアクション	目的
		• **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VPN ルーティングおよび転送（VRF）インスタンスの名前を指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor hh.0.0.1 activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**neighbor***ip-address***send-label** 例： `Router(config-router-af)# neighbor hh.0.0.1 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 • *ip-address* 引数には、ネイバー ルータの IP アドレスを指定します。
ステップ 8	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

VPN-IPv4 ルートを交換するようにルート リフレクタを設定する

ルート リフレクタでマルチホップ マルチプロトコル eBGP を使用して VPN-IPv4 ルートを交換できるようにするには、次の作業を実行します。

また、この手順では、自律システム間でネクスト ホップ情報および VPN ラベルが維持されるように指定します。この手順では、ルート リフレクタの例として RR1 を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
6. **address-family vpnv4** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **next-hopunchanged**
9. **exit-address-family**
10. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータでルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。 自律システム番号によって、他の自律システム内のルータでRR1が特定されます。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor bb.bb.bb.bb remote-as 200`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
		• *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `Router(config-router)# neighbor bb.bb.bb.bb ebgp-multihop 255`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *ttl* 引数には、1 ～ 255 ホップの範囲の存続可能時間を指定します。
ステップ 6	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、BGP セッションなどの、標準 VPNv4 アドレス プレフィックスを使用するルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor bb.bb.bb.bb activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **next-hopunchanged** 例： `Router(config-router-af)# neighbor ip-address next-hop unchanged`	eBGP マルチホップ ピアで、ネクスト ホップを変更せずに伝播できるようにします。 • *ip-address* 引数には、ネクスト ホップの IP アドレスを指定します。 • *peer-group-name* 引数には、ネクスト ホップである BGP ピア グループの名前を指定します。
ステップ 9	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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 10	**end** 例： `Router(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

ルート リフレクタが自律システム内でリモート ルートを反映するように設定する

RR が ASBR から学習した IPv4 ルートおよびラベルを自律システム内の PE ルータに反映できるようにするには、次の作業を実行します。

これは、ASBR および PE ルータを RR のルート リフレクタ クライアントにすることによって実現されます。また、この手順では、RR で VPN-IPv4 ルートを反映できるようにする方法についても説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name***activate**
6. **neighbor***ip-address***route-reflector-client**
7. **neighbor***ip-address***send-label**
8. **exit-address-family**
9. **address-family vpnv4** [**unicast**]
10. **neighbor** {*ip-address* | *peer-group-name*} **activate**
11. **neighbor***ip-address***route-reflector-client**
12. **exit-address-family**
13. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータでルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始して、BGP セッションなどの、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF インスタンスの名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name***activate** 例： `Router(config-router-af)# neighbor ee.ee.ee.ee activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	**neighbor***ip-address***route-reflector-client** 例： `Router(config-router-af)# neighbor ee.ee.ee.ees route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。 • *ip-address* 引数には、クライアントとして設定する BGP ネイバーの IP アドレスを指定します。
ステップ 7	**neighbor***ip-address***send-label** 例： `Router(config-router-af)# neighbor ee.ee.ee.ee send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 • *ip-address* 引数には、ネイバー ルータの IP アドレスを指定します。
ステップ 8	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、BGP セッションなどの、標準 VPNv4 アドレス プレフィックスを使用するルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor ee.ee.ee.ee activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 11	**neighbor***ip-address***route-reflector-client** 例： `Router(config-router-af)# neighbor ee.ee.ee.ee route-reflector-client`	RR がネイバー ルータに iBGP ルートを送信できるようにします。

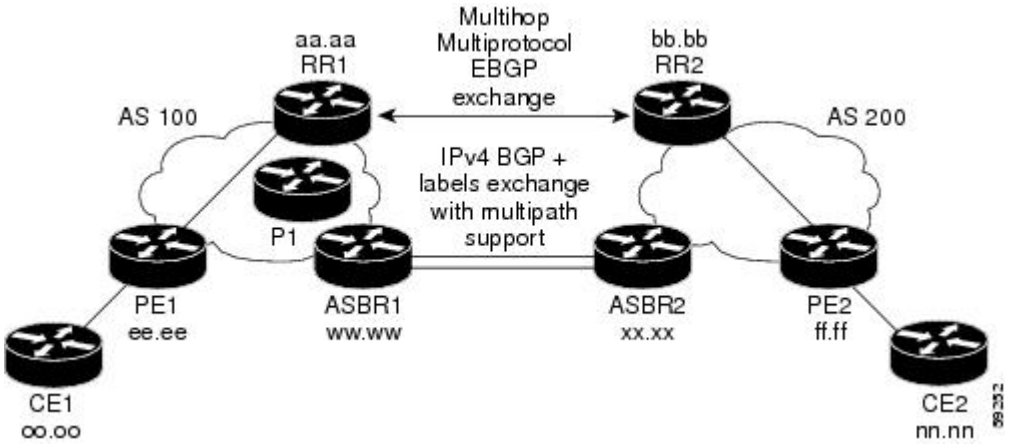
ステップ 12	**exit-address-family**
	
	例：
	
	`Router(config-router-af)#`
	
	`exit-address-family`
		アドレス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の検証

ASBR を使用して IPv4 ラベルとルート リフレクタを配布し、VPN-IPv4 ルートを配布するには、次の手順に従って設定を確認します。

次の図に、以降の項で参照される設定を示します。



ルート リフレクタ設定の確認

ルート リフレクタ設定を確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name* } [**summary**] [**labels**]
3. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name* } [**summary**] [**labels**] 例： `Router# show ip bgp vpnv4 all summary`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • ルートリフレクタ間にマルチホップマルチプロトコル eBGP セッションが存在し、ルートリフレクタ間で VPNv4 ルートが交換されていることを確認するには、**all** キーワードと **summary** キーワードを使用します。 コマンド出力の最後の 2 行に、次の情報が表示されます。 • プレフィックスが PE1 から学習されて RR2 に渡されていること。 • プレフィックスが RR2 から学習されて PE1 に渡されていること。 • ルートリフレクタ間で VPNv4 ラベル情報が交換されていることを確認するには、**all** キーワードと **labels** キーワードを使用します。
ステップ 3	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

CE1 が CE2 と通信できることの確認

ルータ CE1 がルータ CE2 の NLRI を持っていることを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [**protocol** [*protocol-id*]] | [**list** [*access-list-number* | *access-list-name*]
3. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [**protocol** [*protocol-id*]] | [**list** [*access-list-number* | *access-list-name*] 例： `Router# show ip route nn.nn.nn.nn`	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。 • このコマンドを使用して、CE1 が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。
ステップ 3	**disable** 例： `Router# disable`	（任意）終了して、特権 EXEC モードに戻ります。

PE1 が CE2 と通信できることの確認

ルータ PE1 がルータ CE2 の NLRI を持っていることを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip route vrf***vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list***number* [*output-modifiers*]] [**profile**] [**static** [[]] [**summary***output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]]
3. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [*ip-prefix* | *length* [**longer-prefixes**] [*output-modifiers*]]] [**network-address***mask*]]**longer-prefixes** [*output-modifiers*]][**cidr-only**] [**community**][**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]
4. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
5. **show mpls forwarding-table** [{*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
6. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
7. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**]
8. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip route vrf***vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list***number* [*output-modifiers*]] [**profile**] [**static** [[]] [**summary***output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]] 例： `Router# show ip route vrf vpn1 nn.nn.nn.nn`	（任意）VRF 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。 • このコマンドを使用して、ルータ PE1 がルータ CE2（nn.nn.nn.nn）からルートを学習していることを確認します。

ステップ 3	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [*ip-prefix* | *length* [**longer-prefixes**] [*output-modifiers*]]] [**network-address***mask*]]**longer-prefixes** [*output-modifiers*]][**cidr-only**] [**community**][**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]
	
	例：
	`Router# show ip bgp vpnv4 vrf vpn1 nn.nn.nn.nn`
	
	例：
	`Router# show ip bgp vpnv4 all nn.nn.nn.nn`
		（任意）BGP テーブルからの VPN アドレス情報を表示します。
		• ルータ PE2 がルータ CE2 の BGP ネクストホップであることを確認するには、**vrf** キーワードまたは **all** キーワードを使用します。

ステップ 4	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef vrf vpn1 nn.nn.nn.nn`	（任意）転送情報ベース（FIB）のエントリを表示するか、または FIB のサマリーを表示します。 • このコマンドを使用して、Cisco Express Forwarding エントリが正しいことを確認します。
ステップ 5	**show mpls forwarding-table** [{*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]	（任意）MPLS LFIB の内容を表示します。 • このコマンドを使用して、BGP ネクストホップルータ（自律システム境界）の IGP ラベルを確認します。

	コマンドまたはアクション	目的
	例： `Router# show mpls forwarding-table`	
ステップ 6	**show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] 例： `Router# show ip bgp ff.ff.ff.ff`	（任意）BGP ルーティングテーブルのエントリを表示します。 • **show ip bgp** コマンドを使用して、リモート出力 PE ルータ（PE2）のラベルを確認します。
ステップ 7	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**] 例： `Router# show ip bgp vpnv4 all labels`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • PE2 からアドバタイズされた CE2 の VPN ラベルを確認するには、**all** キーワードと **summary** キーワードを使用します。
ステップ 8	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

PE2 が CE2 と通信できることの確認

PE2 が CE2 にアクセスできることを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip route vrf***vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list***number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary**[*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]]
3. **show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
4. **show ip bgp vpnv4** { **all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**]
5. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
6. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip route vrf***vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list***number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary**[*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]] 例： `Router# show ip route vrf vpn1 nn.nn.nn.nn`	（任意）VRF 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。 • このコマンドを使用して、CE2 の VPN ルーティングおよび転送テーブルを確認します。出力に、ネクストホップ情報が表示されます。
ステップ 3	**show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**] 例： `Router# show mpls forwarding-table vrf vpn1 nn.nn.nn.nn`	（任意）LFIB の内容を表示します。 • CE2 の VPN ルーティングおよび転送テーブルを確認するには、**vrf**キーワードを使用します。出力に、CE2 のラベルと発信インターフェイスが表示されます。
ステップ 4	**show ip bgp vpnv4** { **all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**] 例： `Router# show ip bgp vpnv4 all labels`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • Multiprotocol BGP テーブル内の CE2 の VPN ラベルを確認するには、**all** キーワードと **labels** キーワードを使用します。
ステップ 5	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef vpn1 nn.nn.nn.nn`	（任意）FIB のエントリを表示するか、または FIB のサマリーを表示します。 • このコマンドを使用して、CE2 のシスコ エクスプレス フォワーディング エントリを確認します。コマンド出力に、CE2 のローカル ラベルと発信インターフェイスが表示されます。

	コマンドまたはアクション	目的
ステップ 6	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

ASBR の設定の確認

ASBR 間で、ルート マップの指定に従って MPLS ラベル付きの IPv4 ルートまたはラベルなしの IPv4 ルートが交換されていることを確認するには、次の作業を実行します。

ASBR の設定の確認

手順の概要

1. **enable**
2. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
3. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
4. **disable**

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。 • パスワードを入力します（要求された場合）。

ステップ 2	**show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
	
	例：
	`Router# show ip bgp ff.ff.ff.ff`
		（任意）BGP ルーティング テーブルのエントリを表示します。
		• このコマンドを使用して次のことを確認します。
		  • ASBR1 が ASBR2 から PE2 の MPLS ラベルを受信していること。
		  • ASBR1 が ASBR2 から RR2 のラベルなし IPv4 ルートを受信していること。
		  • ASBR2 が ASBR1 に PE2 の MPLS ラベルを配布していること。

	コマンドまたはアクション	目的
		• ASBR2 が ASBR1 に RR2 のラベルを配布していないこと。

ステップ 3	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
	
	例：
	`Router# show ip cef ff.ff.ff.ff`
	
	例：
	`Router# show ip cef bb.bb.bb.bb`
		（任意）FIB のエントリを表示するか、または FIB のサマリーを表示します。
		• ASBR1 と ASBR2 からこのコマンドを使用して、次の点を確認します。
		  • PE2 のシスコ エクスプレス フォワーディング エントリが正しいこと。
		  • RR2 のシスコ エクスプレス フォワーディング エントリが正しいこと。

ステップ 4	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の設定例

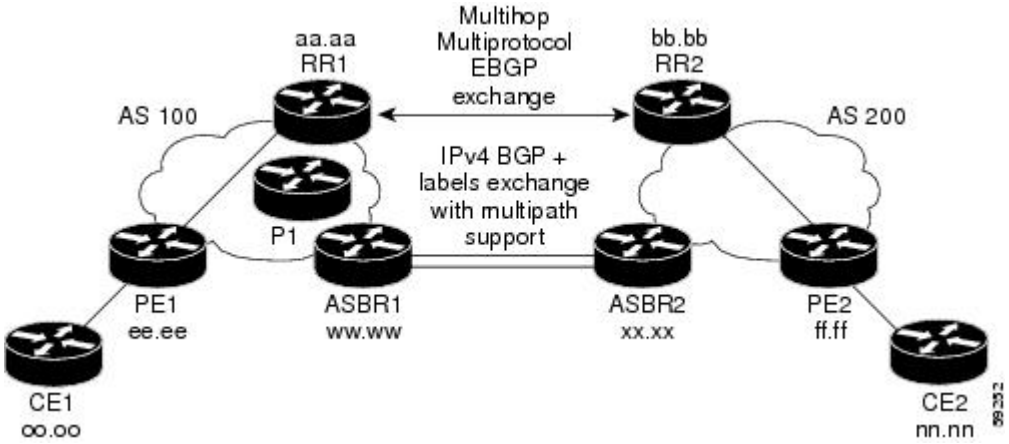
ASBR で MPLS VPN サービス プロバイダーを介して IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の設定例

ここでは、BGP を使用して MPLS VPN サービス プロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS の次の設定例について説明します。

次の図に、2 つの MPLS VPN サービス プロバイダーを示します。サービス プロバイダーは、ルート リフレクタ間で VPN-IPv4 ルートを配布します。MPLS VPN サービス プロバイダーは、ASBR 間で MPLS ラベル付きの IPv4 ルートを配布します。

設定例では、リモートの RR と PE の VPN-IPv4 ルートおよび MPLS ラベル付きの IPv4 ルートをローカルの RR と PE に配布するために使用できる次の 2 つの技術を示しています。

- 自律システム 100 は、RR を使用して、リモート RR から学習した VPN-IPv4 ルートを配布します。また、RR は、IPv4 ラベルを使用して、ASBR1 から学習したリモート PE アドレスとラベルを配布します。
- 自律システム 200 では、ASBR2 が学習した IPv4 ルートは IGP に再配布されます。



ルート リフレクタ 1 の設定例（MPLS VPN サービス プロバイダー）

RR1 の設定例では、次のことが指定されています。

- RR1 は、マルチプロトコル マルチホップ eBGP を使用して、RR2 と VPN-IPv4 ルートを交換します。
- VPN-IPv4 ネクスト ホップ情報および VPN ラベルは、自律システム間で保存されます。
- RR1 から PE1 に次の内容が反映されます。
  - RR2 から学習した VPN-IPv4 ルート
  - ASBR1 から学習した IPv4 ルートおよび MPLS ラベル

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet0/3
 ip address dd.0.0.2 255.0.0.0
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
```

```
 neighbor ee.ee.ee.ee remote-as 100
 neighbor ee.ee.ee.ee update-source Loopback0
 neighbor ww.ww.ww.ww remote-as 100
 neighbor ww.ww.ww.ww update-source Loopback0
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb ebgp-multihop 255
 neighbor bb.bb.bb.bb update-source Loopback0
 no auto-summary
 !
address-family ipv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee route-reflector-client                !IPv4+labels session to PE1
 neighbor ee.ee.ee.ee send-label
 neighbor ww.ww.ww.ww activate
 neighbor ww.ww.ww.ww route-reflector-client                !IPv4+labels session to ASBR1
 neighbor ww.ww.ww.ww send-label
 no neighbor bb.bb.bb.bb activate
 no auto-summary
 no synchronization
 exit-address-family
 !
address-family vpnv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee route-reflector-client                !VPNv4 session with PE1
 neighbor ee.ee.ee.ee send-community extended
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb next-hop-unchanged                    !MH-VPNv4 session with RR2
 neighbor bb.bb.bb.bb send-community extended                 !with next hop unchanged

 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end
```

ASBR1 の設定例（MPLS VPN サービス プロバイダー）

ASBR1 は、ASBR2 と IPv4 ルートおよび MPLS ラベルを交換します。

この例では、ASBR1 で、次のルート マップを使用してルートがフィルタリングされています。

- OUT というルート マップでは、ASBR1 において、PE1 ルート（ee.ee）はラベルを付けて配布し、RR1 ルート（aa.aa）はラベルを付けずに配布する必要があることが指定されています。
- IN というルートマップでは、ASBR1 にラベル付きの PE2 ルート（ff.ff）とラベルなしの RR2 ルート（bb.bb）を受け入れさせるように指定しています。

```
ip subnet-zero
mpls label protocol ldp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
!
interface Ethernet0/2
 ip address hh.0.0.2 255.0.0.0
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
```

```
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor hh.0.0.1 remote-as 200
 no auto-summary
 !
!
address-family ipv4                        ! Redistributing IGP into BGP
 redistribute ospf 10                      ! so that PE1 & RR1 loopbacks
 neighbor aa.aa.aa.aa activate             ! get into the BGP table
 neighbor aa.aa.aa.aa send-label
 neighbor hh.0.0.1 activate
 neighbor hh.0.0.1 advertisement-interval 5
 neighbor hh.0.0.1 send-label
 neighbor hh.0.0.1 route-map IN in         ! accepting routes in route map IN.
 neighbor hh.0.0.1 route-map OUT out       ! distributing routes in route map OUT.
 neighbor kk.0.0.1 activate
 neighbor kk.0.0.1 advertisement-interval 5
 neighbor kk.0.0.1 send-label
 neighbor kk.0.0.1 route-map IN in         ! accepting routes in route map IN.
 neighbor kk.0.0.1 route-map OUT out       ! distributing routes in route map OUT.
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.ee.ee.ee log                !Setting up the access lists
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
route-map IN permit 10                              !Setting up the route maps
 match ip address 2
 match mpls-label
!
route-map IN permit 11
 match ip address 4
!
route-map OUT permit 12
 match ip address 3
!
route-map OUT permit 13
 match ip address 1
 set mpls-label
!
end
```

ルート リフレクタ 2 の設定例（MPLS VPN サービス プロバイダー）

RR2 は、マルチホップ マルチプロトコル eBGP を使用して、RR1 と VPN-IPv4 ルートを交換します。また、この設定では、自律システム間でネクストホップ情報およびVPNラベルが維持されるように指定されています。

```
ip subnet-zero
```

```
ip cef
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.2 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.bb.bb.bb 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa ebgp-multihop 255
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor ff.ff.ff.ff remote-as 200
 neighbor ff.ff.ff.ff update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa next-hop-unchanged              !Multihop VPNv4 session with RR1
 neighbor aa.aa.aa.aa send-community extended              !with next-hop-unchanged
 neighbor ff.ff.ff.ff activate
 neighbor ff.ff.ff.ff route-reflector-client          !VPNv4 session with PE2
 neighbor ff.ff.ff.ff send-community extended
 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end
```

ASBR2 の設定例（MPLS VPN サービス プロバイダー）

ASBR2 は、ASBR1 と IPv4 ルートおよび MPLS ラベルを交換します。ただし、ASBR1 とは異なり、ASBR2 は RR を使用して IPv4 ルートおよび MPLS ラベルを PE2 に反映しません。ASBR2 は、ASBR1 から学習した IPv4 ルートおよび MPLS ラベルを IGP に再配布します。これで、PE2 がこれらのプレフィックスに到達できるようになります。

```
ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet1/0
 ip address hh.0.0.1 255.0.0.0
!
interface Ethernet1/2
 ip address jj.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 !
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets           ! Redistributing the routes learned from
 passive-interface Ethernet1/0               ! ASBR1(eBGP+labels session) into IGP
```

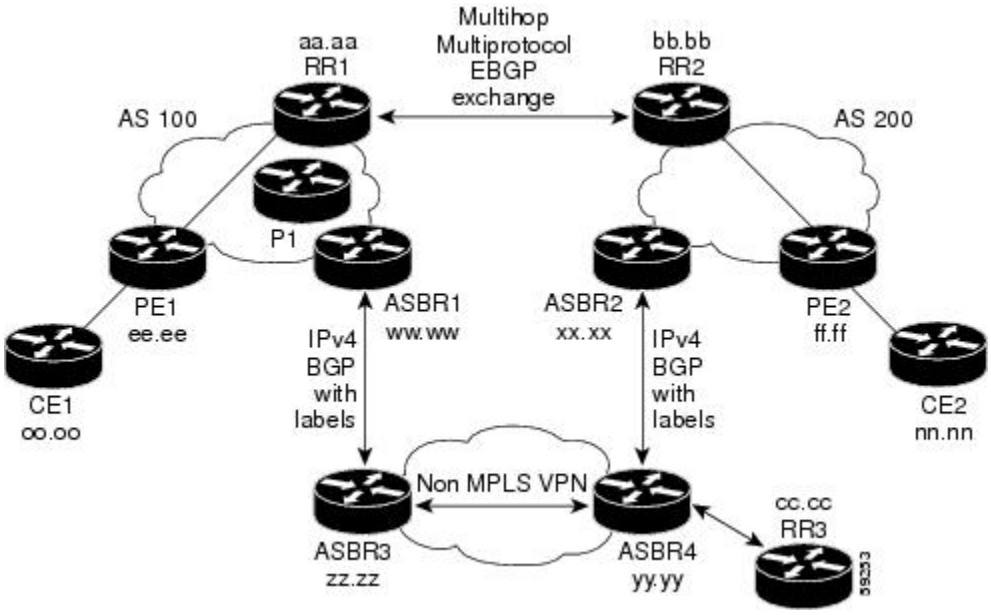
```
 network xx.xx.xx.xx 0.0.0.0 area 200         ! so that PE2 will learn them
 network jj..0.0 0.255.255.255 area 200
 !
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb update-source Loopback0
 neighbor hh.0.0.2 remote-as 100
 no auto-summary
 !
address-family ipv4
 redistribute ospf 20                         ! Redistributing IGP into BGP
 neighbor hh.0.0.2 activate                   ! so that PE2 & RR2 loopbacks
 neighbor hh.0.0.2 advertisement-interval 5   ! will get into the BGP-4 table.
 neighbor hh.0.0.2 route-map IN in
 neighbor hh.0.0.2 route-map OUT out
 neighbor hh.0.0.2 send-label
 neighbor kk.0.0.2 activate
 neighbor kk.0.0.2 advertisement-interval 5
 neighbor kk.0.0.2 route-map IN in
 neighbor kk.0.0.2 route-map OUT out
 neighbor kk.0.0.2 send-label
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb send-community extended
 exit-address-family
 !
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log          !Setting up the access lists
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
route-map IN permit 11                       !Setting up the route maps
 match ip address 2
 match mpls-label
!
route-map IN permit 12
 match ip address 4
!
route-map OUT permit 10
 match ip address 1
 set mpls-label
!
route-map OUT permit 13
 match ip address 3
end
```

ASBR で非 MPLS VPN サービス プロバイダーを介して IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の設定例

ここでは、BGP を使用して非 MPLS VPN サービス プロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS の次の設定例について説明します。

次の図に、非 MPLS VPN サービス プロバイダー経由で接続された 2 つの MPLS VPN サービス プロバイダーを示します。ネットワーク中間の自律システムは、LDP または Tag Distribution Protocol（TDP）を使用して MPLS ラベルを配布するバックボーン自律システムとして設定されます。TDP

や LDP の代わりにトラフィック エンジニアリング トンネルを使用して、非 MPLS VPN サービス プロバイダー全体に LSP を構築することもできます。



ルート リフレクタ 1 の設定例（非 MPLS VPN サービス プロバイダー）

RR1 の設定例では、次のことが指定されています。

- RR1 は、マルチプロトコル マルチホップ eBGP を使用して、RR2 と VPN-IPv4 ルートを交換します。
- VPN-IPv4 ネクスト ホップ情報および VPN ラベルは、自律システム間で保存されます。
- RR1 から PE1 に次の内容が反映されます。
  - RR2 から学習した VPN-IPv4 ルート
  - ASBR1 から学習した IPv4 ルートおよび MPLS ラベル

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
 ip address dd.0.0.2 255.0.0.0
 clockrate 124061
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
```

```
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.ee.ee.ee remote-as 100
 neighbor ee.ee.ee.ee update-source Loopback0
 neighbor ww.ww.ww.ww remote-as 100
 neighbor ww.ww.ww.ww update-source Loopback0
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb ebgp-multihop 255
 neighbor bb.bb.bb.bb update-source Loopback0
 no auto-summary
 !
address-family ipv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee route-reflector-client                !IPv4+labels session to PE1
 neighbor ee.ee.ee.ee send-label
 neighbor ww.ww.ww.ww activate
 neighbor ww.ww.ww.ww route-reflector-client                !IPv4+labels session to ASBR1
 neighbor ww.ww.ww.ww send-label
 no neighbor bb.bb.bb.bb activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee route-reflector-client               !VPNv4 session with PE1
 neighbor ee.ee.ee.ee send-community extended
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb next-hop-unchanged                    !MH-VPNv4 session with RR2
 neighbor bb.bb.bb.bb send-community extended                 with next-hop-unchanged
 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end
```

ASBR1 の設定例（非 MPLS VPN サービス プロバイダー）

ASBR1 は、ASBR2 と IPv4 ルートおよび MPLS ラベルを交換します。

この例では、ASBR1 で、次のルート マップを使用してルートがフィルタリングされています。

- OUT というルート マップでは、ASBR1 において、PE1 ルート（ee.ee）はラベルを付けて配布し、RR1 ルート（aa.aa）はラベルを付けずに配布する必要があることが指定されています。
- IN というルートマップでは、ASBR1 にラベル付きの PE2 ルート（ff.ff）とラベルなしの RR2 ルート（bb.bb）を受け入れさせるように指定しています。

```
ip subnet-zero
ip cef distributed
mpls label protocol ldp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
!
interface Serial3/0/0
 ip address kk.0.0.2 255.0.0.0
```

```
 ip route-cache distributed
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Serial3/0/0
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor kk.0.0.1 remote-as 200
 no auto-summary
!
 address-family ipv4
 redistribute ospf 10                      ! Redistributing IGP into BGP
 neighbor aa.aa.aa.aa activate             ! so that PE1 & RR1 loopbacks
 neighbor aa.aa.aa.aa send-label           ! get into BGP table
 neighbor kk.0.0.1 activate
 neighbor kk.0.0.1 advertisement-interval 5
 neighbor kk.0.0.1 send-label
 neighbor kk.0.0.1 route-map IN in    ! Accepting routes specified in route map IN
 neighbor kk.0.0.1 route-map OUT out  ! Distributing routes specified in route map OUT
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.ee.ee.ee log
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
!
route-map IN permit 10
 match ip address 2
 match mpls-label
!
route-map IN permit 11
 match ip address 4
!
route-map OUT permit 12
 match ip address 3
!
route-map OUT permit 13
 match ip address 1
 set mpls-label
!
end
```

ルート リフレクタ 2 の設定例（非 MPLS VPN サービス プロバイダー）

RR2 は、マルチホップ マルチプロトコル eBGP を使用して、RR1 と VPN-IPv4 ルートを交換します。また、この設定では、自律システム間でネクストホップ情報および VPN ラベルが維持されるように指定されています。

```
ip subnet-zero
ip cef
```

```
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.2 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.bb.bb.bb 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa ebgp-multihop 255
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor ff.ff.ff.ff remote-as 200
 neighbor ff.ff.ff.ff update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa next-hop-unchanged              !MH vpnv4 session with RR1
 neighbor aa.aa.aa.aa send-community extended              !with next-hop-unchanged
 neighbor ff.ff.ff.ff activate
 neighbor ff.ff.ff.ff route-reflector-client          !vpnv4 session with PE2
 neighbor ff.ff.ff.ff send-community extended
 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end
```

ASBR2 の設定例（非 MPLS VPN サービス プロバイダー）

ASBR2 は、ASBR1 と IPv4 ルートおよび MPLS ラベルを交換します。ただし、ASBR1 とは異なり、ASBR2 は RR を使用して IPv4 ルートおよび MPLS ラベルを PE2 に反映しません。ASBR2 は、ASBR1 から学習した IPv4 ルートおよび MPLS ラベルを IGP に再配布します。これで、PE2 がこれらのプレフィックスに到達できるようになります。

```
ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet0/1
 ip address qq.0.0.2 255.0.0.0
!
interface Ethernet1/2
 ip address jj.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 !
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets            !redistributing the routes learned from
 passive-interface Ethernet0/1                !ASBR2 (eBGP+labels session) into IGP
 network xx.xx.xx.xx 0.0.0.0 area 200         !so that PE2 will learn them
```

```
 network jj.0.0.0 0.255.255.255 area 200
 !
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb update-source Loopback0
 neighbor qq.0.0.1 remote-as 100
 no auto-summary
!
address-family ipv4                          ! Redistributing IGP into BGP
                                                                  redistribute ospf 20
                    ! so that PE2 & RR2 loopbacks
 neighbor qq.0.0.1 activate                  !  will get into the BGP-4 table
 neighbor qq.0.0.1 advertisement-interval 5
 neighbor qq.0.0.1 route-map IN in
 neighbor qq.0.0.1 route-map OUT out
 neighbor qq.0.0.1 send-label
 no auto-summary
 no synchronization
 exit-address-family
 !
address-family vpnv4
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb send-community extended
 exit-address-family
 !
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 11
 match ip address 2
 match mpls-label
!
route-map IN permit 12
 match ip address 4
!
route-map OUT permit 10
 match ip address 1
 set mpls-label
!
route-map OUT permit 13
 match ip address 3
!
end
```

ASBR3 の設定例（非 MPLS VPN サービス プロバイダー）

ASBR3 は、非 MPLS VPN サービス プロバイダーに属しています。ASBR3 は、ASBR1 との間で IPv4 ルートおよび MPLS ラベルを交換します。また、ASBR3 は、ASBR1 から学習したルートを RR3 経由で ASBR4 に渡します。

（注） iBGP を使用してルートおよびラベルを配布する場合は、学習した eBGP ルートを iBGP に再配布しないでください。このような設定はサポートされていません。

```
ip subnet-zero
ip cef
!
interface Loopback0
```

```
 ip address yy.yy.yy.yy 255.255.255.255
interface Hssi4/0
 ip address mm.0.0.0.1 255.0.0.0
 mpls ip
 hssi internal-clock
 !
interface Serial5/0
 ip address kk.0.0.1 255.0.0.0
 load-interval 30
 clockrate 124061
!
router ospf 30
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
network yy.yy.yy.yy 0.0.0.0 area 300
network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor kk.0.0.2 remote-as 100
 no auto-summary
 !
 address-family ipv4
 neighbor cc.cc.cc.cc activate            ! iBGP+labels session with RR3
 neighbor cc.cc.cc.cc send-label
 neighbor kk.0.0.2 activate               ! eBGP+labels session with ASBR1
 neighbor kk.0.0.2 advertisement-interval 5
 neighbor kk.0.0.2 send-label
 neighbor kk.0.0.2 route-map IN in
 neighbor kk.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit ee.ee.ee.ee log
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
!
route-map IN permit 10
 match ip address 1
  match mpls-label
!
route-map IN permit 11
   match ip address 3
!
route-map OUT permit 12
 match ip address 2
  set mpls-label
!
route-map OUT permit 13
   match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

ルート リフレクタ 3 の設定例（非 MPLS VPN サービス プロバイダー）

RR3 は、MPLS ラベル付きの IPv4 ルートを ASBR3 および ASBR4 に反映する非 MPLS VPN RR です。

```
ip subnet-zero
mpls label protocol ldp
mpls traffic-eng auto-bw timers
no mpls ip
!
interface Loopback0
 ip address cc.cc.cc.cc 255.255.255.255
!
interface POS0/2
 ip address pp.0.0.1 255.0.0.0
 crc 16
 clock source internal
!
router ospf 30
 log-adjacency-changes
 network cc.cc.cc.cc 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 neighbor zz.zz.zz.zz remote-as 300
 neighbor zz.zz.zz.zz update-source Loopback0
 neighbor yy.yy.yy.yy remote-as 300
 neighbor yy.yy.yy.yy update-source Loopback0
 no auto-summary
 !
address-family ipv4
 neighbor zz.zz.zz.zz activate
 neighbor zz.zz.zz.zz route-reflector-client
 neighbor zz.zz.zz.zz send-label               ! iBGP+labels session with ASBR3
 neighbor yy.yy.yy.yy activate
 neighbor yy.yy.yy.yy route-reflector-client
 neighbor yy.yy.yy.yy send-label               ! iBGP+labels session with ASBR4
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

ASBR4 の設定例（非 MPLS VPN サービス プロバイダー）

ASBR4 は、非 MPLS VPN サービス プロバイダーに属しています。ASBR4 と ASBR3 は、RR3 経由で IPv4 ルートと MPLS ラベルを交換します。

（注） iBGP を使用してルートおよびラベルを配布する場合は、学習した eBGP ルートを iBGP に再配布しないでください。このような設定はサポートされていません。

```
ip subnet-zero
ip cef distributed
!
interface Loopback0
 ip address zz.zz.zz.zz 255.255.255.255
```

```
!
interface Ethernet0/2
 ip address qq.0.0.1 255.0.0.0
!
interface POS1/1/0
 ip address pp.0.0.2 255.0.0.0
 ip route-cache distributed
 !
interface Hssi2/1/1
 ip address mm.0.0.2 255.0.0.0
 ip route-cache distributed
 mpls label protocol ldp
 mpls ip
 hssi internal-clock
!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network zz.zz.zz.zz 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
 network mm.0.0.0 0.255.255.255 area 300
 !
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor qq.0.0.2 remote-as 200
 no auto-summary
 !
 address-family ipv4
 neighbor cc.cc.cc.cc activate
 neighbor cc.cc.cc.cc send-label
 neighbor qq.0.0.2 activate
 neighbor qq.0.0.2 advertisement-interval 5
 neighbor qq.0.0.2 send-label
 neighbor qq.0.0.2 route-map IN in
 neighbor qq.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 10
 match ip address 1
  match mpls-label
!
route-map IN permit 11
   match ip address 3
!
route-map OUT permit 12
 match ip address 2
  set mpls-label
!
route-map OUT permit 13
   match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

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
MPLS	『MPLS Product Literature』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1700	『*Assigned Numbers*』
RFC 1966	『*BGP Route Reflection: An Alternative to Full Mesh IBGP*』
RFC 2842	『*Capabilities Advertisement with BGP-4*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3107	『*Carrying Label Information in BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3*：*ASBR* で *IPv4* ルートおよび *MPLS* ラベルを交換する *MPLS VPN Inter-AS* の機能情報

機能名	リリース	機能の設定情報
ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS	12.0(21)ST 12.0(22)S 12.0(23)S 12.2(13)T 12.0(24)S 12.2(14)S 12.0(27)S 12.0(29)S Cisco IOS XE Release 2.5	この章では、ASBR がプロバイダー エッジ（PE）ルータの MPLS ラベル付きの IPv4 ルートを交換できるように MPLS VPN Inter-AS ネットワークを設定する方法について説明しています。ルート リフレクタ（RR）は、マルチホップ マルチプロトコル外部ボーダーゲートウェイ プロトコル（eBGP）を使用して VPN-IPv4 ルートを交換します。 この機能は、Cisco IOS XE Release 2.5 で、Cisco ASR 1000 シリーズ ルータに実装されました。 この機能で使用される新しいコマンドまたは変更されたコマンドはありません。

第 4 章

MPLS VPN--Inter-AS オプション AB

MPLS VPN--Inter-AS オプション AB 機能は、Inter-AS オプション（10）A ネットワークと Inter-AS オプション（10）B ネットワークの最良の機能を組み合わせたものです。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）サービスプロバイダーは、この機能を使用して、さまざまな自律システムを相互接続して VPN サービスを提供できます。これらのネットワークは、RFC 4364 の第 10 項「Multi-AS Backbones」のサブセクション「a」およびサブセクション「b」としてそれぞれ定義されています。

MPLS VPN--Inter-AS オプション AB 設定においてさまざまな自律システムが相互接続されると、ネットワーク設定全体がスケーラブルで簡易なものとなり、自律システム境界ルータ（ASBR）ピア間で IP Quality of Service（QoS）機能が維持されます。

Inter-AS オプション A ネットワークでは、ASBR ピアは複数のサブインターフェイスによって接続され、2 つの自律システムにまたがるインターフェイス VPN が少なくとも 1 つ設定されます。これらの ASBR では、ラベル付けされていない IP プレフィックスをシグナリングするため、各サブインターフェイスが、VPN ルーティングおよび転送（VRF）インスタンスおよび Border Gateway Protocol（BGP）セッションに関連付けられます。その結果、バックツーバック VRF 間のトラフィックは IP になります。このシナリオでは、各 VPN は相互に分離されます。また、トラフィックが IP であるため、IP トラフィック上で動作する QoS メカニズムを適用して、カスタマー サービス レベル契約（SLA）を実現できます。この設定の欠点は、各サブインターフェイスに 1 つの BGP セッションが必要となることです（各 VPN に少なくとも 1 つのサブインターフェイスも必要となります）。このことは、このネットワークの規模が大きくなるにつれて、スケーラビリティに関する問題が発生する原因となります。

Inter-AS オプション B ネットワークでは、ASBR ピアは、MPLS トラフィックを受信できる 1 つ以上のサブインターフェイスによって接続されます。ASBR 間でのラベル付き VPN プレフィックスの配布には、マルチプロトコル Border Gateway Protocol（MP-BGP）セッションが使用されます。その結果、それらの間のトラフィック フローはラベル付きとなります。この設定の欠点は、トラフィックが MPLS であるため、IP トラフィックにのみ適用できる QoS メカニズムを適用できず、VRF を分離することもできないことです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN--Inter-AS オプション AB の前提条件

次のマニュアルに説明されている適切な設定作業を実行してください。

- 『Configuring MPLS Layer 3 VPNs』
- 『MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses』
- 『MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels』

MPLS VPN--Inter-AS オプション AB 機能を設定する前に、次の作業を実行する必要があります。

- MPLS VPN ルーティングおよび転送動作に必要な Cisco Express Forwarding の有効化
- MPLS VPN--Inter-AS オプション AB ネットワークの VPN の特定、およびこれらの VPN が属する VRF の設定これらの VRF は、ASBR インターフェイス上の Inter-AS オプション AB 接続で使用されます。

MPLS VPN--Inter-AS オプション AB の制約事項

- In Service Software Upgrade（ISSU）機能は、スタンバイ ルート プロセッサ（RP）でこの機能がサポートされている場合にのみアクティブ RP で設定できます。アクティブ RP とスタンバイ RP の両方でこの機能がサポートされている場合には、ISSU 機能を設定できます。

- Carrier Supporting Carrier（CSC）MPLS ロードバランシングは、ASBR オプション AB VRF インターフェイスではサポートされていません。
- VPNv6 はサポートされていません。

MPLS VPN--Inter-AS オプション AB に関する情報

MPLS VPN--Inter-AS オプション AB の概要

MPLS VPN サービス プロバイダーは、さまざまな自律システムを相互接続して、複数の VPN カスタマーにサービスを提供する必要があります。MPLS VPN--Inter-AS オプション AB 機能を使用すると、グローバル ルーティング テーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムを相互接続し、コントロールプレーン トラフィックを伝送できます。このMP-BGP セッションでは、2 つの ASBR 間で、各 VRF インスタンスの VPN プレフィックスがシグナリングされます。データ プレーン トラフィックは VRF インターフェイス経由で送受信されます。このトラフィックは、IP または MPLS です。

（注） Inter-AS 接続は、異なるプロバイダー間の接続を持つ ASBR 間でも持たない ASBR 間でも設定できます。

MPLS VPN--Inter-AS オプション AB の利点

MPLS VPN--Inter-AS オプション AB 機能には、サービス プロバイダーにとって次の利点があります。

- ASBR で各 VRF に対して 1 つの BGP セッションのみが設定されるため、ネットワーク設定が簡略化されます。
- BGP セッションが 1 つで済むため、CPU 使用率が低減されます。
- ルータでグローバルにイネーブル化される単一のMP-BGPセッションのみが必要なため複数の VPN で必要となるセッション数が減り、また VPN が相互に分離および保護されることによって、ネットワークのスケーラビリティを向上できます。
- ASBR ピア間の IP QoS 機能を維持し、カスタマー SLA を実現できます。
- データ プレーン トラフィックは、セキュリティ上の目的で VRF ごとに分離されます。

共有リンク転送によるオプション B スタイルのピアリング

Inter-AS オプション AB を拡張した機能が、MPLS VPN—Inter-AS オプション AB+ 機能です。この機能では、MPLS VPN—Inter-AS オプション A のスケーラビリティの問題に対処するため、グローバル ルーティング テーブルで 1 つの BGP セッションを使用して VPN プレフィックスをシグナリングします（Inter-AS オプション B の説明を参照）。

オプション AB+ とオプション B の主な違いは、ASBR 間のルート配布です。オプション AB+ の場合、ASBR で、VRF にインポートされたルートが（VRF のルート識別子およびルート ターゲットと共に）ネイバー ASBR に配布されます。オプション B の場合、インポート前の元のルートが（元の RD および RT と共に）ネイバー ASBR に配布されますが、インポートされたルートは配布されません。

オプション AB+ の場合、PE と ASBR はグローバル インターフェイスを介した MPLS 転送を導入します。これはオプション B での動作に似ています。シグナリングは 1 つの MP-eBGP VPNv4 セッションにより処理されます。したがってプロバイダー エッジと ASBR の間では、標準のオプション B スタイルのピアリングが使用されます。共有リンク経由で MPLS-VPN トラフィックを受け取り、VRF ルーティング テーブルの IP ルックアップに基づいてトラフィックを転送します。ただし、オプション B の場合と同様にトラフィックは MPLS カプセル化されます。

非 CSC ネットワークにおけるルート配布およびパケット転送

ここでは、MPLS VPN--Inter-AS オプション AB の動作について説明します。

（注） すべてのルートのインポートは、適切なルート ターゲット（RT）を設定することによって行われます。

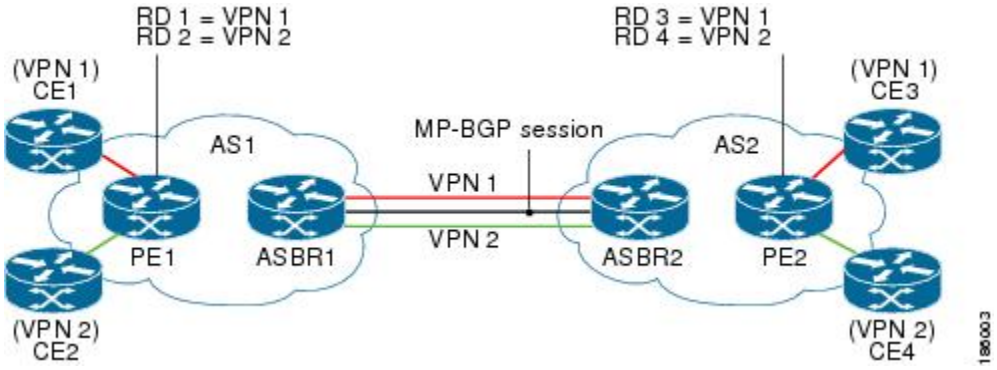
次の属性は、次の図に示すサンプル MPLS VPN--Inter-AS オプション AB ネットワークのトポロジを示しています。

- カスタマー エッジ 1（CE1）と CE3 は VPN 1 に属しています。
- CE2 と CE4 は VPN 2 に属しています。
- プロバイダー エッジ 1（PE1）では、VPN 1（VRF 1）にルート識別子 1（RD 1）を、VPN 2（VRF 2）に RD 2 を使用しています。
- PE2 は、VPN 1（VRF 1）に RD 3 を、VPN 2（VRF 2）に RD 4 を使用しています。
- ASBR1 では、VRF 1 が RD 5 に、VRF 2 が RD 6 にプロビジョニングされています。
- ASBR2 では、VRF 1 が RD 7 に、VRF 2 が RD 8 にプロビジョニングされています。
- ASBR1 と ASBR2 との間には 3 つのリンクがあります。
  - VRF 1
  - VRF 2

- MP-BGP セッション

（注） ASBR で設定した VRF はオプション AB VRF と呼ばれます。ASBR での eBGP ピアはオプション AB ピアと呼ばれます。

図 *9*：*MPLS VPN Inter-AS* オプション *AB* トポロジ



VPN 1 のルート配布

ルート識別子（RD）は、各ルートにどの VPN が属しているかを識別するためにルートに付加される識別子です。各ルーティング インスタンスには、一意な RD 自律システムが関連付けられている必要があります。RD は、VPN の周囲に境界を設置して、異なる VPN で同じ IP アドレス プレフィックスを使用してもこれらのIPアドレスプレフィックスが重複しないようにするために使用されます。

（注） RD 文は、インスタンス タイプが VRF である場合は必須です。

次のプロセスは、上記の図の VPN 1 のルート配布プロセスを示しています。このプロセスで使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

1. CE1 は、プレフィックス N を PE1 にアドバタイズします。
2. PE1 は、VPN プレフィックス RD 1:N を ASBR1 に MP 内部 BGP（iBGP）経由でアドバタイズします。
3. ASBR1 は、プレフィックスを VPN 1 にインポートして、プレフィックス RD 5:N を作成します。
4. ASBR1 は、インポートしたプレフィックス RD 5:N を ASBR2 にアドバタイズします。ASBR1 は、自身をプレフィックス RD 5:N のネクスト ホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルを割り当てます。

5 ASBR1 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。デフォルトで、ASBR1 はソース プレフィックス RD 1:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

（注） オプション 10B 接続では、ASBR1 がオプション 10B 接続を持っている他の ASBR にソース プレフィックスをアドバタイズできます。オプション 10B 接続を持っている ASBR では、すべての VPNv4 ルートが BGP テーブルに維持されます。

1 ASBR2 は、プレフィックス RD 5:N を受信して、RD 7:N として VPN 1 にインポートします。

2 ASBR2 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。

3 プレフィックスのインポート時に、ASBR2 は RD 7:N のネクスト ホップを VRF 1 の ASBR1 インターフェイス IP アドレスに設定します。ネクスト ホップ テーブル ID も VRF 1 に設定されます。RD 7:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。

4 ASBR2 は、インポートしたプレフィックス RD 7:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。デフォルトで、ASBR2 はソース プレフィックス RD 5:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

5 PE2 は、RD 7:N を RD 3:N として VRF 1 にインポートします。

VPN 1 のパケット転送

次のパケット転送プロセスは、オプション A のシナリオと同様に動作します。ASBR は VPN の終端となることによって PE と同様に動作し、トラフィックを標準 IP パケットとして VPN ラベルなしで次の PE に転送します。その後、次の PE で VPN プロセスが繰り返されます。したがって、各 PE ルータは隣接 PE ルータを CE ルータとして扱い、各自律システムでのルート再配布には標準的なレイヤ 3 MPLS VPN メカニズムが使用されます。つまり、各 PE は、外部 BGP（eBGP）を使用して相互にラベルなし IPv4 アドレスを配布します。

（注） このプロセスで使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

1 CE3 は、N 宛てのパケットを PE2 に送信します。

2 PE2 は、ASBR2 によって割り当てられた VPN ラベル、およびパケットを ASBR2 にトンネリングするために必要な内部ゲートウェイ プロトコル（IGP）ラベルでパケットをカプセル化します。

3 パケットは、VPN ラベルが付いた状態で ASBR2 に到達します。ASBR2 は VPN ラベルを削除し、パケットを IP として ASBR1 の VRF 1 インターフェイスに送信します。

4 IP パケットが、ASBR1 の VRF 1 インターフェイスに到達します。ASBR1 は、PE1 によって割り当てられた VPN ラベル、およびパケットを PE1 にトンネリングするために必要な IGP ラベルでパケットをカプセル化します。

5 パケットは、VPN ラベルが付いた状態で PE1 に到達します。PE1 は VPN ラベルを削除して、IP パケットを CE1 に転送します。

VPN 2 のルート配布

次の情報は、上記の図の VPN 2 のルート配布プロセスを示しています。

1 CE2 は、プレフィックス N を PE1 にアドバタイズします。N は VPN IP アドレスです。

2 PE1 は、VPN プレフィックス RD 2:N を ASBR1 に MP-iBGP 経由でアドバタイズします。

3 ASBR1 は、プレフィックスを VPN 2 にインポートして、プレフィックス RD 6:N を作成します。

4 ASBR1 は、インポートしたプレフィックス RD 6:N を ASBR2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。デフォルトで、ASBR1 はソース プレフィックス RD 2:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

（注） オプション 10B 接続では、ASBR1 がオプション 10B 接続を持っている他の ASBR にソース プレフィックスをアドバタイズできます。オプション 10B 接続を持っている ASBR では、すべての VPNv4 ルートが BGP テーブルに維持されます。

1 ASBR2 は、プレフィックス RD 6:N を受信して、RD 8:N として VPN 2 にインポートします。

2 プレフィックスのインポート時に、ASBR2 は RD 8:N のネクスト ホップを VRF 2 の ASBR1 インターフェイス アドレスに設定します。ネクスト ホップ テーブル ID も VRF 2 の ID に設定されます。RD 8:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。

3 ASBR2 は、インポートしたプレフィックス RD 8:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。デフォルトで、ASBR2 はソース プレフィックス RD 6:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

4 PE2 は、RD 8:N を RD 4:N として VRF 2 にインポートします。

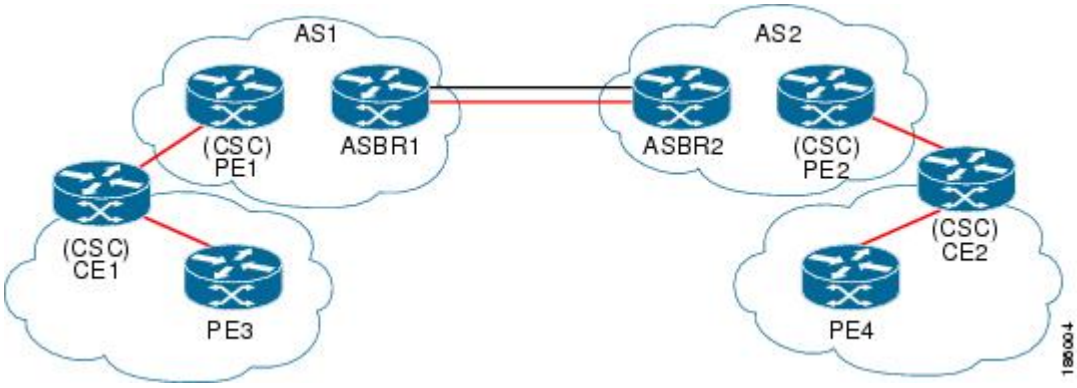
CSC におけるルート配布およびパケット転送

ここでは、VPN 1 の CSC シナリオでの MPLS VPN--Inter-AS オプション AB の動作について説明します。ここでの説明は、VPN 1 の非 CSC ネットワークにおけるルート配布およびパケット転送の説明と似ていますが、2 つの ASBR 間での MPLS ラベルの処理方法が異なります。

（注） ここでは、VPN 2 については説明しません。

次の図に、VPN 1 によって小規模カスタマー キャリアに VPN サービスが提供され、さらにその小規模カスタマー キャリアが顧客に VPN サービスを提供するようすを示します。この設定では、小規模カスタマー キャリアの PE（PE3 および PE4）ループバック インターフェイス間でラベル スイッチド パス（LSP）を提供するために VPN 1 が使用されています。

図 *10*：*MPLS VPN Inter-AS* オプション *AB CSC* トポロジ



（注） ここでの RD、RT、VRF、およびリンクのプロビジョニングは、非 CSC ネットワークにおけるルート配布およびパケット転送の VPN 1 についての例と同様です。

VPN 1 のルート配布

次の情報は、図 1 の VPN 1 のルート配布プロセスを示しています。これらの手順で使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

1. CE1 は、PE3 ループバック N を PE1 にアドバタイズします。
2. PE1 は、VPN プレフィックス RD 1:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
3. ASBR1 は、プレフィックスを VPN 1 にインポートして、プレフィックス RD 5:N を作成します。

4 ASBR1 は、インポートしたプレフィックス RD 5:N を ASBR2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。

5 ASBR1 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。デフォルトで、ASBR1 はソース プレフィックス RD 1:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

（注） オプション 10B 接続では、ASBR1 がオプション 10B 接続を持っている他の ASBR にソース プレフィックスをアドバタイズできます。オプション 10B 接続を持っている ASBR では、すべての VPNv4 ルートが BGP テーブルに維持されます。

1 ASBR2 は、プレフィックス RD 5:N を受信して、RD 7:N として VPN 1 にインポートします。

2 ASBR2 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。

3 プレフィックスのインポート時に、ASBR2 は RD 7:N のネクスト ホップを VRF 1 の ASBR1 インターフェイス アドレスに設定します。ネクスト ホップ テーブル ID も VRF 1 の ID に設定されます。

（注） CSC シナリオでは、設定を変更することによって、転送に発信 MPLS ラベルをインストールできます。Inter-AS オプション AB の設定方法, （88 ページ）を参照してください。

1 RD 7:N 用の MPLS 転送エントリをインストールする場合、ASBR2 により転送プロセス中に発信ラベルがインストールされ、これにより ASBR 間のトラフィックを MPLS トラフィックにすることができます。

2 ASBR2 は、インポートしたプレフィックス RD 7:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。デフォルトで、ASBR2 はソース プレフィックス RD 5:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

3 PE2 は、RD 7:N を RD 3:N として VRF 1 にインポートします。

VPN 1 のパケット転送

次のパケット転送プロセスは、オプション A のシナリオと同様に動作します。オプション A の詳細については、「非 CSC ネットワークにおけるルート配布およびパケット転送」の項を参照してください。

1 PE4 は、N 宛ての MPLS パケットを CE2 に送信します。

2. CE2 は MPLS ラベルを交換して、N 宛てのパケットを PE2 に送信します。
3. PE2 は、ASBR2 によって割り当てられた VPN ラベル、およびパケットを ASBR2 にトンネリングするために必要な IGP ラベルでパケットをカプセル化します。
4. パケットは、VPN ラベルが付いた状態で ASBR2 に到達します。ASBR2 は受信した VPN ラベルを ASBR1 から受信した発信ラベルと交換して、MPLS パケットを VRF 1 インターフェイスに送信します。
5. MPLS パケットが、ASBR1 の VRF 1 インターフェイスに到達します。ASBR1 は、受信した MPLS ラベルを、PE1 によって割り当てられた VPN ラベルおよびパケットを PE1 にトンネリングするために必要な IGP ラベルで構成されるラベル スタックと交換します。
6. パケットは、VPN ラベルが付いた状態で PE1 に到達します。PE1 は VPN ラベルを削除して、MPLS パケットを CE1 に転送します。その後、CE1 はラベルを交換して、ラベル付きパケットを PE3 に転送します。

非 CSC ネットワークにおける共有リンクの転送

（注） すべてのルートのインポートは、適切なルート ターゲット（RT）を設定することによって行われます。

次の属性は、「非 CSC ネットワークにおけるルート配布およびパケット転送」の項に示すサンプル ネットワーク トポロジを示しています。

- カスタマー エッジ 1（CE1）と CE3 は VPN 1 に属しています。
- CE2 と CE4 は VPN 2 に属しています。
- プロバイダー エッジ 1（PE1）では、VPN 1（VRF 1）にルート識別子 1（RD 1）を、VPN 2（VRF 2）に RD 2 を使用しています。
- PE2 は、VPN 1（VRF 1）に RD 3 を、VPN 2（VRF 2）に RD 4 を使用しています。
- ASBR1 では、VRF 1 が RD 5 に、VRF 2 が RD 6 にプロビジョニングされています。
- ASBR2 では、VRF 1 が RD 7 に、VRF 2 が RD 8 にプロビジョニングされています。
- ASBR1 と ASBR2 との間には 3 つのリンクがあります。
  - VRF 1
  - VRF 2
  - MP-BGP セッション

（注） ASBR で設定した VRF はオプション AB+ VRF と呼ばれます。ASBR での eBGP ピアはオプション AB+ ピアと呼ばれます。

ここでは、非 CSC ネットワークでの MPLS VPN—Inter-AS オプション AB+ 共有リンクの転送について説明します。

VPN 1 のルート配布

次のプロセスは、「非 CSC ネットワークにおけるルート配布およびパケット転送」の項の図の VPN 1 のルート配布プロセスを示しています。これらの手順で使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

1. CE1 は、PE3 ループバック N を PE1 にアドバタイズします。
2. PE1 は、VPN プレフィックス RD 1:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
3. ASBR1 は、プレフィックスを VPN 1 にインポートして、プレフィックス RD 5:N を作成します。
4. ASBR1 は、インポートしたプレフィックス RD 5:N を ASBR2 にアドバタイズします。ASBR1 は、自身をプレフィックス RD 5:N のネクスト ホップとして設定し、またこのプレフィックスとともにシグナリングされるローカル ラベルを割り当てます。
5. デフォルトで、ASBR1 はソース プレフィックス RD 1:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB+ VRF にインポートされるプレフィックスであるため、アドバタイズされません。

（注） オプション 10B 接続では、ASBR1 がオプション 10B 接続を持っている他の ASBR にソース プレフィックスをアドバタイズできます。オプション 10B 接続を持っている ASBR では、すべての VPNv4 ルートが BGP テーブルに維持されます。

1. ASBR2 は、プレフィックス RD 5:N を受信して、RD 7:N として VPN 1 にインポートします。
2. プレフィックスのインポート時に、ASBR2 は ASBR2 からの BGP アップデートで受信した RD7:N のネクスト ホップを維持します。これは、グローバル テーブルの ASBR1 共有インターフェイス アドレスのアドレスです。ネクスト ホップ テーブル ID も変更されず、グローバル テーブルの ID に対応しています。
3. RD 7:N 用の MPLS 転送エントリをインストールする場合、ASBR2 は転送プロセスで発信ラベルをインストールします。これにより、ASBR 間のトラフィックを IP にすることができます。
4. ASBR2 は、インポートしたプレフィックス RD 7:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカル ラベルも割り当てます。

5 デフォルトで、ASBR2 はソース プレフィックス RD 5:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB+ VRF にインポートされるプレフィックスであるため、アドバタイズされません。

6 PE2 は、RD 7:N を RD 3:N として VRF 1 にインポートします。

VPN1 のパケット転送

次のパケット転送プロセスは、オプション B のシナリオと同様に動作します。

1 CE3 は、N 宛てのパケットを PE2 に送信します。

2 PE2 は、ASBR2 によって割り当てられた VPN ラベル、およびパケットを ASBR2 にトンネリングするために必要な IGP ラベルでパケットをカプセル化します。

3 パケットは、VPN ラベルが付いた状態で ASBR2 に到達します。ASBR2 は受信した VPN ラベルを ASBR1 から受信した発信ラベルと交換して、MPLS パケットをグローバル共有リンク インターフェイスで送信します。

4 MPLS パケットが、グローバル共有リンク インターフェイスで ASBR1 に到達します。ASBR1 は、受信した MPLS ラベルを、PE1 によって割り当てられた VPN ラベルおよびパケットを PE1 にトンネリングするために必要な IGP ラベルで構成されるラベル スタックと交換します。

5 パケットは、VPN ラベルが付いた状態で PE1 に到達します。PE1 は VPN ラベルを削除して、IP パケットを CE1 に転送します。

Inter-AS オプション AB の設定方法

ここでは、MPLS VPN または CSC をサポートする MPLS VPN において ASBR で Inter-AS オプション AB 機能を設定する方法について説明します。

（注） Inter-AS オプション AB がすでにネットワークに導入されており、いくつかのプレフィックスでオプション B スタイルのピアリングを実行する場合（Inter-AS オプション AB+ を実装する場合）は、「Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定」の項の説明に従って **inter-as-hybrid global** コマンドを設定します。

Inter-AS オプション AB 接続の設定

ここでは、ASBR に Inter-AS オプション AB 接続を設定する方法について説明します。

（注） MPLS VPN における PE および CE ルータの設定の詳細については、『Configuring MPLS Layer 3 VPNs』の章を参照してください。

各 VPN カスタマーの ASBR インターフェイスへの VRF の設定

各 VPN カスタマーの ASBR インターフェイスに VRF を設定して、これらの VPN が MPLS VPN--Inter-AS オプション AB ネットワークを介して接続できるようにするには、次の手順を実行します。

（注） **mpls bgp forwarding** コマンドは、CSC をサポートする VRF の ASBR インターフェイスでのみ使用されます。

ASBR インターフェイスに設定する必要がある追加の VRF およびピア ASBR インターフェイスに設定する必要がある VRF を設定するには、次に示すすべての手順を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***typenumber*
4. **ip vrf forwarding***vrf-name*
5. **mpls bgp forwarding**
6. **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。 • 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： `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。

	コマンドまたはアクション	目的
ステップ 3	**interface***typenumber* 例： `Router(config)# interface Ethernet 5/0`	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	**ip vrf forwarding***vrf-name* 例： `Router(config-if)# ip vrf forwarding vpn1`	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。
ステップ 5	**mpls bgp forwarding** 例： `Router(config-if)# mpls bgp forwarding`	（任意）BGP を設定して、MPLS トラフィックをサポートする必要がある VRF の接続インターフェイスで MPLS 転送をイネーブルにします。 • この手順は CSC ネットワークにのみ適用されます。
ステップ 6	**end** 例： `Router(config-if)# end`	（任意）終了して、特権 EXEC モードに戻ります。

ASBR ピア間での MP-BGP セッションの設定

BGP では、IPv4 以外のアドレス ファミリのサポートを定義する BGP マルチプロトコル拡張（RFC 2283、『Multiprotocol Extensions for BGP-4』を参照）を使用して、PE ルータ間の VPN-IPv4 プレフィックスの到達可能性情報を伝播します。この拡張を使用すると、指定された VPN のルートが、その VPN の他のメンバによってのみ学習されるようになり、VPN のメンバ間の相互通信が可能になります。

この項の次の手順に従って、ASBR で MP-BGP セッションを設定します。

この手順のすべてのステップを使用して、ピア ASBR で MP-BGP セッションを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
5. **address-family vpnv4** [**unicast**]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **inter-as-hybrid**
8. **exit-address-family**
9. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータでルータ コンフィギュレーション モードを開始します。 • as-number 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor 192.168.0.1 remote-as 200`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。

	コマンドまたはアクション	目的
ステップ 5	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ 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 プレフィックスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 192.168.0.1 activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **inter-as-hybrid** 例： `Router(config-router-af)# neighbor 192.168.0.1 inter-as-hybrid`	eBGP ピア ルータ（ASBR）を Inter-AS オプション AB ピアとして設定します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • プレフィックスがオプション AB VRF にインポートされると、インポートされたパスがこのピアにアドバタイズされます。 • プレフィックスをこのピアから受信し、オプション AB VRF にインポートすると、インポートされたパスが iBGP ピアにアドバタイズされます。 （注） アドバタイズされたルートには、VRF で設定された RT があります。アドバタイズされたルートには、元の RT はありません。
ステップ 8	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定

適切なルーティング ポリシーおよびオプション AB 設定を設定して、ASBR ピア間で Inter-AS 接続が必要な VPN の VRF を設定するには、この項の手順を使用します。

この手順のすべてのステップを使用して、この ASBR とピア ASBR で Inter-AS オプション AB 接続が必要な追加の VPN を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family ipv4**
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. Inter-AS オプション AB+ の場合はステップ 10 に進みます。それ以外の場合はステップ 8 に進みます。
8. **inter-as-hybrid** [**csc**]
9. **inter-as-hybrid** [**csc**] [**next-hop***ip-address*]
10. **inter-as-hybrid next-hop global**
11. **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。 • 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： `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	**vrf definition***vrf-name* 例： `Router(config)# vrf definition vpn1`	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。

	コマンドまたはアクション	目的

ステップ 4	**rd***route-distinguisher*
	
	例：
	
	`Router(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。RD 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：101:3 などの 32 ビット数値
		
		  • 32 ビットの IP アドレス:16 ビットの番号。192.168.122.15:1 など。

ステップ 5	**address-family ipv4** 例： `Router(config-vrf)# address-family ipv4`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf-af)# route-target import 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、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	Inter-AS オプション AB+ の場合はステップ 10 に進みます。それ以外の場合はステップ 8 に進みます。	—
ステップ 8	**inter-as-hybrid** [**csc**] 例： `Router(config-vrf-af)# inter-as-hybrid`	VRF をオプション AB VRF として指定します。これには次のような効果があります。 • この VRF にインポートされるルートは、オプション AB ピアと VPNv4 iBGP ピアにアドバタイズできます。

	コマンドまたはアクション	目的
		• オプション AB ピアからルートを受信し、そのルートが VRF にインポートされると、そのルートのネクスト ホップ テーブル ID が VRF のテーブル ID に設定されます。 • **csc** キーワードを使用しない場合、インポートされたルートに対し VRF 単位のラベルが割り当てられます。 • **csc** キーワードを使用する場合、オプション AB ピアからルートを受信し、そのルートが VRF に次にインポートされた場合、学習されたラベルは転送時にのみインストール可能です。 **csc** キーワードを使用する場合、次のようになります。 • インポートされたルートに対してプレフィックス単位のラベルが割り当てられます。 • オプション AB ピアから受信し、VRF にインポートされたルートの場合、学習されたラベルが転送時にインストールされます。

ステップ 9	**inter-as-hybrid** [**csc**] [**next-hop***ip-address*]
	
	例：
	
	`Router(config-vrf-af)# inter-as-hybrid next-hop 192.168.1.0`
		（任意）VRF にインポートされ、オプション AB ピアから受信したパスに設定するネクスト ホップ IP アドレスを指定します。
		• ネクスト ホップ コンテキストも、これらのパスをインポートした VRF に設定されます。
		• **csc** キーワードを使用する場合、次のようになります。
		  • インポートされたルートに対してプレフィックス単位のラベルが割り当てられます。
		  • オプション AB ピアから受信し、VRF にインポートされたルートの場合、学習されたラベルが転送時にインストールされます。

ステップ 10	**inter-as-hybrid next-hop global** 例： `Router(config-vrf-af)# inter-as-hybrid next-hop global`	（オプション AB+）Inter-AS オプション AB+ を有効にします。 • VRF にインポートされたパスと、オプション AB+ ピアから受信したパスに設定する、BGP アップデートのネクスト ホップ アドレスを、グローバル ルーティング テーブルに格納することを指定します。 • 使用されるアドレスは、外部 BGP（eBGP）グローバル共有リンクのリモート エンドにあるインターフェイスのアドレスです。ネクストホップ コンテキストはグローバルとして維持され、インポート VRF のコンテキストには変更されません。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(config-vrf-af)# end`	（オプション）終了して、特権 EXEC モードに戻ります。

Inter-AS オプション A 配置からオプション AB 配置への変更

オプション A 配置では、VRF インスタンスは ASBR ルータ間でバックツーバックであり、異なる自律システムの PE ルータが直接接続されています。PE ルータは複数の物理または論理インターフェイスによって接続され、各インターフェイスは特定の VPN に関連しています（VRF インスタンスを通して）。

オプション AB 配置では、グローバル ルーティング テーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムが相互接続され、コントロールプレーン トラフィックが伝送されます。

MPLS VPN Inter-AS オプション A 配置からオプション AB 配置へ変更するには、次の手順を実行します。

1. ASBR で MP-BGP セッションを設定します。特定の VPN のルートをその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、BGP マルチプロトコル拡張を使用して IPv4 以外のアドレス ファミリのサポートが定義されます。設定の詳細については、ASBR ピア間での MP-BGP セッションの設定, （90 ページ）を参照してください。
2. オプション A からのアップグレードが必要な VRF を特定し、**inter-as-hybrid** コマンドを使用してこれらの VRF をオプション AB に対して設定します。設定の詳細については、Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定, （93 ページ）を参照してください。
3. eBGP（ピア ASBR）ネイバーの設定を削除するには、この項の次の手順に従います。
4. 追加 eBGP（ピア ASBR）ネイバーの設定を削除するには、次の手順のステップをすべて繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4 vrf***vrf-name*
5. **no neighbor** {*ip-address* | *peer-group-name*}
6. **exit-address-family**
7. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータでルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4 vrf***vrf-name* 例： `Router(config-router)# address-family ipv4 vrf vpn4`	特定の VPN のルートをその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、ASBR の MP-BGP セッションで識別される各 VRF を設定します。 • アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。
ステップ 5	**no neighbor** {*ip-address* | *peer-group-name*} 例： `Router(config-router-af)# no neighbor 192.168.0.1`	ネイバー eBGP（ASBR）ルータとの情報交換のための設定が削除されます。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 6	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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 7	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

MPLS VPN--Inter-AS オプション AB の設定例

ここでは、Inter-AS AB 機能を使用する 2 つの ASBR ピア間での標準および CSC MPLS VPN 設定について説明します。

例：Inter-AS AB ネットワーク設定

次に、重複しない IP アドレスを使用する Inter-AS オプション AB ネットワークの設定例を示します。

例：CE1

```
!
ip cef distributed
!
interface lo0
 ip address 192.168.13.13 255.255.255.255
 no shutdown
!
interface et4/0
 ip address 192.168.36.1 255.255.255.0
 no shutdown
!
router ospf 300
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface et4/0
 network 192.168.13.13 0.0.0.0 area 300
!
router bgp 300
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.36.2 remote-as 100
 neighbor 192.168.36.2 advertisement-interval 5
 address-family ipv4 no auto-summary
 redistribute connected
 neighbor 192.168.36.2 activate
```

例：CE2

```
!
ip cef distributed
!
interface lo0
 ip address 192.168.14.14 255.255.255.255
 no shutdown
!
interface et1/6
 ip address 192.168.37.1 255.255.255.0
 no ipv6 address
 no shutdown
!
router ospf 400
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface et1/6
 network 192.168.14.14 0.0.0.0 area 400
!
router bgp 400
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.0.2 remote-as 100
 neighbor 192.168.0.2 advertisement-interval 5
 address-family ipv4  no auto-summary
 redistribute connected
 neighbor 192.168.0.2 activate
!
```

例：PE1

```
!
ip cef distributed
!
ip vrf vpn1
   rd 100:1
   route-target import 100:1
   route-target import 200:1
   route-target export 100:1
!
ip vrf vpn2
   rd 100:2
   route-target import 100:2
   route-target import 200:2
   route-target export 100:2
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
 ip address 192.168.17.17 255.255.255.255
 no shutdown
!
interface gi3/1
 ip vrf forwarding vpn1
 ip address 192.168.36.2 255.255.255.0
 no shutdown
!
```

```
interface gi3/8
 mpls ip
 mpls label protocol ldp
 ip address 192.168.31.2 255.255.255.0
!
interface gi3/10
 mpls ip
 mpls label protocol ldp
 ip address 192.168.40.1 255.255.255.0
 no shutdown
!
interface gi3/13
 ip vrf forwarding vpn2
 ip address 192.168.0.2 255.0.0.0
 no shutdown
!
router ospf 100
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface gi3/1
 passive-interface gi3/13
 network 192.168.0.0 0.0.255.255 area 10
 network 192.168.17.17 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 no synchronization
 neighbor 192.168.19.19 remote-as 100
 neighbor 192.168.19.19 update-source Loopback0
 address-family ipv4 vrf vpn1
no auto-summary
 redistribute connected
 neighbor 192.168.36.1 remote-as 300
 neighbor 192.168.36.1 activate
 neighbor 192.168.36.1 advertisement-interval 5
 address-family ipv4 vrf vpn2  no auto-summary
 redistribute connected
 neighbor 192.168.37.1 remote-as 400
 neighbor 192.168.37.1 activate
 neighbor 192.168.37.1 advertisement-interval 5
 address-family vpnv4
 bgp scan-time import 5
 neighbor 192.168.19.19 activate
 neighbor 192.168.19.19 send-community extended
!
```

例：ルート リフレクタ 1

```
!
ip cef distributed
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls ip
mpls label protocol ldp
!
interface lo0
 ip address 192.168.19.19 255.255.255.255
 no shutdown
!
interface gi3/3
 mpls ip
 mpls label protocol ldp
```

```
 ip address 192.168.40.2 255.255.255.0
 no shutdown
!
router ospf 100
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 network 192.168.19.19 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100 !
router bgp 100
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.11.11 remote-as 100
 neighbor 192.168.11.11 update-source Loopback0
 neighbor 192.168.17.17 remote-as 100
 neighbor 192.168.17.17 update-source Loopback0
 neighbor 192.168.11.11 route-reflector-client
 address-family ipv4
 no neighbor 192.168.17.17 activate
 neighbor 192.168.11.11 route-reflector-client
 address-family vpnv4
 bgp scan-time import 5
 neighbor 192.168.11.11 activate
 neighbor 192.168.11.11 send-community extended
 neighbor 192.168.17.17 activate
 neighbor 192.168.17.17 send-community extended
 neighbor 192.168.11.11 route-reflector-client
 neighbor 192.168.17.17 route-reflector-client
!
```

例：ASBR1

```
!
ip cef distributed
!
ip vrf vpn1
   rd 100:1
   route-target import 100:1
   route-target import 200:1
   route-target export 100:1
   inter-as-hybrid next-hop 192.168.32.2
exit
ip vrf vpn2
   rd 100:2
   route-target import 100:2
   route-target import 200:2
   route-target export 100:2
   inter-as-hybrid next-hop 192.168.33.2
exit
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
 mpls ip
 mpls label protocol ldp
interface lo0
 ip address 192.168.11.11 255.255.255.255
 no ipv6 address
ip route-cache distributed
ip route-cache cef distributed
no shutdown
interface gi3/8
mpls ip
 mpls label protocol ldp
 ip address 192.168.13.1 255.255.255.0
 no ipv6 address
ip route-cache distributed
ip route-cache cef distributed
```

```
no shutdown
interface gi3/10
   ip vrf forwarding vpn1
 ip address 192.168.32.1 255.255.255.0
 no ipv6 address
ip route-cache distributed
ip route-cache cef distributed
no shutdown
interface gi3/11
   ip vrf forwarding vpn2
 ip address 192.168.33.1 255.255.255.0
 no ipv6 address
ip route-cache distributed
ip route-cache cef distributed
no shutdown
interface gi3/46
 ip address 192.168.34.1 255.255.255.0
 no ipv6 address
ip route-cache distributed
ip route-cache cef distributed
no shutdown
router ospf 100
nsf enforce global
 redistribute connected subnets
auto-cost reference-bandwidth 1000
passive-interface gi3/10
passive-interface gi3/11
passive-interface gi3/46
network 192.168.0.0 0.0.255.255 area 100
network 192.168.11.11 0.0.0.0 area 100

router bgp 100
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 no bgp default route-target filter
 bgp router-id 192.168.11.11
 neighbor 192.168.34.2 remote-as 200
 neighbor 192.168.34.2 advertisement-interval 5
 neighbor 192.168.19.19 remote-as 100
 neighbor 192.168.19.19 update-source Loopback0
 address-family ipv4
  no auto-summary
 address-family ipv4 vrf vpn1
  no auto-summary
 address-family ipv4 vrf vpn2
  no auto-summary
 address-family vpnv4
  bgp scan-time import 5
  neighbor 192.168.34.2 activate
  neighbor 192.168.34.2 send-community both
  neighbor 192.168.34.2 inter-as-hybrid
  neighbor 192.168.19.19 activate
  neighbor 192.168.19.19 send-community extended !
ip route vrf vpn1 192.168.12.12 255.255.255.255 gi3/10 192.168.32.2
ip route vrf vpn2 192.168.12.12 255.255.255.255 gi3/11 192.168.33.2
!
```

例：ASBR 3

```
!
ip cef distributed
!
ip vrf vpn1
   rd 200:1
   route-target import 100:1
   route-target import 200:1
   route-target export 200:1
   inter-as-hybrid next-hop 192.168.32.1
```

```
!
ip vrf vpn2
   rd 200:2
   route-target import 100:2
   route-target import 200:2
   route-target export 200:2
   inter-as-hybrid next-hop 192.168.33.1
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
 ip address 192.168.12.12 255.255.255.255
 no shutdown
!
interface po2/1/0
 mpls ip
 mpls label protocol ldp
 ip address 192.168.35.1 255.255.255.0
 crc 16
 clock source internal
 no shutdown
!
interface gi3/10
 ip vrf forwarding vpn1
 ip address 192.168.32.2 255.255.255.0
 no shutdown
!
interface gi3/11
 ip vrf forwarding vpn2
 ip address 192.168.33.2 255.255.255.0
 no shutdown
!
interface gi3/45
 ip address 192.168.34.2 255.255.255.0
 no shutdown
!
router ospf 200
nsf enforce global
redistribute connected subnets
auto-cost reference-bandwidth 1000
passive-interface gi3/10
passive-interface gi3/11
passive-interface gi3/45
network 192.168.0.0 0.0.255.255 area 200 network 192.168.12.12 0.0.0.0 area 200

router bgp 200
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 no bgp default route-target filter
 bgp router-id 192.168.12.12
 neighbor 192.168.34.1 remote-as 100
 neighbor 192.168.34.1 advertisement-interval 5
 neighbor 192.168.20.20 remote-as 200
 neighbor 192.168.20.20 update-source Loopback0
 address-family ipv4
 no auto-summary
 address-family ipv4 vrf vpn1
  no auto-summary
 address-family ipv4 vrf vpn2
  no auto-summary
 address-family vpnv4
  bgp scan-time import 5
  neighbor 192.168.34.1 activate
  neighbor 192.168.34.1 send-community both
  neighbor 192.168.34.1 inter-as-hybrid
  neighbor 192.168.20.20 activate
```

```
  neighbor 192.168.20.20 send-community extended !
ip route vrf vpn1 192.168.11.11 255.255.255.255 gi3/10 192.168.32.1
ip route vrf vpn2 192.168.11.11 255.255.255.255 gi3/11 192.168.33.1
!
```

例：PE2

```
!
ip cef distributed
!
ip vrf vpn1
   rd 200:1
   route-target import 100:1
   route-target import 200:1
   route-target export 200:1
!
ip vrf vpn2
   rd 200:2
   route-target import 100:2
   route-target import 200:2
   route-target export 200:2
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
 ip address 192.168.18.18 255.255.255.255
 no shutdown
!
interface po1/0/0
 mpls ip
 mpls label protocol ldp
 ip address 192.168.35.2 255.255.255.0
 crc 16
 clock source internal
 no shutdown
!
interface gi3/2
 ip vrf forwarding vpn1
 ip address 192.168.38.2 255.255.255.0
 no shutdown
!
interface gi3/8
 mpls ip
 mpls label protocol ldp
 ip address 192.168.4.1 255.255.255.0
 no shutdown
!
interface gi3/10
 ip vrf forwarding vpn2
 ip address 192.168.39.2 255.255.255.0
 no shutdown
!
router ospf 200
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface gi3/10
 passive-interface gi3/2
 network 192.168.0.0 0.0.255.255 area 200
 network 192.168.18.18 0.0.0.0 area 200
 network 192.168.0.0 0.0.255.255 area 200 !
 router bgp 200
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
```

```
 no bgp default ipv4-unicast
 no synchronization
 neighbor 192.168.20.20 remote-as 200
 neighbor 192.168.20.20 update-source Loopback0
 address-family ipv4 vrf vpn1
    no auto-summary
    redistribute connected
    neighbor 192.168.38.1 remote-as 500
    neighbor 192.168.38.1 activate
    neighbor 192.168.38.1 advertisement-interval 5
 address-family ipv4 vrf vpn2
    no auto-summary
    redistribute connected
    neighbor 192.168.9.1 remote-as 600
    neighbor 192.168.9.1 activate
    neighbor 192.168.9.1 advertisement-interval 5
 address-family vpnv4
    bgp scan-time import 5
    neighbor 192.168.20.20 activate
    neighbor 192.168.20.20 send-community extended
!
```

例：CE3

```
!
ip cef distributed
!
interface lo0
 ip address 192.168.15.15 255.255.255.255
 no shutdown
!
interface gi0/2
 ip address 192.168.38.1 255.255.255.0
 no shutdown
!
router ospf 500
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface gi0/2
 network 192.168.15.15 0.0.0.0 area 500
!
router bgp 500
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.38.2 remote-as 200
 neighbor 192.168.38.2 advertisement-interval 5
 address-family ipv4
 no auto-summary
 redistribute connected
 neighbor 192.168.38.2 activate
!
```

例：CE4

```
!
ip cef distributed
!
interface lo0
 ip address 192.168.16.16 255.255.255.255
 no shutdown
!
interface et6/2
 ip address 192.168.9.1 255.255.255.0
```

```
 no shutdown
!
router ospf 600
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface et6/2
 network 192.168.16.16 0.0.0.0 area 600
!
router bgp 600
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.39.2 remote-as 200
 neighbor 192.168.39.2 advertisement-interval 5
 address-family ipv4  no auto-summary
 redistribute connected
 neighbor 192.168.39.2 activate
!
```

例：Inter-AS AB CSC 設定

次に、CSC を使用した Inter-AS オプション AB ネットワークの設定例を示します。

例：CE1

```
!
ip cef distributed
!
interface Loopback0
 ip address 192.168.20.20 255.255.255.255
!
interface Ethernet3/3
 ip address 192.168.41.2 255.255.255.0
!
!
router bgp 500
 bgp router-id 192.168.20.20
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.4.1 remote-as 300
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.4.1 activate
  neighbor 192.168.4.1 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CE2

```
!
ip cef distributed
!
interface Loopback0
 ip address 192.168.21.21 255.255.255.255
!
interface Ethernet0/0/7
```

```
 ip address 192.168.42.2 255.255.255.0
!
router bgp 600
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart  neighbor 192.168.42.1 remote-as 400
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.42.1 activate
  neighbor 192.168.42.1 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CE3

```
!
ip cef distributed
!
interface Loopback0
 ip address 192.168.22.22 255.255.255.255
!
interface Ethernet6/2
 ip address 192.168.43.2 255.255.255.0
!
router bgp 500
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart neighbor 192.168.43.1 remote-as 300
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.43.1 activate
  neighbor 192.168.43.1 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CE4

```
!
ip cef distributed
!
interface Loopback0
 ip address 192.168.23.23 255.255.255.255
!
!
interface Ethernet0/0/7
 ip address 192.168.44.2 255.255.255.0
!
router bgp 600
 bgp router-id 192.168.23.23
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
neighbor 192.168.44.1 remote-as 400
 !
 address-family ipv4
  redistribute connected
  neighbor 192.168.44.1 activate
```

```
  neighbor 192.168.44.1 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：PE1

```
!
ip cef distributed
!
ip vrf vpn3
 rd 300:3
 route-target export 300:3
 route-target import 300:3
!
mpls ldp graceful-restart
!
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.192.10 255.255.255.255
!
interface Ethernet3/1
 ip vrf forwarding vpn3
 ip address 192.168.4.1 255.255.255.0
!
interface Ethernet5/3
 ip address 192.168.3.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 network 192.168.192.10 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
!
router bgp 300
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.19.19 remote-as 300
 neighbor 192.168.19.19 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.19.19 activate
  neighbor 192.168.19.19 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn3
  redistribute connected
  neighbor 192.168.41.2 remote-as 500
  neighbor 192.168.41.2 activate
  neighbor 192.168.41.2 as-override
  neighbor 192.168.41.2 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CSC-CE1

```
!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.11.11 255.255.255.255
!
!
interface Ethernet3/4
 ip address 192.168.30.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 300 metric 3 subnets
 passive-interface FastEthernet1/0
 network 192.168.11.11 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
 distance ospf intra-area 19 inter-area 19
!
router bgp 300
 bgp router-id 192.168.11.11
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.13.1 remote-as 100
 !
 address-family ipv4
  redistribute ospf 300 metric 4 match internal external 1 external 2
  neighbor 192.168.13.1 activate
  neighbor 192.168.13.1 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CSC-PE1

```
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 100:5
 route-target import 200:1
!
ip vrf vpn2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 route-target import 100:6
 route-target import 200:2
!
mpls ldp graceful-restart
mpls label protocol ldp
```

```
!
mpls ip
!
interface Loopback0
 ip address 192.168.12.12 255.255.255.255
!
!
interface FastEthernet4/0/0
 ip address 192.168.34.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet4/0/1
 ip vrf forwarding vpn1
 ip address 192.168.13.1 255.255.255.0
 mpls bgp forwarding
!
!
interface FastEthernet4/1/0
 ip vrf forwarding vpn2
 ip address 192.168.33.1 255.255.255.0
 mpls bgp forwarding
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.12.12 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
 bgp router-id 192.168.12.12
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.15.15 remote-as 100
 neighbor 192.168.15.15 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.15.15 activate
  neighbor 192.168.15.15 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn2
  neighbor 192.168.33.2 remote-as 400
  neighbor 192.168.33.2 update-source FastEthernet4/1/0
  neighbor 192.168.33.2 activate
  neighbor 192.168.33.2 as-override
  neighbor 192.168.33.2 advertisement-interval 5
  neighbor 192.168.33.2 send-label
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
  neighbor 192.168.31.2 remote-as 300
  neighbor 192.168.31.2 update-source FastEthernet4/0/1
  neighbor 192.168.31.2 activate
  neighbor 192.168.31.2 as-override
  neighbor 192.168.31.2 advertisement-interval 5
  neighbor 192.168.31.2 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：PE 2

```
ip cef distributed
!
ip vrf vpn4
 rd 400:4
 route-target export 400:4
 route-target import 400:4
!
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.13.13 255.255.255.255
!
!
interface Ethernet4/1/2
 ip vrf forwarding vpn4
 ip address 192.168.42.1 255.255.255.0
!
!
interface Ethernet4/1/6
 ip address 192.168.32.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.13.13 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
 bgp router-id 192.168.13.13
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.25.25 remote-as 400
 neighbor 192.168.25.25 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.25.25 activate
  neighbor 192.168.25.25 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn4
  redistribute connected
  neighbor 192.168.42.2 remote-as 600
  neighbor 192.168.42.2 activate
  neighbor 192.168.42.2 as-override
  neighbor 192.168.42.2 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CSC-CE2

```
!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
interface Loopback0
 ip address 192.168.14.14 255.255.255.255
!
!
interface GigabitEthernet8/16
 ip address 192.168.33.2 255.255.255.0
 mpls bgp forwarding
!
!
interface GigabitEthernet8/24
 ip address 192.168.32.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 redistribute bgp 400 metric 3 subnets
 passive-interface GigabitEthernet8/16
 network 192.168.14.14 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
 distance ospf intra-area 19 inter-area 19
!
router bgp 400
 bgp router-id 192.168.14.14
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.33.1 remote-as 100
 !
 address-family ipv4
  no synchronization
  redistribute connected
  redistribute ospf 400 metric 4 match internal external 1 external 2
  neighbor 192.168.33.1 activate
  neighbor 192.168.33.1 advertisement-interval 5
  neighbor 192.168.33.1 send-label
  no auto-summary
 exit-address-family
!
```

例：ASBR1

```
!
ip vrf vpn5
 rd 100:5
 route-target export 100:5
 route-target import 100:5
 route-target import 100:1
 route-target import 200:5
 inter-as-hybrid csc next-hop 192.168.35.2
!
```

```
ip vrf vpn6
 rd 100:6
 route-target export 100:6
 route-target import 100:6
 route-target import 100:2
 route-target import 200:6
 inter-as-hybrid csc next-hop 192.168.36.2
!
mpls ldp graceful-restart
mpls label protocol ldp
!
!
interface Loopback0
 ip address 192.168.15.15 255.255.255.255
!
interface GigabitEthernet2/3
 ip vrf forwarding vpn5
 ip address 192.168.35.1 255.255.255.0
 mpls bgp forwarding
!
interface GigabitEthernet2/4
 ip vrf forwarding vpn6
 ip address 192.168.36.1 255.255.255.0
 mpls bgp forwarding
!
!
interface GigabitEthernet2/5
 ip address 192.168.34.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
interface GigabitEthernet2/16
 ip address 192.168.37.1 255.255.255.0
 mpls bgp forwarding
!
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.15.15 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
 bgp router-id 192.168.15.15
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.12.12 remote-as 100
 neighbor 192.168.12.12 update-source Loopback0
 neighbor 192.168.0.2 remote-as 200
 neighbor 192.168.0.2 disable-connected-check
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.12.12 activate
  neighbor 192.168.12.12 send-community extended
  neighbor 192.168.0.2 activate
  neighbor 192.168.0.2 send-community extended
  neighbor 192.168.0.2 inter-as-hybrid
 exit-address-family
 !
 address-family ipv4 vrf vpn5
  no synchronization
```

```
 exit-address-family
 !
 address-family ipv4 vrf vpn6
  no synchronization
 exit-address-family
!
ip route 192.168.16.16 255.255.255.255 GigabitEthernet2/16 192.168.0.2
ip route vrf vpn5 192.168.16.16 255.255.255.255 GigabitEthernet2/3 192.168.35.2
ip route vrf vpn6 192.168.16.16 255.255.255.255 GigabitEthernet2/4 192.168.36.2
!
ip vrf vpn5
 rd 200:5
 route-target export 200:5
 route-target import 200:5
 route-target import 200:1
 route-target import 100:1
 route-target import 100:5
 inter-as-hybrid csc next-hop 192.168.35.1
!
ip vrf vpn6
 rd 200:6
 route-target export 200:6
 route-target import 200:6
 route-target import 200:2
 route-target import 100:2
 route-target import 100:6
 inter-as-hybrid csc next-hop 192.168.36.1
!
mpls ldp graceful-restart
mpls label protocol ldp
!
!
interface Loopback0
 ip address 192.168.16.16 255.255.255.255
!
!
interface GigabitEthernet3/1
 ip vrf forwarding vpn5
 ip address 192.168.35.2 255.255.255.0
 mpls bgp forwarding
!
interface GigabitEthernet3/2
 ip vrf forwarding vpn6
 ip address 192.168.36.2 255.255.255.0
 mpls bgp forwarding
!      !
interface GigabitEthernet3/14
 ip address 192.168.0.2 255.0.0.0
 mpls bgp forwarding
!
interface GigabitEthernet3/15
 ip address 192.168.38.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.16.16 0.0.0.0 area 200
 network 192.168.0.0 0.0.255.255 area 200
!
router bgp 200
 bgp router-id 192.168.16.16
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.17.17 remote-as 200
 neighbor 192.168.17.17 update-source Loopback0
```

```
 neighbor 192.168.37.1 remote-as 100
 neighbor 192.168.37.1 disable-connected-check
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.17.17 activate
  neighbor 192.168.17.17 send-community extended
  neighbor 192.168.37.1 activate
  neighbor 192.168.37.1 send-community extended
  neighbor 192.168.37.1 inter-as-hybrid
 exit-address-family
 !
 address-family ipv4 vrf vpn5
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn6
  no synchronization
 exit-address-family
!
ip route 192.168.15.15 255.255.255.255 GigabitEthernet3/14 192.168.37.1
ip route vrf vpn5 192.168.15.15 255.255.255.255 GigabitEthernet3/1 192.168.35.1
ip route vrf vpn6 192.168.15.15 255.255.255.255 GigabitEthernet3/2 192.168.36.1
!
```

例：CSC-PE 3

```
ip vrf vpn1
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 route-target import 200:5
 route-target import 100:1
!
ip vrf vpn2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 route-target import 200:6
 route-target import 100:2
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.17.17 255.255.255.255
!
interface FastEthernet4/0/2
 ip vrf forwarding vpn2
 ip address 192.168.5.1 255.255.255.0
 mpls bgp forwarding
!
!
interface FastEthernet4/0/4
 ip vrf forwarding vpn1
 ip address 192.168.9.1 255.255.255.0
 mpls bgp forwarding
!
!
interface FastEthernet4/0/7
 ip address 192.168.38.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
```

```
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.17.17 0.0.0.0 area 200
 network 192.168.0.0 0.0.255.255 area 200
!
router bgp 200
 bgp router-id 192.168.17.17
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.16.16 remote-as 200
 neighbor 192.168.16.16 update-source Loopback0
 !
 address-family vpnv4
  neighbor 192.168.16.16 activate
  neighbor 192.168.16.16 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn2
  neighbor 192.168.55.0 remote-as 400
  neighbor 192.168.55.0 update-source FastEthernet4/0/2
  neighbor 192.168.55.0 activate
  neighbor 192.168.55.0 as-override
  neighbor 192.168.55.0 advertisement-interval 5
  neighbor 192.168.55.0 send-label
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
  neighbor 192.168.39.2 remote-as 300
  neighbor 192.168.39.2 update-source FastEthernet4/0/4
  neighbor 192.168.39.2 activate
  neighbor 192.168.39.2 as-override
  neighbor 192.168.39.2 advertisement-interval 5
  neighbor 192.168.39.2 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CSC-CE3

```
!
interface Loopback0
 ip address 192.168.18.18 255.255.255.255
!
!
interface Ethernet3/3
 ip address 192.168.40.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
interface FastEthernet5/0
 ip address 192.168.39.2 255.255.255.0
 mpls bgp forwarding
!
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 300 metric 3 subnets
```

```
 network 192.168.18.18 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
 distance ospf intra-area 19 inter-area 19
!
router bgp 300
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.9.1 remote-as 200
 !
 address-family ipv4
  redistribute connected
  redistribute ospf 300 metric 4 match internal external 1 external 2
  neighbor 192.168.9.1 activate
  neighbor 192.168.9.1 advertisement-interval 5
  neighbor 192.168.9.1 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
```

例：CSC-CE 4

```
!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.24.24 255.255.255.255
!
!
interface FastEthernet1/1
 ip address 192.168.55.0 255.255.255.0
 mpls bgp forwarding
!
!
interface Ethernet3/5
 ip address 192.168.56.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 400 metric 3 subnets
 network 192.168.24.24 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
 bgp log-neighbor-changes
 neighbor 192.168.5.1 remote-as 200
 !
 address-family ipv4
  redistribute connected
  redistribute ospf 400 metric 4 match internal external 1 external 2
  neighbor 192.168.5.1 activate
  neighbor 192.168.5.1 advertisement-interval 5
  neighbor 192.168.5.1 send-label
  no auto-summary
  no synchronization
 exit-address-family
```

例：PE 3

```
!
ip cef distributed
!
ip vrf vpn3
 rd 300:3
 route-target export 300:3
 route-target import 300:3
 mpls ip
!
!
mpls ldp graceful-restart
mpls label protocol ldp
!
!
interface Loopback0
 ip address 192.168.19.19 255.255.255.255
!
!
interface Ethernet5/1/1
 ip vrf forwarding vpn3
 ip address 192.168.43.1 255.255.255.0
!
!
interface Ethernet5/1/4
 ip address 192.168.40.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.19.19 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
 network 192.168.0.0 0.0.255.255 area 300
!
router bgp 300
 bgp router-id 192.168.19.19
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.192.10 remote-as 300
 neighbor 192.168.192.10 update-source Loopback0
 !
 address-family ipv4
  no neighbor 192.168.192.10 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.192.10 activate
  neighbor 192.168.192.10 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn3
  neighbor 192.168.43.2 remote-as 500
  neighbor 192.168.43.2 activate
  neighbor 192.168.43.2 as-override
  neighbor 192.168.43.2 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
```

例：PE 4

```
!
ip cef distributed
!
ip vrf vpn4
 rd 400:4
 route-target export 400:4
 route-target import 400:4
!
mpls ldp graceful-restart
mpls ldp protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.25.25 255.255.255.255
!
!
interface Ethernet5/0/4
 ip address 192.168.56.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
interface Ethernet5/0/7
 ip vrf forwarding vpn4
 ip address 192.168.44.1 255.255.255.0
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.25.25 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
 bgp router-id 192.168.25.25
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.13.13 remote-as 400
 neighbor 192.168.13.13 ebgp-multihop 7
 neighbor 192.168.13.13 update-source Loopback0
 !
 address-family ipv4
  no neighbor 192.168.13.13 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.13.13 activate
  neighbor 192.168.13.13 send-community extended
  bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn4
  neighbor 192.168.44.2 remote-as 600
  neighbor 192.168.44.2 activate
  neighbor 192.168.44.2 as-override
  neighbor 192.168.44.2 advertisement-interval 5
  no auto-summary
  no synchronization
 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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS コマンド	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
MPLS VPN	『Configuring MPLS Layer 3 VPNs』
MPLS VPN 相互自律システム	• 『MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses』 • 『MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2283	『*Multiprotocol Extensions for BGP-4*』
RFC 4364	『*BGP/MPLS IP Virtual Private Networks*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN--Inter-AS オプション AB の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：***MPLS VPN--Inter-AS*** オプション ***AB*** の機能情報

機能名	リリース	機能情報
MPLS VPN--Inter-AS オプション AB	12.2(33)SRC 15.0(1)M 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.4	この機能は、Inter-AS オプション 10 A ネットワークと Inter-AS オプション 10 B ネットワークの最良の機能を組み合わせたものです。MPLS VPN サービスプロバイダーは、この機能を使用して、さまざまな自律システムを相互接続して VPN サービスを提供できます。 この機能は、Cisco IOS Release 12.2(33)SRC で導入されました。 この機能は、Cisco IOS Release 15.0(1)M で Cisco 1900、2900、3800、3900 シリーズ ルータに実装されました。 この機能は、Cisco IOS XE Release 2.4 で、Cisco ASR 1000 シリーズ ルータに実装されました。 次のコマンドが導入または変更されました：**neighbor inter-as-hybrid**、**inter-as-hybrid**。

機能名	リリース	機能情報
MPLS VPN--Inter-AS オプション AB+	15.0(1)SY	MPLS VPN--Inter-AS オプション AB+ 機能では、VPN プレフィックスをシグナリングするため、（Inter-AS オプション B に示すように）1 つの BGP セッションを使用して、MPLS VPN—Inter-AS オプション A のスケーラビリティの問題に対処します。Inter-AS AB+ の配置では、ASBR 間の転送接続は VRF 単位で維持され、コントロールプレーン情報が 1 つの Multiprotocol BGP セッションにより交換されます。 この機能は、Cisco IOS Release 15.0(1)SY で導入されました。 次のコマンドが導入または変更されました：**inter-as-hybrid**。

用語集

ASBR：Autonomous System Boundary Router（自律システム境界ルータ）。自律システムを別の自律システムに接続するルータ。

自律システム：共通管理で共通のルーティング方針が共有される、ネットワークの集合。

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとネットワーク到達可能性情報を交換する、ドメイン間ルーティング プロトコル（同じ自律システム内の場合も、複数の自律システム間の場合もあります）。

CE ルータ：カスタマー エッジ ルータ。カスタマー ネットワークに属し、プロバイダー エッジ（PE）ルータとのインターフェイスとなるルータ。CE ルータは、関連する MPLS VPN を認識しません。

CSC：Carrier Supporting Carrier。小規模サービス プロバイダー（カスタマー キャリア）が MPLS バックボーンを経由してそれぞれの IP ネットワークまたは MPLS ネットワークを相互接続できる階層型 VPN モデル。これにより、カスタマー キャリアは独自の MPLS バックボーンを構築および維持する必要がなくなります。

eBGP：external Border Gateway Protocol（外部 Border Gateway Protocol）。異なる自律システムにあるルータ間の BGP。異なる自律システムにある 2 つのルータが互いに 2 ホップ以上離れている場合、これら 2 つのルータ間の eBGP セッションはマルチホップ BGP であると見なされます。

エッジ ルータ：ネットワークのエッジにあるルータ。MPLS ネットワークの境界を定義します。パケットを送受信します。エッジ ラベル スイッチ ルータおよびラベル エッジ ルータとも呼ばれます。

iBGP：internal Border Gateway Protocol（内部ボーダー ゲートウェイ プロトコル）。同じ自律システム内にあるルータ間の BGP。

IGP：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。単一の自律システム内でのルーティング情報の交換に使用されるインターネット プロトコル。インターネット IGP プロトコルの例として、IGRP、OSPF、IS-IS、RIP があります。

IP：Internet Protocol（インターネット プロトコル）。TCP/IP スタックにおいてコネクションレス型のネットワーク間サービスを提供するネットワーク層プロトコル。IP では、アドレッシング、タイプ オブ サービス指定、フラグメンテーションと再編成、セキュリティなどの機能が提供されます。RFC 791 に定義されています。

LDP：Label Distribution Protocol。パケットの転送に使用されるラベル（アドレス）をネゴシエーションするための、MPLS 対応ルータ間の標準プロトコル。

LFIB：Label Forwarding Information Base（ラベル転送情報ベース）。着信ラベルと発信ラベル、および関連する Forward Equivalence Class（FEC）パケットについての情報を保持するために MPLS で使用されるデータ構造。

MP-BGP：Multiprotocol BGP。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベル スイッチングを担当する IETF ワーキング グループの名前、およびそのワーキング グループで標準化されたラベル スイッチング アプローチの名前。

NLRI：Network Layer Reachability Information（ネットワーク層到達可能性情報）。BGP では、ルートおよびそのルートへのアクセス方法を記述した NLRI を含むルーティング アップデート メッセージが送信されます。この場合、NLRI がプレフィックスとなります。BGP アップデート メッセージでは、1 つ以上の NLRI プレフィックス、および NLRI プレフィックスのルートの属性が伝送されます。ルート属性には、BGP ネクスト ホップ ゲートウェイ アドレスおよび拡張コミュニティ値が含まれています。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）によって、ルータは、ルート プロセッサが他のルート プロセッサにテイクオーバーまたはスイッチオーバーされたあとでも継続して IP パケットを転送できます。NSF では、レイヤ 3 のルーティングおよび転送情報をバックアップルートプロセッサに保持および更新することによって、スイッチオーバーやルート収束のプロセス中にも継続して IP パケットおよびルーティングプロトコル情報が転送されることが保証されます。

PE ルータ：プロバイダー エッジ ルータ。サービス プロバイダーのネットワークの一部であるルータ。このルータは、カスタマー エッジ（CE）ルータに接続されます。すべての MPLS VPN 処理は PE ルータで実行されます。

QoS：Quality of Service。転送システムのパフォーマンスを測定したものであり、転送品質およびサービス アベイラビリティを示します。

RD：Route Distinguisher（ルート識別子）。IPv4 プレフィックスに連結される 8 バイトの値で、一意の VPN IPv4 プレフィックスを形成します。

RT：Route Target（ルート ターゲット）。プレフィックスのインポート先となる VRF ルーティング テーブルの識別に使用する拡張コミュニティ属性。

SLA：VPN 加入者に保証されるサービス レベル契約。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。1 つ以上の物理ネットワークのリソースを共有する、セキュアな MPLS ベースのネットワーク（一般的に1 つまたは複数のサービスプロバイダーによって実行されます）。VPNには地理的に分散したサイトが含まれており、共有バックボーン ネットワーク上で安全に通信できるようになっています。

VRF：VPN ルーティングおよび転送（VRF）インスタンス。PE ルータに付加される VPN サイトを定義するルーティング情報。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。

第 5 章

LDP および IGP を使用する MPLS VPN Carrier Supporting Carrier

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）Carrier Supporting Carrier（CSC）を使用すると、MPLS VPN ベースのサービス プロバイダーは、そのバックボーン ネットワークのセグメントを他のサービス プロバイダーが使用できるようにすることができます。この章では、MPLS ラベルを配布するための MPLS ラベル配布プロトコル（LDP）、およびルートを配布するための Interior Gateway Protocol（IGP）を使用する MPLS VPN CSC ネットワークを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

LDP および IGP を使用する MPLS VPN CSC の前提条件

- バックボーン キャリアのプロバイダー エッジ（PE）ルータには、128 MB のメモリが必要です。
- バックボーン キャリアでは、カスタマー エッジ（CE）ルータから PE ルータが受信するパケットに、PE ルータが CE ルータにアドバタイズしたラベルのみが含まれていることを確認するように、PE ルータをイネーブルにする必要があります。これにより、データ スプーフィングを防ぐことができます。データ スプーフィングは、パケットが認識できない IP アドレスからルータに送信された場合に発生します。

LDP および IGP を使用する MPLS VPN CSC の制約事項

この機能では、次の機能がサポートされていません。

- ATM MPLS
- Carrier Supporting Carrier トラフィック エンジニアリング
- Carrier Supporting Carrier Quality of Service（QoS）
- RSVP 集約
- カスタマー キャリアとバックボーン キャリア ネットワーク間の VPN マルチキャスト

次のルータ プラットフォームは、MPLS VPN のエッジでサポートされています。

- Cisco 7200 シリーズ
- Cisco 7500 シリーズ
- Cisco 12000 シリーズ

Cisco IOS リリースに追加された Cisco 12000 シリーズ ラインカードのサポートについては、次の表を参照してください。

表 *5*：*Cisco IOS* リリースに追加された *Cisco 12000* シリーズ ラインカードのサポート

タイプ	ラインカード	追加された Cisco IOS Release
Packet Over Sonet（POS）	4 ポート OC-3 POS 1 ポート OC-12 POS 8 ポート OC-3 POS 16 ポート OC-3 POS 4 ポート OC-12 POS 1 ポート OC-48 POS 4 ポート OC-3 POS ISE 8 ポート OC-3 POS ISE 16 x OC-3 POS ISE 4 ポート OC-12 POS ISE 1 ポート OC-48 POS ISE	12.0(16)ST 12.0(21)ST 12.0(22)S
電気インターフェイス	6 ポート DS3 12 ポート DS3 6 ポート E3	12.0(16)ST 12.0(21)ST
ATM	4 ポート OC-3 ATM 1 ポート OC12 ATM 4 ポート OC-12 ATM	12.0(22)S
チャネライズド インターフェイス	2 ポート CHOC-3 6 ポート Ch T3 (DS1) 1 ポート CHOC-12 (DS3) 1 ポート CHOC-12 (OC-3) 4 ポート CHOC-12 ISE 1 ポート CHOC-48 ISE	12.0(22)S

LDP および IGP を使用する MPLS VPN CSC に関する情報

MPLS VPN CSC の概要

Carrier Supporting Carrier により、サービス プロバイダーは、そのバックボーン ネットワークのセグメントを別のサービス プロバイダーが使用できるようにすることができます。他のプロバイダーにバックボーン ネットワークのセグメントを提供するサービスプロバイダーは、バックボーン キャリアと呼ばれます。バックボーン ネットワークのセグメントを使用するサービス プロバイダーは、カスタマー キャリアと呼ばれます。

バックボーン キャリアは、ボーダー ゲートウェイ プロトコル/マルチプロトコル ラベル スイッチング（BGP/MPLS）VPN サービスを提供します。カスタマー キャリアは、次のいずれかになります。

- インターネット サービス プロバイダー（ISP）
- BGP/MPLS VPN サービス プロバイダー

MPLS VPN CSC の実装の利点

MPLS VPN CSC ネットワークは、バックボーン キャリアであるサービス プロバイダー、およびカスタマー キャリアに対して次の利点をもたらします。

バックボーン キャリアにとっての利点

- バックボーン キャリアは、多数のカスタマー キャリアに対応し、そのバックボーンにカスタマー キャリアがアクセスできるようにします。バックボーン キャリアは、それぞれのカスタマー キャリア用に個別のバックボーンを作成および維持する必要はありません。1 つのバックボーン ネットワークを使用して複数のカスタマー キャリアをサポートすると、バックボーン キャリアの VPN 動作が簡略化されます。バックボーン キャリアは、一貫した方法を使用して、バックボーン ネットワークを管理および維持します。この方法は、個々のバックボーンを維持するよりも安価かつ効率的でもあります。
- MPLS VPN Carrier Supporting Carrier 機能は、スケーラブルです。Carrier Supporting Carrier では、帯域幅および接続の変化するニーズに合わせて VPN を変更できます。この機能は、予定外の成長や変更に対応できます。Carrier Supporting Carrier 機能により、同じネットワーク上で何万もの VPN をセットアップでき、サービス プロバイダーは VPN サービスとインターネット サービスの両方を提供できます。
- MPLS VPN Carrier Supporting Carrier 機能は、柔軟なソリューションです。バックボーン キャリアは、多くのタイプのカスタマー キャリアに対応できます。バックボーン キャリアは、ISP であるカスタマー キャリアおよび VPN サービス プロバイダーであるカスタマー キャリアのいずれかまたは両方を受け入れることができます。バックボーンキャリアは、セキュリティおよびさまざまな帯域幅を必要とするカスタマー キャリアに対応できます。

カスタマー キャリアにとっての利点

- MPLS VPN Carrier Supporting Carrier 機能により、カスタマー キャリアでは、独自のバックボーンを設定、運用、および維持する必要がなくなります。カスタマーキャリアは、バックボーン キャリアのバックボーン ネットワークを使用しますが、ネットワークのメンテナンスと運用はバックボーン キャリアが担当します。
- バックボーン キャリアが提供する VPN サービスを使用するカスタマー キャリアには、フレーム リレーまたは ATM ベースの VPN が提供するのと同じレベルのセキュリティがもたらされます。また、カスタマー キャリアは VPN で IPSec を使用することにより、より高いレベルのセキュリティを確保できます。これは、バックボーン キャリアにとっては完全に透過的です。
- カスタマー キャリアは、任意のリンク層テクノロジー（SONET、DSL、フレーム リレーなど）を使用して、CE ルータを PE ルータに接続し、PE ルータを P ルータに接続します。MPLS VPN Carrier Supporting Carrier 機能は、リンク層とは独立しています。CE ルータと PE ルータは IP を使用して通信し、バックボーン キャリアは MPLS を使用します。
- カスタマー キャリアは、任意のアドレッシング方式を使用でき、バックボーン キャリアによるサポートを引き続き受けることができます。カスタマーのアドレス空間およびルーティング情報は、他のカスタマー キャリアまたはバックボーン プロバイダーのアドレス空間およびルーティング情報とは独立しています。

LDP および IGP を使用する MPLS VPN CSC の設定オプション

バックボーン キャリアは、BGP サービスと MPLS VPN サービスを提供します。カスタマー キャリアは、ここで説明する 2 つのタイプのサービス プロバイダーのいずれかになります。ここでは、バックボーン キャリアとカスタマー キャリアが IPv4 ルートと MPLS ラベルを配布する方法について説明します。

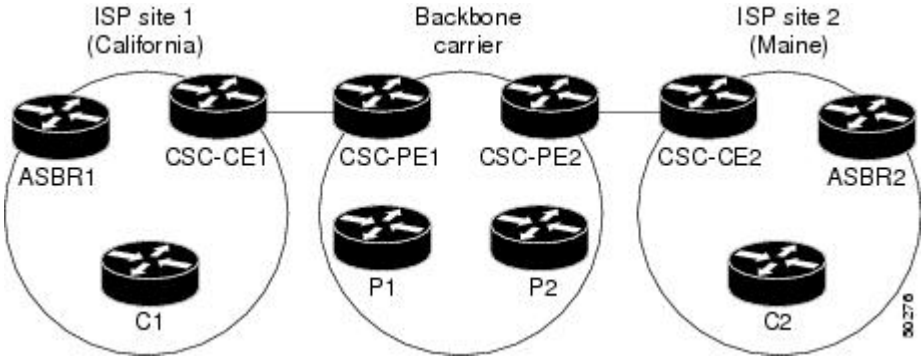
カスタマー キャリアが ISP である場合

この項では、BGP/MPLS VPN サービス プロバイダー（バックボーン キャリア）が、そのバックボーン ネットワークのセグメントを ISP であるカスタマーに提供する方法について説明します。

次の例について考えてみます。

ISP には 2 つのサイトがあります。1 つはカリフォルニア州に、もう 1 つはメイン州にあります。各サイトは、Point of Presence（POP）です。ISP は、バックボーン キャリアが提供する VPN サービスを使用してこれらのサイトを接続しようと考えています。次の図に、この状況を示します。

図 *11*：*ISP* をサポートするサンプル *BGP/MPLS* バックボーン キャリア



（注） この図の CE ルータは、バックボーン キャリアにとっての CE ルータです。ただし、これらはカスタマー キャリアにとっては PE ルータです。

この例では、バックボーン キャリアのみが MPLS を使用します。カスタマー キャリア（ISP）は IP のみを使用します。そのため、バックボーンキャリアは、カスタマーキャリアのすべてのインターネット ルート（100,000 ルートにもなる可能性があります）を伝送する必要があります。これにより、バックボーン キャリアに関してスケーラビリティの問題が生じる可能性があります。スケーラビリティの問題を解決するには、バックボーン キャリアを次のように設定する必要があります。

- バックボーン キャリアでは、カスタマー キャリアの CE ルータとバックボーン キャリアの PE ルータ間で、カスタマー キャリアの内部ルート（IGP ルート）のみが交換されることを許可します。
- MPLS は、カスタマー キャリアの CE ルータとバックボーン キャリアの PE ルータ間のインターフェイスでイネーブルになっています。

内部ルートと外部ルートは、次の方法で区別されています。

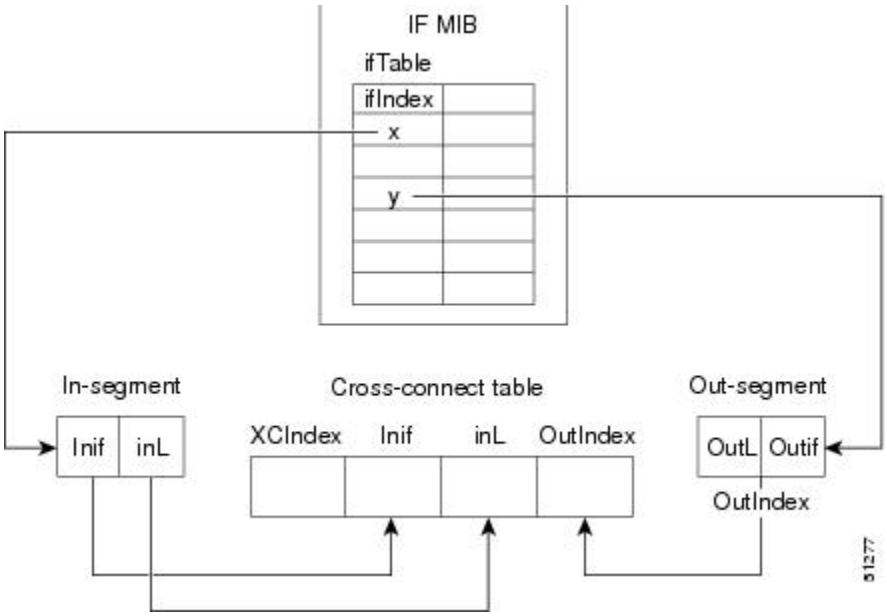
- 内部ルートは、ISP 内のいずれかのルータに進みます。
- 外部ルートはインターネットに進みます。

内部ルートの数は、外部ルートの数よりも大幅に少なくなります。カスタマーキャリアの CE ルータとバックボーン キャリアの PE ルータ間のルートを制限すると、PE ルータが維持する必要があるルートの数が大幅に減ります。

PE ルータは、VRF ルーティング テーブル内の外部ルートを伝送する必要がないため、パケット内の着信ラベルを使用して、カスタマー キャリアのインターネット トラフィックを転送できます。MPLS をルータに追加すると、カスタマー キャリアからバックボーン キャリアへのパケット

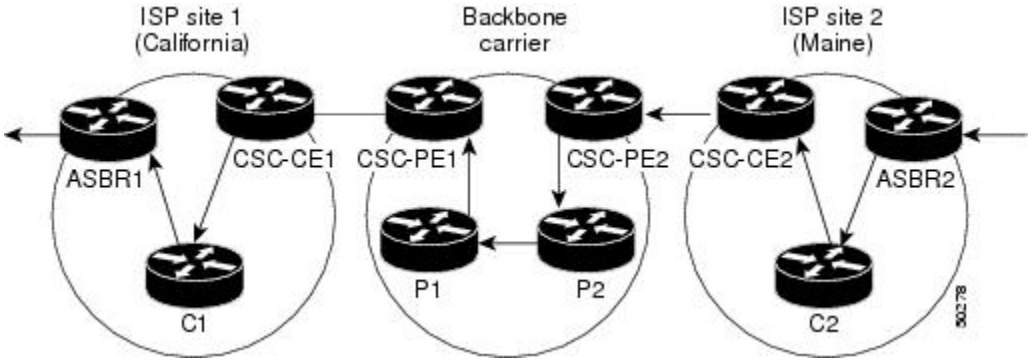
転送を一貫した方法で行うことができます。MPLS により、PE ルータと CE ルータ間で、すべての内部カスタマー キャリア ルートの MPLS ラベルを交換できます。カスタマー キャリアのルータには、インターネットに接続するために、内部ボーダー ゲートウェイ プロトコル（iBGP）またはルート再配布のいずれかを経由するすべての外部ルートが含まれています。次の図に、ネットワークがこの方法で設定されている場合に、情報が交換される方法を示します。

図 *12*：バックボーン キャリアと、*ISP* であるカスタマー キャリアとの間のルーティング情報の交換



次の図では、ルートは、バックボーン キャリアとカスタマー キャリア サイトとの間で作成されています。ASBR2 は、ネットワーク外で生成されたインターネット ルートを受信します。ISP サイトのすべてのルータは、ルータ間の IBGP 接続を介してすべての外部ルートを取得します。

図 *13*：バックボーン キャリアと、*ISP* であるカスタマー キャリアとの間でのルートの確立



次の表に、ルートを確立するプロセスの説明を示します。このプロセスは、次の 2 つの独立した手順に分けられます。

- バックボーン キャリアは、カスタマー キャリアの IGP 情報を伝播します。これにより、カスタマー キャリア ルータは、リモート サイトのすべてのカスタマー キャリア ルータに到達できます。
- 異なるサイト内のカスタマー キャリアのルータに到達可能になると、バックボーン キャリア ルータを使用しないで IBGP を使用して、外部ルートをカスタマー キャリア サイト内で伝播できるようになります。

表 *6* : バックボーン キャリアとカスタマー キャリア *ISP* 間でのルートの確立

ステップ	説明
1	CSC-CE2 は、サイト 2 内の内部ルートを CSC-PE2 に送信します。これらのルートには、ASBR2 へのルートが含まれています。
2	CSC-PE2 は、MPLS VPN プロセスを使用して、サイト 2 から CSC-PE1 にルーティング情報を送信します。CSC-PE1 は、ASBR2 の VPN-IP アドレスへのルートに関連付けられている 1 つのラベル（L3 と呼びます）を取得します。CSC-PE1 は、CSC-PE2 へのルートに関連付けられている別のラベル（L2 と呼びます）を取得します。
3	CSC-PE1 は、内部ルートに関連付けられているルーティング情報をサイト 2 から CSC-CE1 に送信します。CSC-PE1 は、ラベル バインディング情報も送信します。その結果、CSC-CE1 は、ネクスト ホップとして、CSC-PE1 による ASBR2 へのルートを取得します。このルートに関連付けられているラベルを L1 と呼びます。
4	CSC-CE1 は、サイト 1 経由でルーティング情報を配布します。サイト 1 のすべてのルータは、サイト 2 のすべての内部宛先へのルートを取得します。したがって、サイト 1 のすべてのルータは、サイト 2 のルータに到達でき、IBGP を介して外部ルートを学習できます。
5	ASBR2 は、インターネット ルートを受信します。

ステップ	説明
6	IBGP セッションは、インターネットへのルートを含む、ISP の外部ルーティング情報を交換します。サイト 1 のすべてのルータは、ASBR2 をルートのネクストホップとして使用して、インターネットへのルートを認識します。

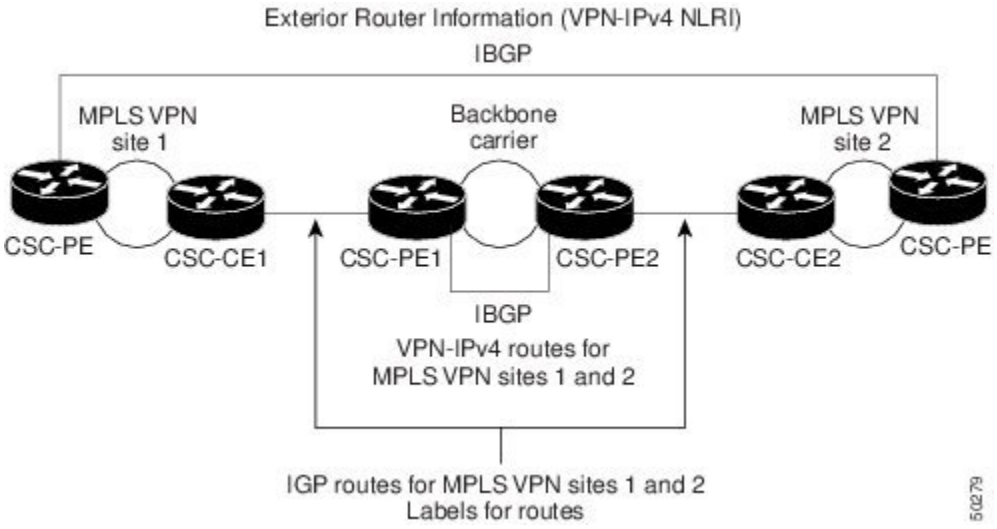
カスタマー キャリアが BGP/MPLS VPN サービス プロバイダーである場合

バックボーン キャリアとカスタマー キャリアの両方が BGP/MPLS VPN サービスを提供する場合、データの転送方式は、カスタマー キャリアが ISP サービスのみを提供する場合とは異なります。次のリストは、これらの相違の重要点を示しています。

- カスタマー キャリアが BGP/MPLS VPN サービスを提供する場合、その外部ルートは VPN-IPv4 ルートです。カスタマー キャリアが ISP である場合、その外部ルートは IP ルートです。
- カスタマー キャリアが BGP/MPLS VPN サービスを提供する場合、カスタマー キャリア内のすべてのサイトは、MPLS を使用する必要があります。カスタマー キャリアが ISP である場合、そのサイトでは MPLS を使用する必要はありません。

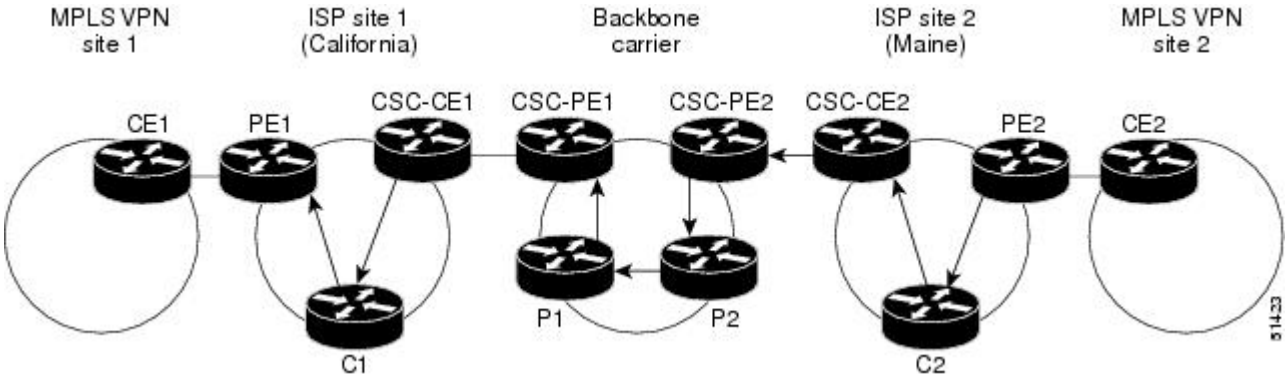
次の図に、MPLS VPN サービスがすべてのカスタマー キャリア サイトおよびバックボーン キャリアに存在する場合の情報の交換方法を示します。

図 *14*：バックボーン キャリアと、*MPLS VPN* サービス プロバイダーであるカスタマー キャリアとの間の情報の交換



次の図の例では、ルートは、バックボーン キャリアとカスタマー キャリア サイトとの間で作成されています。

図 *15*：バックボーン キャリアと、*MPLS VPN* サービス プロバイダーであるカスタマー キャリアとの間でのルートの確立



次の表に、ルートの確立プロセスの説明を示します。

表 *7*：バックボーン キャリアとカスタマー キャリア サイトとの間のルートの確立

ステップ	説明
1	CE2 は、サイト 2 内のすべての内部ルートを CSC-PE2 に送信します。
2	CSC-PE2 は、MPLS VPN プロセスを使用して、サイト 2 から CSC-PE1 にルーティング情報を送信します。CSC-PE1 は、PE2 の VPN-IP アドレスへのルートに関連付けられている 1 つのラベル（L3 と呼びます）を取得します。CSC-PE1 は、CSC-PE2 へのルートに関連付けられている別のラベル（L2 と呼びます）を取得します。
3	CSC-PE1 は、内部ルートに関連付けられているルーティング情報をサイト 2 から CSC-CE1 に送信します。CSC-PE1 は、ラベル バインディング情報も送信します。その結果、CSC-CE1 は、ネクスト ホップとして、CSC-PE1 による PE2 へのルートを取得します。このルートに関連付けられているラベルを L1 と呼びます。

ステップ	説明
4	CE1 は、サイト 1 経由でルーティングとラベル情報を配布します。サイト 1 のすべてのルータは、サイト 2 のすべての内部宛先へのルートを取得します。したがって、PE1 は、PE2 との MP-IBGP セッションを確立できます。
5	CE2 は、MPLS VPN サイト 2 の内部ルートを PE2 にアドバタイズします。
6	PE2 は、MP-IBGP を使用して、すべての VPN ルートのラベルを割り当て（標準の MPLS VPN 機能）、ラベルを PE1 にアドバタイズします。
7	PE1 は、VPN サイト 2 を宛先とする、VPN サイト 1 からのトラフィックを転送できます。

LDP および IGP を使用する MPLS VPN CSC の設定方法

バックボーン キャリア コアの設定

バックボーン キャリア コアの設定では、CSC コアおよび CSC-PE ルータに接続およびルーティング機能を設定する必要があります。

CSC コア（バックボーン キャリア）を設定および確認するには、次の作業を実行します。

前提条件

バックボーン キャリア コアを設定する前に、CSC コア ルータ上で次のプロトコルを設定します。

- IGP ルーティング プロトコル：BGP、OSPF、IS-IS、EIGRP、スタティックなど。詳細については、『Configuring a Basic BGP Network』、『Configuring OSPF』、『Configuring a Basic IS-IS Network』、および『Configuring EIGRP』を参照してください。
- ラベル配布プロトコル（LDP）。詳細については、『MPLS Label Distribution Protocol』を参照してください。

CSC コアにおける IP 接続と LDP 設定の確認

CSC コアにおける IP 接続と LDP 設定を確認するには、次の作業を実行します。この作業の設定例については、CSC コアにおける IP 接続と LDP 設定の確認, （137 ページ）を参照してください。

手順の概要

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**]
5. **show mpls ldp discovery** [**vrf***vrf-name* | **all**]
6. **show mpls ldp neighbor** [[**vrf***vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf***vrf-name*] [*interface*] [**detail**] |**all**]
9. **show ip route**
10. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**ping** [*protocol*] {*host-name* | *system-address*} 例： `Router# ping ip 10.0.0.1`	（任意）AppleTalk、コネクションレス型ネットワーク サービス（CLNS）、IP、Novell、Apollo、VINES、DECnet、または Xerox Network System（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 ip** コマンドを使用して、CSC コア ルータから別の CSC コア ルータへの接続を確認します。
ステップ 3	**trace** [*protocol*] [*destination*] 例： `Router# trace ip 10.0.0.1`	（任意）パケットがその宛先に送信されるときに実際に取るルートを検出します。 • **trace** コマンドを使用して、パケットがその最終的な宛先に到達するまでに通過するパスを確認します。**trace** コマンドは、2 つのルータが通信できない場合に問題のある箇所を分離するのに役立ちます。
ステップ 4	**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels***label* [-*label*] | **interface***interface* | **next-hop***address* |	（任意）MPLS ラベル転送情報ベース（LFIB）の内容を表示します。 • **show mpls forwarding-table** コマンドを使用して、MPLS パケットが転送されていることを確認します。

	コマンドまたはアクション	目的
	lsp-tunnel [*tunnel-id*]] [**vrf***vrf-name*] [**detail**] 例： `Router# show mpls forwarding-table`	
ステップ 5	**show mpls ldp discovery** [**vrf***vrf-name* | **all**] 例： `Router# show mpls ldp discovery`	（任意）LDP ディスカバリ プロセスのステータスを表示します。 • **show mpls ldp discovery** コマンドを使用して、LDP が CSC コアで動作していることを確認します。
ステップ 6	**show mpls ldp neighbor** [[**vrf***vrf-name*] [*address* | *interface*] [**detail**] | **all**] 例： `Router# show mpls ldp neighbor`	（任意）LDP セッションのステータスを表示します。 • **show mpls ldp neighbor** コマンドを使用して、CSC コアにおける LDP 設定を確認します。
ステップ 7	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef`	（任意）転送情報ベース（FIB）のエントリを表示します。 • **show ip cef** コマンドを使用して、転送テーブル（プレフィックス、ネクストホップ、およびインターフェイス）を確認します。
ステップ 8	**show mpls interfaces** [[**vrf***vrf-name*] [*interface*] [**detail**] |**all**] 例： `Router# show mpls interfaces`	（任意）ラベル スイッチングに設定されている 1 つ以上のインターフェイスまたはすべてのインターフェイスに関する情報を表示します。 • **show mpls interfaces** コマンドを使用して、LDP を使用するようにインターフェイスが設定されていることを確認します。
ステップ 9	**show ip route** 例： `Router# show ip route`	（任意）IP ルーティング テーブルのエントリを表示します。 • **show ip route** コマンドを使用して、ホスト IP アドレス、ネクストホップ、インターフェイスを含む、ルーティングテーブル全体を表示します。
ステップ 10	**disable** 例： `Router# disable`	（任意）特権 EXEC モードに戻ります。

トラブルシューティングのヒント

ping コマンドと **trace** コマンドを使用して、コアにおける MPLS 接続の詳細を確認します。さらに **show** コマンドを使用して、有用なトラブルシューティング情報を入手することもできます。

CSC-PE ルータの VRF の設定

VPN ルーティングおよび転送（VRF）インスタンスをバックボーン キャリア エッジ（CSC-PE）ルータに設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map***route-map*
7. **exit**
8. **interface***typenumber*
9. **ip vrf forwarding***vrf-name*
10. **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。 • 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： `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 vpn1`	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。

	コマンドまたはアクション	目的

ステップ 4	**rd***route-distinguisher*
	
	例：
	
	`Router(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。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。192.168.122.15:1 など。

ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target import 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、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 6	**import map***route-map* 例： `Router(config-vrf)# import map vpn1-route-map`	（任意）VRF のインポート ルート マップを設定します。 • *route-map* 引数には、VRF のインポート ルート マップとして使用されるルート マップを指定します。
ステップ 7	**exit** 例： `Router(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。
ステップ 8	**interface***typenumber* 例： `Router(config)# interface Ethernet5/0`	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。

	コマンドまたはアクション	目的
		• *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 9	**ip vrf forwarding***vrf-name* 例： `Router(config-if)# ip vrf forwarding vpn1`	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。
ステップ 10	**end** 例： `Router(config-if)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip vrf detail コマンドを入力し、MPLS VPN が稼働しており、適切なインターフェイスに関連付けられていることを確認します。

バックボーン キャリアにおける VPN 接続の Multiprotocol BGP の設定

バックボーン キャリアでマルチプロトコル BGP（MP-BGP）接続を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source***interface-type*
7. **address-family vpnv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	（任意）IPv4 ユニキャスト アドレス ファミリをすべてのネイバーでディセーブルにします。 • ネイバーを MPLS ルートのみに使用している場合は、**no bgp default-unicast** コマンドを no 形式で使用します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor 10.5.5.5 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **update-source***interface-type* 例： `Router(config-router)# neighbor 10.2.0.0 update-source loopback0`	BGP セッションで、TCP 接続の特定の動作インターフェイスを使用できるようになります。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
		• *interface-type* 引数には、ソースとして使用するインターフェイスを指定します。
ステップ 7	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ 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 プレフィックスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Router(config-router-af)# neighbor 10.0.0.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.4.0.0 activate`	ネイバー BGP ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 10	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip bgp neighbor コマンドを入力すると、ネイバーが稼働中であることを確認できます。このコマンドが成功しなかった場合は、**debug ip bgp***x.x.x.x***events** コマンドを入力します。ここで、*x.x.x.x* はネイバーの IP アドレスです。

CSC-PE ルータと CSC-CE ルータの設定

ルートおよび MPLS ラベルを配布するように、CSC-PE ルータと CSC-CE ルータをイネーブルにするには、次の作業を実行します。

前提条件

CSC-PE ルータと CSC-CE ルータを設定する前に、CSC-PE ルータと CSC-CE ルータで IGP を設定する必要があります。バックボーン キャリアをカスタマー キャリアに接続する PE ルータと CE ルータとの間には、ルーティングプロトコルが必要です。ルーティングプロトコルにより、カスタマー キャリアは IGP ルーティング情報をバックボーン キャリアと交換できます。カスタマー キャリアが使用するのと同じルーティングプロトコルを使用します。ルーティングプロトコルとして、RIP、OSPF、またはスタティック ルーティングを選択できます。BGP はサポートされていません。設定手順については、『Configuring MPLS Layer 3 VPNs』を参照してください。

CSC-PE ルータと CSC-CE ルータでの LDP の設定

バックボーン キャリアをカスタマー キャリアに接続する PE ルータと CE ルータとの間には、MPLS LDP が必要です。LDP をデフォルトのラベル配布プロトコルとして、ルータ全体、または VRF の PE から CE へのインターフェイスのみに設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls label protocol ldp**
4. **interface***typenumber*
5. **mpls label protocol ldp**
6. **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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `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 label protocol ldp** 例： `Router(config)# mpls label protocol`	MPLS LDP をルータのデフォルトのラベル配布プロトコルとして指定します。

	コマンドまたはアクション	目的
	`ldp`	
ステップ 4	**interface***typenumber* 例： `Router(config)# interface Ethernet5/0`	（任意）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 5	**mpls label protocol ldp** 例： `Router(config-if)# mpls label protocol ldp`	（任意）MPLS LDP をインターフェイスのデフォルトのラベル配布プロトコルとして指定します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	（任意）終了して、特権 EXEC モードに戻ります。

CSC-PE ルータと CSC-CE ルータでの MPLS カプセル化の有効化

バックボーン キャリアを通過するすべてのパケットはカプセル化される必要があるため、パケットには MPLS ラベルが含まれています。MPLS カプセル化は、ルータ全体に対してイネーブルにしたり、PE や CE ルータのインターフェイスに対してのみイネーブルにしたりすることができます。パケットのカプセル化をイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **interface***typenumber*
5. **mpls ip**
6. **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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `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 ip** 例： `Router(config)# mpls ip`	ルータの MPLS カプセル化をイネーブルにします。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface Ethernet5/0`	（任意）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 5	**mpls ip** 例： `Router(config-if)# mpls ip`	（任意）指定したインターフェイスの MPLS カプセル化をイネーブルにします。
ステップ 6	**exit** 例： `Router(config-if)# exit`	（任意）終了して、特権 EXEC モードに戻ります。

Carrier Supporting Carrier 設定の確認

次のコマンドを使用して、バックボーンキャリアとカスタマーキャリア間に設定されたLDPセッションのステータスを確認します。これで、カスタマー キャリア ISP サイトが、バックボーンキャリアの VPN カスタマーとして表示されます。

手順の概要

1. **show mpls ldp discovery vrf***vrf-name*
2. **show mpls ldp discovery all**

手順の詳細

ステップ 1 **show mpls ldp discovery vrf***vrf-name*

このコマンドを使用して、バックボーン キャリアの PE ルータの VRF VPN1 に LDP セッションが存在することを示します。次に例を示します。

例：

```
Router# show mpls ldp discovery vrf vpn1
Local LDP Identifier:
    10.0.0.0:0
Discovery Sources:
    Interfaces:
        Ethernet1/0 (ldp): xmit/recv
            LDP Id: 10.0.0.1:0
POS6/0 (ldp): xmit
```

ステップ 2 **show mpls ldp discovery all**

このコマンドを使用して、ルータのすべてのLDPセッションのリストを表示します。次に例を示します。

例：

```
Router# show mpls ldp discovery all
Local LDP Identifier:
    10.10.10.10:0
Discovery Sources:
    Interfaces:
        Ethernet1/5 (ldp): xmit/recv
            LDP Id: 10.5.5.5:0
VRF vpn1: Local LDP Identifier:
    10.0.0.1:0
Discovery Sources:
    Interfaces:
        Ethernet1/0 (ldp): xmit/recv
            LDP Id: 10.0.0.1:0
POS6/0 (ldp): xmit
```

Local LDP Identifier フィールドには、このセッションのローカル ラベル スイッチング ルータの LDP ID が表示されます。Interfaces フィールドには、次のように、LDP ディスカバリ アクティビティを行うインターフェイスが表示されます。

- xmit は、インターフェイスが LDP ディスカバリ hello パケットを送信することを示します。

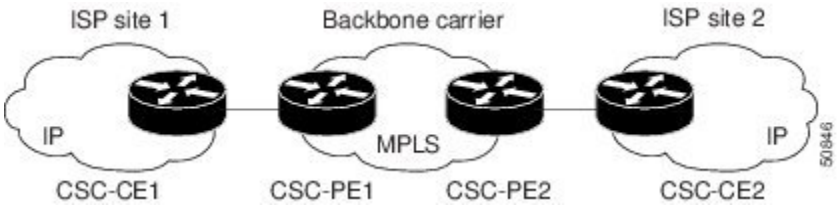
- recv は、インターフェイスが LDP ディスカバリ hello パケットを受信することを示します。

LDP および IGP を使用する MPLS VPN CSC の設定例

ISP であるカスタマーを含む MPLS VPN CSC ネットワーク：例

次の図に、カスタマー キャリアが ISP である Carrier Supporting Carrier ネットワーク設定を示します。このカスタマー キャリアには 2 つのサイトがあり、それぞれが POP です。カスタマー キャリアは、バックボーン キャリアによって提供される VPN サービスを使用してこれらのサイトを接続します。バックボーン キャリアは MPLS を使用します。ISP サイトは IP を使用します。ISP サイトとバックボーン キャリア間のパケット転送をイネーブルにするには、ISP をバックボーン キャリアに接続する CE ルータで MPLS が実行されている必要があります。

図 *16*：*ISP* であるカスタマー キャリアを含む *Carrier Supporting Carrier* ネットワーク



次に、Carrier Supporting Carrier ネットワーク内の各ルータの設定例を示します。OSPF を使用して、カスタマー キャリアをバックボーン キャリアに接続します。

CSC-CE1 の設定

```
mpls label protocol ldp
!
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
```

```
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.14.14.14 0.0.0.0 area 200
 network 10.15.0.0 0.255.255.255 area 200
 network 10.16.0.0 0.255.255.255 area 200
```

CSC-PE1 の設定

```
ip cef distributed
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.11.11.11 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 10.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface ATM1/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1/0.1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
```

```
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.11.11.11 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.19.19.19 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 200 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-PE2 の設定

```
ip cef distributed
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
```

```
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.12.12.12 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.20.20.20 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.11.11.11 remote-as 100
 neighbor 10.11.11.11 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 200 match internal external 1 external 2
```

```
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-CE2 の設定

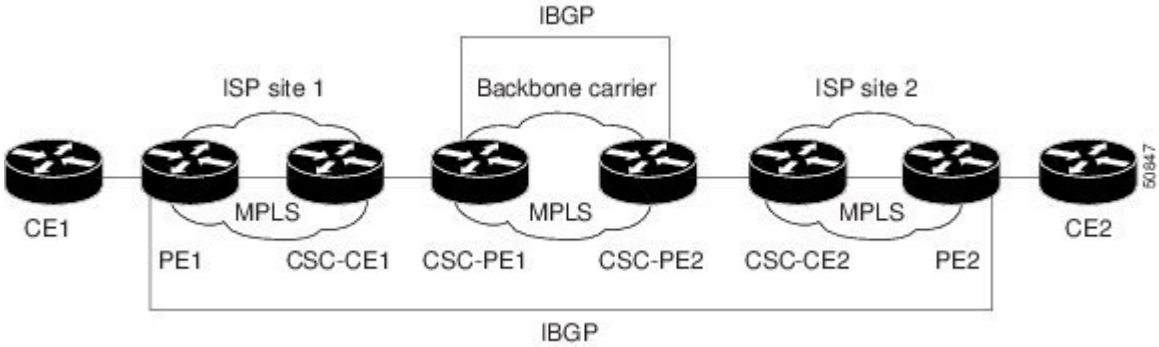
```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.16.16.16 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
 network 10.0.0.0 0.255.255.255 area 200
```

MPLS VPN プロバイダーであるカスタマーを含む MPLS VPN CSC ネットワーク：例

次の図には、カスタマー キャリアが MPLS VPN プロバイダーである Carrier Supporting Carrier ネットワーク設定が示されています。カスタマー キャリアには 2 つのサイトがあります。バックボー

ン キャリアおよびカスタマー キャリアは、MPLS を使用します。IBGP セッションは、ISP の外部ルーティング情報を交換します。

図 *17*：***MPLS VPN*** プロバイダーであるカスタマー キャリアを含む ***Carrier Supporting Carrier*** ネットワーク



次の設定例は、Carrier Supporting Carrier ネットワーク内の各ルータの設定を示しています。OSPF は、カスタマーキャリアをバックボーン キャリアに接続するために使用されるプロトコルです。

CE1 の設定

```
ip cef
!
interface Loopback0
 ip address 10.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 log-adjacency-changes
 redistribute bgp 300 subnets
 passive-interface Ethernet0/1
 network 10.17.17.17 0.0.0.0 area 300
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute ospf 300 match internal external 1 external 2
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 advertisement-interval 5
 no auto-summary
```

PE1 の設定

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
```

```
!
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 passive-interface Ethernet3/0
 network 10.13.13.13 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.15.15.15 remote-as 200
 neighbor 10.15.15.15 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.15.15.15 activate
 neighbor 10.15.15.15 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.15.15.15 activate
 neighbor 10.15.15.15 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 neighbor 10.0.0.2 advertisement-interval 5
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-CE1 の設定

```
mpls label protocol ldp
!
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
```

```
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.14.14.14 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
 network 10.0.0.0 0.255.255.255 area 200
```

CSC-PE1 の設定

```
ip cef distributed
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 10.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface ATM1/1/0
 no ip address
 no ip directed-broadcast
```

```
 no ip route-cache distributed
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.11.11.11 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.19.19.19 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 200 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-PE2 の設定

```
ip cef distributed
```

```
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.12.12.12 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.20.20.20 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.11.11.11 remote-as 100
```

```
 neighbor 10.11.11.11 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 200 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-CE2 の設定

```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.16.16.16 0.0.0.0 area 200
```

```
 network 10.0.0.0 0.255.255.255 area 200
 network 10.0.0.0 0.255.255.255 area 200
```

PE2 の設定

```
ip cef
ip cef accounting non-recursive
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address 10.15.15.15 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 passive-interface Ethernet3/0
 network 10.15.15.15 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.13.13.13 remote-as 200
 neighbor 10.13.13.13 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 neighbor 10.0.0.2 advertisement-interval 5
 no auto-summary
```

```
 no synchronization
 exit-address-family
```

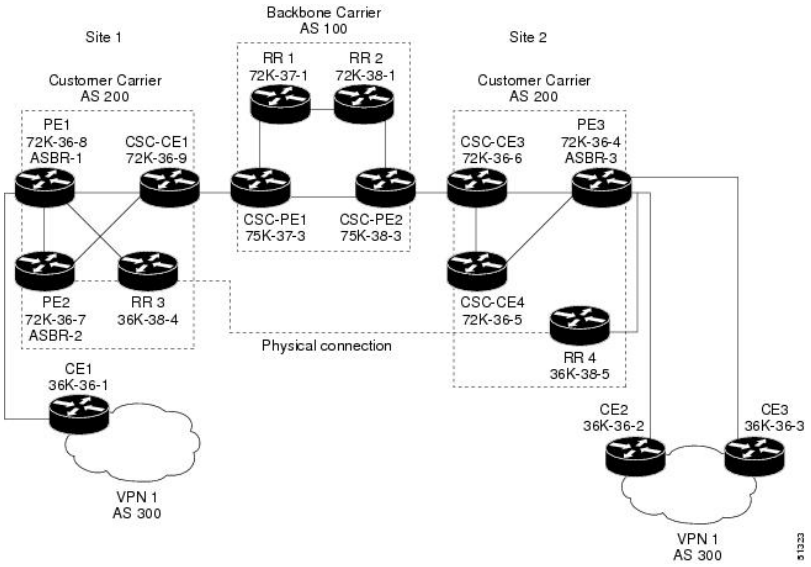
CE2 の設定

```
ip cef
!
interface Loopback0
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 log-adjacency-changes
 redistribute bgp 300 subnets
 passive-interface Ethernet0/1
 network 10.18.18.18 0.0.0.0 area 300
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute ospf 300 match internal external 1 external 2
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 advertisement-interval 5
 no auto-summary
```

ルート リフレクタを含む MPLS VPN CSC ネットワーク：例

次の図に、ルート リフレクタを含む Carrier Supporting Carrier ネットワーク設定を示します。カスタマー キャリアには 2 つのサイトがあります。

図 *18*：ルート リフレクタを含む *Carrier Supporting Carrier* ネットワーク



（注） ルート リフレクタ（RR）間の接続は必要ありません。

次の設定例は、Carrier Supporting Carrier ネットワーク内の各ルータの設定を示しています。次の点に注意してください。

- ルータの IP アドレスは、読みやすさのために省略されています。たとえば、PE 1 のループバック アドレスの 25 は、10.25.25.25 に相当します。
- 次のリストに、CSC-PE ルータのループバック アドレスを示します。
  - CSC-PE1（75K-37-3）：ループバック 0 = 10.15.15.15、ループバック 1 = 10.18.18.18
  - CSC-PE2（75K-38-3）：ループバック 0 = 10.16.16.16、ループバック 1 = 10.20.20.20

バックボーン キャリアの設定

ルート リフレクタ 1（72K-37-1）の設定

```
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
 network 10.2.0.0 0.255.255.255 area 100
```

```
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 10.15.15.15 remote-as 100
 neighbor 10.15.15.15 update-source Loopback0
 neighbor 10.16.16.16 remote-as 100
 neighbor 10.16.16.16 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.15.15.15 activate
 neighbor 10.15.15.15 route-reflector-client
 neighbor 10.15.15.15 send-community extended
 neighbor 10.16.16.16 activate
 neighbor 10.16.16.16 route-reflector-client
 neighbor 10.16.16.16 send-community extended
 bgp scan-time import 5
 exit-address-family
```

ルート リフレクタ 2（72K-38-1）の設定

```
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
 ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0 0.255.255.255 area 100
 network 10.2.0.0 0.255.255.255 area 100
!
router bgp 100
```

```
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 10.15.15.15 remote-as 100
 neighbor 10.15.15.15 update-source Loopback0
 neighbor 10.16.16.16 remote-as 100
 neighbor 10.16.16.16 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.15.15.15 activate
 neighbor 10.15.15.15 route-reflector-client
 neighbor 10.15.15.15 send-community extended
 neighbor 10.16.16.16 activate
 neighbor 10.16.16.16 route-reflector-client
 neighbor 10.16.16.16 send-community extended
 bgp scan-time import 5
 exit-address-family
```

CSC-PE1（75K-37-3）の設定

```
ip cef distributed
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
interface Loopback0
 ip address 10.15.15.15 255.255.255.255
 no ip directed-broadcast
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/0/1
 ip vrf forwarding vpn1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip route-cache distributed
 mpls label protocol ldp
 mpls ip
!
interface ATM1/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1/0.1 mpls
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
```

```
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/1/0.1 mpls
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
 network 10.2.0.0 0.255.255.255 area 100
 network 10.3.0.0 0.255.255.255 area 100
 network 10.4.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
 redistribute bgp 100 metric-type 1 subnets
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.13.13.13 remote-as 100
 neighbor 10.13.13.13 update-source Loopback0
 neighbor 10.14.14.14 remote-as 100
 neighbor 10.14.14.14 update-source Loopback0
 !
 address-family ipv4
 redistribute static
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 neighbor 10.14.14.14 activate
 neighbor 10.14.14.14 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 1 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

CSC-PE2（75K-38-3）の設定

```
ip cef distributed
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM2/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/1/0.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
```

```
interface ATM3/1/0
 no ip address
 no ip directed-broadcast
no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 6 33 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
 redistribute bgp 100 metric-type 1 subnets
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.13.13.13 remote-as 100
 neighbor 10.13.13.13 update-source Loopback0
 neighbor 10.14.14.14 remote-as 100
 neighbor 10.14.14.14 update-source Loopback0
 !
 address-family ipv4
 redistribute static
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 neighbor 10.14.14.14 activate
 neighbor 10.14.14.14 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute ospf 1 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

カスタマー キャリア サイト 1 の設定

PE1（72K-36-8）の設定

```
ip cef
!
ip vrf vpn2
 rd 200:1
```

```
 route-target export 200:1
 route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
 ip address 10.25.25.25 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet3/1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 redistribute connected
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.22.22.22 activate
 neighbor 10.22.22.22 send-community extended
 neighbor 10.23.23.23 activate
 neighbor 10.23.23.23 send-community extended
 exit-address-family
```

CSC-CE1（72K-36-9）の設定

```
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 10.11.11.11 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
```

PE2（72K-36-7）の設定

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
```

```
 route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
 ip address 10.24.24.24 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet3/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet3/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/3
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.22.22.22 activate
 neighbor 10.22.22.22 send-community extended
 neighbor 10.23.23.23 activate
 neighbor 10.23.23.23 send-community extended
 exit-address-family
```

ルート リフレクタ 3（36K-38-4）の設定

```
ip cef
!
interface Loopback0
 ip address 10.23.23.23 255.255.255.255
!
```

```
interface Ethernet1/1
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface Ethernet1/2
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM3/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 10.21.21.21 remote-as 200
 neighbor 10.21.21.21 update-source Loopback0
 neighbor 10.24.24.24 remote-as 200
 neighbor 10.24.24.24 update-source Loopback0
 neighbor 10.25.25.25 remote-as 200
 neighbor 10.25.25.25 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.21.21.21 activate
 neighbor 10.21.21.21 route-reflector-client
 neighbor 10.21.21.21 send-community extended
 neighbor 10.24.24.24 activate
 neighbor 10.24.24.24 route-reflector-client
 neighbor 10.24.24.24 send-community extended
 neighbor 10.25.25.25 activate
 neighbor 10.25.25.25 route-reflector-client
 neighbor 10.25.25.25 send-community extended
 exit-address-family
```

CE1（36K-36-1）の設定

```
ip cef
!
interface Loopback0
 ip address 10.28.28.28 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
```

```
!
interface Ethernet0/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router bgp 300
 network 10.0.0.0
 network 10.0.0.0
 network 10.0.0.0
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 remote-as 200
```

カスタマー キャリア サイト 2 の設定

CSC-CE3（72K-36-6）の設定

```
ip cef
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
mpls label protocol ldp
 mpls ip
!
interface POS2/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
mpls label protocol ldp
mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
 mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
```

PE3（72K-36-4）の設定

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
!
!
interface Loopback0
 ip address 10.21.21.21 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
mpls label protocol ldp
mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
mpls label protocol ldp
mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 redistribute connected
```

```
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.22.22.22 activate
 neighbor 10.22.22.22 send-community extended
 neighbor 10.23.23.23 activate
 neighbor 10.23.23.23 send-community extended
 exit-address-family
```

CSC-CE4（72K-36-5）の設定

```
ip cef
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast
!
interface POS4/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
mpls label protocol ldp
mpls ip
 clock source internal
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
mpls label protocol ldp
mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 33 aal5snap
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
```

ルート リフレクタ 4（36K-38-5）の設定

```
ip cef
```

```
!
interface Loopback0
 ip address 10.22.22.22 255.255.255.255
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 10.21.21.21 remote-as 200
 neighbor 10.21.21.21 update-source Loopback0
 neighbor 10.24.24.24 remote-as 200
 neighbor 10.24.24.24 update-source Loopback0
 neighbor 10.25.25.25 remote-as 200
 neighbor 10.25.25.25 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.21.21.21 activate
 neighbor 10.21.21.21 route-reflector-client
 neighbor 10.21.21.21 send-community extended
 neighbor 10.24.24.24 activate
 neighbor 10.24.24.24 route-reflector-client
 neighbor 10.24.24.24 send-community extended
 neighbor 10.25.25.25 activate
 neighbor 10.25.25.25 route-reflector-client
 neighbor 10.25.25.25 send-community extended
 exit-address-family
```

CE2（36K-36-2）の設定

```
ip cef
!
interface Loopback0
 ip address 10.26.26.26 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet0/2
```

```
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 10.0.0.0 0.255.255.255 area 300
 network 10.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 10.0.0.0
 network 10.1.0.0
 network 10.2.0.0
 neighbor 10.0.0.1 remote-as 200
```

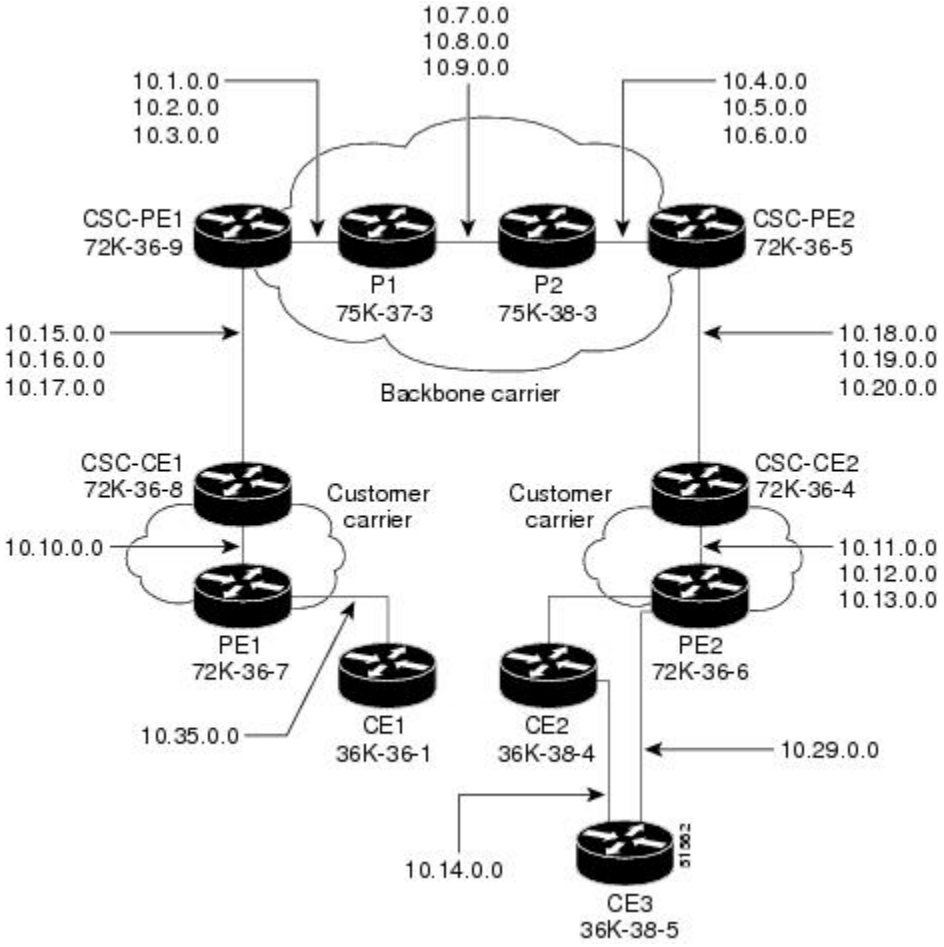
CE3（36K-36-3）の設定

```
ip cef
!
interface Loopback0
 ip address 10.27.27.27 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet1/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet1/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 10.0.0.0 0.255.255.255 area 300
 network 10.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 10.0.0.0
 network 10.1.0.0
 network 10.2.0.0
 neighbor 10.0.0.1 remote-as 200
```

VPNを持つカスタマーがネットワークエッジに存在するMPLSVPNCSCネットワーク：例

次の図に、VPN を持つカスタマーがネットワーク エッジに存在する Carrier Supporting Carrier ネットワーク設定を示します。

図 *19*：*Carrier Supporting Carrier* ネットワーク



バックボーン キャリアの設定

CSC-PE1（72K-36-9）の設定

```
ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
```

```
route-target import 100:0
mpls label protocol ldp
!
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.22.22.22 255.255.255.255
no ip directed-broadcast
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.1.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 10.2.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 10.3.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.15.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0.2 point-to-point
ip vrf forwarding vpn1
ip address 10.16.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
```

```
interface ATM2/0.3 point-to-point
ip vrf forwarding vpn1
ip address 10.17.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM2/0.1
passive-interface ATM2/0.2
passive-interface ATM2/0.3
passive-interface Loopback100
network 10.14.14.14 0.0.0.0 area 100
network 10.1.0.0 0.0.255.255 area 100
network 10.2.0.0 0.0.255.255 area 100
network 10.3.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 10.22.22.22 0.0.0.0 area 200
network 10.15.0.0 0.0.255.255 area 200
network 10.16.0.0 0.0.255.255 area 200
network 10.17.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

P1（75K-37-3）の設定

```
ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
```

```
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
ip address 10.7.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.2 point-to-point
ip address 10.8.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.3 point-to-point
ip address 10.9.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip address 10.1.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls accounting experimental input
tag-switching ip
!
interface ATM3/0/0.2 point-to-point
ip address 10.2.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0.3 point-to-point
ip address 10.3.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 10.12.12.12 0.0.0.0 area 100
network 10.1.0.0 0.0.255.255 area 100
network 10.2.0.0 0.0.255.255 area 100
network 10.3.0.0 0.0.255.255 area 100
network 10.7.0.0 0.0.255.255 area 100
network 10.8.0.0 0.0.255.255 area 100
network 10.9.0.0 0.0.255.255 area 100
```

P2（75K-38-3）の設定

```
ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.13.13.13 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM0/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
ip address 10.7.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM0/1/0.2 point-to-point
ip address 10.8.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM0/1/0.3 point-to-point
ip address 10.9.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
ip address 10.4.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0.2 point-to-point
ip address 10.5.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
```

```
interface ATM3/1/0.3 point-to-point
ip address 10.6.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 10.13.13.13 0.0.0.0 area 100
network 10.4.0.0 0.0.255.255 area 100
network 10.5.0.0 0.0.255.255 area 100
network 10.6.0.0 0.0.255.255 area 100
network 10.7.0.0 0.0.255.255 area 100
network 10.8.0.0 0.0.255.255 area 100
network 10.9.0.0 0.0.255.255 area 100
!
```

CSC-PE2（72K-36-5）の設定

```
ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.23.23.23 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.18.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip vrf forwarding vpn1
ip address 10.19.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip vrf forwarding vpn1
```

```
ip address 10.20.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 10.4.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.2 point-to-point
ip address 10.5.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 10.6.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM5/0.1
passive-interface ATM5/0.2
passive-interface ATM5/0.3
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.4.0.0 0.0.255.255 area 100
network 10.5.0.0 0.0.255.255 area 100
network 10.6.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 10.23.23.23 0.0.0.0 area 200
network 10.18.0.0 0.0.255.255 area 200
network 10.19.0.0 0.0.255.255 area 200
network 10.20.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.14.14.14 remote-as 100
neighbor 10.14.14.14 update-source Loopback0
!
address-family ipv4
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
no synchronization
exit-address-family
!
```

```
address-family vpnv4
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

カスタマー キャリア サイト 1 の設定

CSC-CE1（72K-36-8）の設定

```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.15.15.15 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.15.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 10.16.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 10.17.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface Ethernet3/1
ip address 10.10.0.2 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
```

```
redistribute connected subnets
network 10.15.15.15 0.0.0.0 area 200
network 10.10.0.0 0.0.255.255 area 200
network 10.15.0.0 0.0.255.255 area 200
network 10.16.0.0 0.0.255.255 area 200
network 10.17.0.0 0.0.255.255 area 200
```

PE2（72K-36-7）の設定

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
 ip address 10.24.24.24 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet3/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet3/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/3
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
 !
```

```
 address-family vpnv4
 neighbor 10.22.22.22 activate
 neighbor 10.22.22.22 send-community extended
 neighbor 10.23.23.23 activate
 neighbor 10.23.23.23 send-community extended
 exit-address-family
```

CE1（36K-36-1）の設定

```
ip cef
!
interface Loopback0
ip address 10.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 30.35.0.1 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet0/2
network 10.19.19.19 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.35.0.2 remote-as 200
neighbor 10.35.0.2 advertisement-interval 5
no auto-summary
```

カスタマー キャリア サイト 2 の設定

CSC-CE2（72K-36-4）の設定

```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.17.17.17 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 10.11.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
```

```
interface ATM5/0.2 point-to-point
ip address 10.12.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 10.13.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 10.18.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.2 point-to-point
ip address 10.19.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 10.20.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 10.17.17.17 0.0.0.0 area 200
network 10.11.0.0 0.0.255.255 area 200
network 10.12.0.0 0.0.255.255 area 200
network 10.13.0.0 0.0.255.255 area 200
network 10.18.0.0 0.0.255.255 area 200
network 10.19.0.0 0.0.255.255 area 200
network 10.20.0.0 0.0.255.255 area 200
```

PE2（72K-36-6）の設定

```
ip cef
!
ip vrf customersite
rd 200:1
route-target export 200:1
route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
```

```
ip address 10.18.18.18 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Ethernet3/0
ip vrf forwarding customersite
ip address 10.29.0.2 255.255.0.0
no ip directed-broadcast
!
interface Ethernet3/1
ip vrf forwarding customersite
ip address 10.30.0.2 255.255.0.0
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 10.11.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip address 10.12.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 10.13.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
passive-interface Ethernet3/0
passive-interface Ethernet3/1
network 10.18.18.18 0.0.0.0 area 200
network 10.11.0.0 0.0.255.255 area 200
network 10.12.0.0 0.0.255.255 area 200
network 10.13.0.0 0.0.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.16.16.16 remote-as 200
neighbor 10.16.16.16 update-source Loopback0
!
address-family ipv4
neighbor 10.16.16.16 activate
neighbor 10.16.16.16 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.16.16.16 activate
```

```
neighbor 10.16.16.16 send-community extended
exit-address-family
!
address-family ipv4 vrf customersite
neighbor 10.29.0.1 remote-as 300
neighbor 10.29.0.1 activate
neighbor 10.29.0.1 as-override
neighbor 10.29.0.1 advertisement-interval 5
neighbor 10.30.0.1 remote-as 300
neighbor 10.30.0.1 activate
neighbor 10.30.0.1 as-override
neighbor 10.30.0.1 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

CE2（36K-38-4）の設定

```
ip cef
!
interface Loopback0
ip address 10.21.21.21 255.255.255.255
!
interface Ethernet1/3
ip address 10.29.0.1 255.255.0.0
!
interface Ethernet5/0
ip address 10.14.0.1 255.255.0.0
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet1/3
network 10.21.21.21 0.0.0.0 area 300
network 10.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.29.0.2 remote-as 200
neighbor 10.29.0.2 advertisement-interval 5
no auto-summary
```

CE3（36K-38-5）の設定

```
ip cef
!
interface Loopback0
ip address 10.20.20.20 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 10.30.0.1 255.255.0.0
no ip directed-broadcast
!
interface Ethernet0/3
ip address 10.14.0.2 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet0/2
```

```
network 10.20.20.20 0.0.0.0 area 300
network 10.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.30.0.2 remote-as 200
neighbor 10.30.0.2 advertisement-interval 5
no auto-summary
```

LDP および IGP を使用する MPLS VPN Carrier Supporting Carrier のその他の関連資料

関連資料

関連項目	マニュアル タイトル
MPLS	『MPLS Product Literature』

RFC

RFC	タイトル
RFC 2547	『BGP/MPLS VPNs』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

LDP および IGP を使用する MPLS VPN CSC の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8*：*LDP* および *IGP* を使用する *MPLS VPN CSC* の機能情報

機能名	リリース	機能の設定情報
MPLS VPN Carrier Supporting Carrier	12.0(14)ST 12.0(16)ST 12.2(8)T 12.0(21)ST 12.0(22)S 12.0(23)S Cisco IOS XE Release 2.2	この機能により、LDP を使用して MPLS ラベルを転送し、IGP を使用してルートを転送する MPLS VPN CSC ネットワークをセットアップおよび作成できます。 この機能は、12.0(14)ST で導入されました。 この機能は、12.0(16)ST で統合されました。 この機能は、12.2(8)T で統合されました。 この機能は、12.0(21)ST で統合されました。 この機能は、12.0(22)S で統合されました。 この機能は、12.0(23)S で統合されました。 この機能は、Cisco IOS XE Release 2.2 で、Cisco ASR 1000 シリーズ ルータに実装されました。 この機能で使用される新しいコマンドまたは変更されたコマンドはありません。

用語集

ASBR：Autonomous System Boundary Router（自律システム境界ルータ）。自律システムを別の自律システムに接続するルータ。

自律システム：共通管理で共通のルーティング方針が共有される、ネットワークの集合。

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとネットワーク到達可能性情報を交換する、ドメイン間ルーティング プロトコル（同じ自律システム内の場合も、複数の自律システム間の場合もあります）。

CE ルータ：カスタマー エッジ ルータ。カスタマー ネットワークに属し、プロバイダー エッジ（PE）ルータとのインターフェイスとなるルータ。CE ルータは、関連する MPLS VPN を認識しません。

CSC：Carrier Supporting Carrier。小規模サービス プロバイダー（カスタマー キャリア）が MPLS バックボーンを経由してそれぞれの IP ネットワークまたは MPLS ネットワークを相互接続できる階層型 VPN モデル。これにより、カスタマー キャリアは独自の MPLS バックボーンを構築および維持する必要がなくなります。

eBGP：external Border Gateway Protocol（外部 Border Gateway Protocol）。異なる自律システムにあるルータ間の BGP。異なる自律システムにある 2 つのルータが互いに 2 ホップ以上離れている場合、これら 2 つのルータ間の eBGP セッションはマルチホップ BGP であると見なされます。

エッジ ルータ：ネットワークのエッジにあるルータ。MPLS ネットワークの境界を定義します。パケットを送受信します。エッジ ラベル スイッチ ルータおよびラベル エッジ ルータとも呼ばれます。

iBGP：internal Border Gateway Protocol（内部ボーダー ゲートウェイ プロトコル）。同じ自律システム内にあるルータ間の BGP。

IGP：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。単一の自律システム内でのルーティング情報の交換に使用されるインターネット プロトコル。インターネット IGP プロトコルの例として、IGRP、OSPF、IS-IS、RIP があります。

IP：Internet Protocol（インターネット プロトコル）。TCP/IP スタックにおいてコネクションレス型のネットワーク間サービスを提供するネットワーク層プロトコル。IP では、アドレッシング、タイプ オブ サービス指定、フラグメンテーションと再編成、セキュリティなどの機能が提供されます。RFC 791 に定義されています。

LDP：Label Distribution Protocol。パケットの転送に使用されるラベル（アドレス）をネゴシエーションするための、MPLS 対応ルータ間の標準プロトコル。

LFIB：Label Forwarding Information Base（ラベル転送情報ベース）。着信ラベルと発信ラベル、および関連する Forward Equivalence Class（FEC）パケットについての情報を保持するために MPLS で使用されるデータ構造。

MP-BGP：Multiprotocol BGP。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベル スイッチングを担当する IETF ワーキング グループの名前、およびそのワーキング グループで標準化されたラベル スイッチング アプローチの名前。

NLRI：Network Layer Reachability Information（ネットワーク層到達可能性情報）。BGP では、ルートおよびそのルートへのアクセス方法を記述した NLRI を含むルーティング アップデート メッセージが送信されます。この場合、NLRI がプレフィックスとなります。BGP アップデート メッセージでは、1 つ以上の NLRI プレフィックス、および NLRI プレフィックスのルートの属性が伝送されます。ルート属性には、BGP ネクスト ホップ ゲートウェイ アドレスおよび拡張コミュニティ値が含まれています。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）によって、ルータは、ルート プロセッサが他のルート プロセッサにテイクオーバーまたはスイッチオーバーされたあとでも継続して IP パケットを転送できます。NSF では、レイヤ 3 のルーティングおよび転送情報をバックアップルートプロセッサに保持および更新することによって、スイッチオーバーやルート収束のプロセス中にも継続して IP パケットおよびルーティング プロトコル情報が転送されることが保証されます。

PE ルータ：プロバイダー エッジ ルータ。サービス プロバイダーのネットワークの一部であるルータ。このルータは、カスタマー エッジ（CE）ルータに接続されます。すべての MPLS VPN 処理は PE ルータで実行されます。

QoS：Quality of Service。転送システムのパフォーマンスを測定したものであり、転送品質およびサービス アベイラビリティを示します。

RD：Route Distinguisher（ルート識別子）。IPv4 プレフィックスに連結される 8 バイトの値で、一意の VPN IPv4 プレフィックスを形成します。

RT：Route Target（ルート ターゲット）。プレフィックスのインポート先となる VRF ルーティング テーブルの識別に使用する拡張コミュニティ属性。

SLA：VPN 加入者に保証されるサービス レベル契約。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。1 つ以上の物理ネットワークのリソースを共有する、セキュアな MPLS ベースのネットワーク（一般的に1 つまたは複数のサービスプロバイダーによって実行されます）。VPN には地理的に分散したサイトが含まれており、共有バックボーン ネットワーク上で安全に通信できるようになっています。

VRF：VPN ルーティングおよび転送（VRF）インスタンス。PE ルータに付加される VPN サイトを定義するルーティング情報。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。

第 6 章

BGP を使用する MPLS VPN Carrier Supporting Carrier

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）Carrier Supporting Carrier（CSC）を使用すると、MPLS VPN ベースのサービス プロバイダーは、そのバックボーン ネットワークのセグメントを他のサービス プロバイダーが使用できるようにすることができます。この章では、ボーダー ゲートウェイ プロトコル（BGP）を使用してルートおよびMPLS ラベルを配布する MPLS VPN CSC ネットワークの設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BGP を使用する MPLS VPN CSC の前提条件

- エンドツーエンド（CE から CE へのルータ）の ping が機能するように MPLS VPN を設定できる必要があります。そのためには、内部ゲートウェイ プロトコル（IGP）、MPLS ラベル配布プロトコル（LDP）、およびマルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）の設定方法を理解している必要があります。
- CSC-PE ルータおよび CSC-CE ルータが、BGP ラベル配布をサポートするイメージを実行できる必要があります。実行できない場合は、これらのルータ間で外部 BGP（EBGP）を実行できません。カスタマー キャリアとバックボーンキャリア間の接続を確認します。EBGP ベースのラベル配布は、MPLS をカスタマー キャリアとバックボーンキャリア間でイネーブルにするために、これらのリンク上で設定されています。

BGP を使用する MPLS VPN CSC の制約事項

プロバイダー エッジ（PE）ルータ上で、ラベルを使用する BGP または LDP のいずれかのインターフェイスを設定できます。両方のタイプのラベル配布を同じインターフェイス上でイネーブルにすることはできません。プロトコルを別のプロトコルに切り替える場合は、別のプロトコルをイネーブルにする前に、すべてのインターフェイス上の既存のプロトコルをディセーブルにする必要があります。

この機能は次の処理をサポートしません。

- CSC-PE ルータと CSC-CE ルータ間の EBGP マルチホップ
- EIBGP のマルチパス ロード シェアリング

複数の BGP スピーカーを接続する物理インターフェイスは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングと MPLS をサポートしている必要があります。

BGP を使用する MPLS VPN CSC に関する情報

MPLS VPN CSC の概要

Carrier Supporting Carrier により、サービス プロバイダーは、そのバックボーン ネットワークのセグメントを別のサービス プロバイダーが使用できるようにすることができます。他のプロバイダーにバックボーン ネットワークのセグメントを提供するサービスプロバイダーは、バックボー

ン キャリアと呼ばれます。バックボーン ネットワークのセグメントを使用するサービス プロバイダーは、カスタマー キャリアと呼ばれます。

バックボーン キャリアは、ボーダー ゲートウェイ プロトコル/マルチプロトコル ラベル スイッチング（BGP/MPLS）VPN サービスを提供します。カスタマー キャリアは、次のいずれかになります。

- インターネット サービス プロバイダー（ISP）
- BGP/MPLS VPN サービス プロバイダー

MPLS VPN CSC の実装の利点

MPLS VPN CSC ネットワークは、バックボーン キャリアであるサービス プロバイダー、およびカスタマー キャリアに対して次の利点をもたらします。

バックボーン キャリアにとっての利点

- バックボーン キャリアは、多数のカスタマー キャリアに対応し、そのバックボーンにカスタマー キャリアがアクセスできるようにします。バックボーン キャリアは、それぞれのカスタマー キャリア用に個別のバックボーンを作成および維持する必要はありません。1 つのバックボーン ネットワークを使用して複数のカスタマー キャリアをサポートすると、バックボーン キャリアの VPN 動作が簡略化されます。バックボーン キャリアは、一貫した方法を使用して、バックボーン ネットワークを管理および維持します。この方法は、個々のバックボーンを維持するよりも安価かつ効率的でもあります。
- MPLS VPN Carrier Supporting Carrier 機能は、スケーラブルです。Carrier Supporting Carrier では、帯域幅および接続の変化するニーズに合わせて VPN を変更できます。この機能は、予定外の成長や変更に対応できます。Carrier Supporting Carrier 機能により、同じネットワーク上で何万もの VPN をセットアップでき、サービス プロバイダーは VPN サービスとインターネット サービスの両方を提供できます。
- MPLS VPN Carrier Supporting Carrier 機能は、柔軟なソリューションです。バックボーン キャリアは、多くのタイプのカスタマー キャリアに対応できます。バックボーン キャリアは、ISP であるカスタマー キャリアおよび VPN サービス プロバイダーであるカスタマー キャリアのいずれかまたは両方を受け入れることができます。バックボーン キャリアは、セキュリティおよびさまざまな帯域幅を必要とするカスタマー キャリアに対応できます。

カスタマー キャリアにとっての利点

- MPLS VPN Carrier Supporting Carrier 機能により、カスタマー キャリアでは、独自のバックボーンを設定、運用、および維持する必要がなくなります。カスタマーキャリアは、バックボーン キャリアのバックボーン ネットワークを使用しますが、ネットワークのメンテナンスと運用はバックボーン キャリアが担当します。
- バックボーン キャリアが提供する VPN サービスを使用するカスタマー キャリアには、フレーム リレーまたは ATM ベースの VPN が提供するのと同じレベルのセキュリティがもたらされます。また、カスタマー キャリアは VPN で IPSec を使用することにより、より高いレ

ベルのセキュリティを確保できます。これは、バックボーン キャリアにとっては完全に透過的です。

- カスタマー キャリアは、任意のリンク層テクノロジー（SONET、DSL、フレーム リレーなど）を使用して、CE ルータを PE ルータに接続し、PE ルータを P ルータに接続します。MPLS VPN Carrier Supporting Carrier 機能は、リンク層とは独立しています。CE ルータと PE ルータは IP を使用して通信し、バックボーン キャリアは MPLS を使用します。
- カスタマー キャリアは、任意のアドレッシング方式を使用でき、バックボーン キャリアによるサポートを引き続き受けることができます。カスタマーのアドレス空間およびルーティング情報は、他のカスタマー キャリアまたはバックボーン プロバイダーのアドレス空間およびルーティング情報とは独立しています。

BGP を使用する MPLS VPN CSC の実装の利点

BGP をイネーブルにするように CSC ネットワークを設定して、バックボーン キャリア PE ルータとカスタマー キャリア CE ルータ間のルートおよび MPLS ラベルを複数パスを使用して転送できます。BGP を使用して IPv4 ルートと MPLS ラベル ルートを配布する利点を次に示します。

- BGP は、VPN ルーティング/転送（VRF）インスタンス テーブルでの IGP および LDP の代わりになります。BGP を使用して、ルートおよび MPLS ラベルを配布できます。2 つではなく単一のプロトコルを使用すると、設定およびトラブルシューティングが簡単になります。
- BGP は、2 つの ISP を接続する場合の優先ルーティング プロトコルです。主な理由は、そのルーティング ポリシーと拡張性です。ISP では、通常、2 つのプロバイダー間で BGP を使用します。この機能を使用すると、これらの ISP は BGP を使用できます。

BGP を使用する MPLS VPN CSC の設定オプション

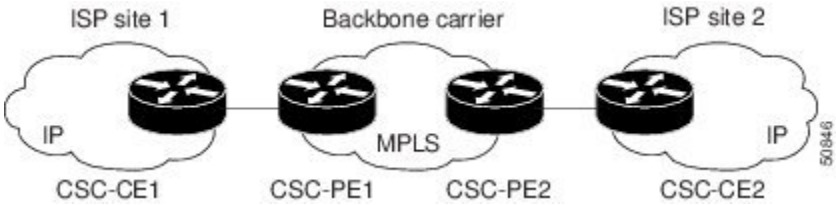
ここでは、バックボーン キャリアおよびカスタマー キャリアが、IPv4 ルートと MPLS ラベルを配布する方法について説明します。バックボーン キャリアは、BGP サービスと MPLS VPN サービスを提供します。カスタマー キャリアは、次のいずれかになります。

カスタマー キャリアが IP コアを使用する ISP である場合

次の図に、カスタマー キャリアが ISP であるネットワーク設定を示します。このカスタマー キャリアには 2 つのサイトがあり、それぞれが Point of Presence（POP）です。カスタマー キャリア

は、バックボーン キャリアによって提供される VPN サービスを使用してこれらのサイトを接続します。バックボーン キャリアは MPLS を使用します。ISP サイトは IP を使用します。

図 *20*：カスタマー キャリアが *ISP* であるネットワーク



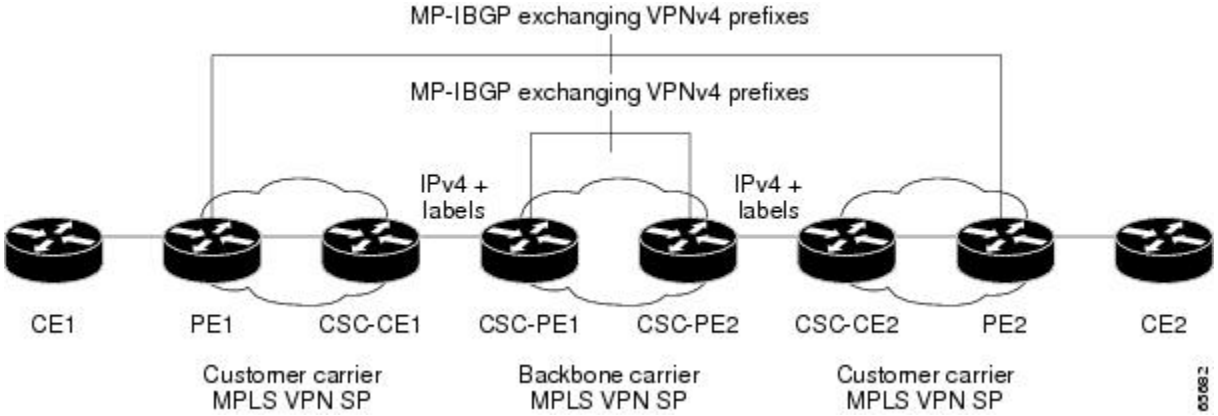
CE ルータと PE ルータ間のリンクでは、EBGP を使用して、IPv4 ルートと MPLS ラベルを配布します。これらのリンク間では、PE ルータはマルチプロトコル IBGP を使用して、VPNv4 ルートを配布します。

（注） Cisco ルータ以外のルータが CSC-PE または CSC-CE として使用される場合、そのルータで IPv4 BGP ラベル配布（RFC 3107）がサポートされている必要があります。サポートされていない場合は、ラベルを使用する EBGP をルータ間で実行できません。

カスタマー キャリアが VPN サービスを使用または使用しない MPLS サービス プロバイダーである場合

次の図に、バックボーン キャリアとカスタマー キャリアが BGP/MPLS VPN サービス プロバイダーであるネットワーク設定を示します。これは、階層型 VPN と呼ばれています。カスタマー キャリアには 2 つのサイトがあります。バックボーン キャリアとカスタマー キャリアは両方とも、それぞれのネットワークで MPLS を使用します。

図 *21*：カスタマー キャリアが *MPLS VPN* サービス プロバイダーであるネットワーク



この設定では、カスタマー キャリアは、そのネットワークを次のいずれかの方法で設定できます。

- カスタマー キャリアは、そのコア ネットワークで IGP および LDP を実行できます。この場合、カスタマー キャリアの CSC-CE1 ルータは、バックボーン キャリアの CSC-PE1 ルータから学習した EBGP ルートを IGP に再配布します。
- カスタマー キャリア システムの CSC-CE1 ルータは、PE1 ルータとの間で IPv4 およびラベル IBGP セッションを実行できます。

BGP を使用する MPLS VPN CSC の設定方法

Carrier Supporting Carrier トポロジの識別

BGP を使用して MPLS VPN CSC を設定する前に、バックボーン キャリアとカスタマー キャリアの両方のトポロジを識別する必要があります。

階層型 VPN の場合、MPLS VPN ネットワークのカスタマー キャリアは、カスタマーに対して MPLS VPN サービスを提供します。この場合、カスタマー キャリアのタイプ、およびカスタマー キャリアのトポロジを識別する必要があります。階層型VPNでは、追加の設定手順が必要となります。この設定手順については、設定の項で説明します。

（注） 複数のインターフェイスを使用して、複数の CSC-CE ルータを同じ PE に接続したり、単一の CSC-CE ルータを複数の CSC-PE に接続したりすることにより、CSC トポロジでの冗長性および複数パス サポートを提供できます。

Carrier Supporting Carrier 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. カスタマーキャリアのタイプ、ISP、またはMPLS VPNサービスプロバイダーを識別します。
2. （階層型 VPN の場合のみ）CE ルータを識別します。
3. （階層型 VPN の場合のみ）カスタマー キャリアのコア ルータの設定を識別します。
4. カスタマー キャリア エッジ（CSC-CE）ルータを識別します。
5. バックボーン キャリア ルータ設定を識別します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	カスタマーキャリアのタイプ、ISP、または MPLS VPN サービス プロバイダーを識別します。	Carrier Supporting Carrier ネットワークの設定に関する要件を設定します。 • ISP の場合、カスタマーサイトの設定は必要ありません。 • MPLS VPN サービス プロバイダーの場合、カスタマーサイトを設定し、「階層型 VPN の場合のみ」と示されている作業または手順をすべて実行する必要があります。
ステップ 2	（階層型 VPN の場合のみ）CE ルータを識別します。	CE から PE への接続の設定に関する要件を設定します。
ステップ 3	（階層型 VPN の場合のみ）カスタマーキャリアのコア ルータの設定を識別します。	コア（P）ルータ間、およびコア（P）ルータとエッジルータ（PE ルータと CSC-CE ルータ）間の接続設定に関する要件を設定します。
ステップ 4	カスタマー キャリア エッジ（CSC-CE）ルータを識別します。	CSC-CE から CSC-PE への接続の設定に関する要件を設定します。
ステップ 5	バックボーン キャリア ルータ設定を識別します。	CSC コア ルータ間、および CSC コア ルータとエッジルータ（CSC-CE ルータと CSC-PE ルータ）間の接続設定に関する要件を設定します。

次の作業

バックボーン キャリア コアの設定, （201 ページ）で説明しているように、Carrier Supporting Carrier ネットワークをセットアップします。

バックボーン キャリア コアの設定

バックボーン キャリア コアの設定では、CSC コア ルータと CSC-PE ルータの接続およびルーティング機能をセットアップする必要があります。

CSC コア（バックボーン キャリア）を設定および確認するには、次の作業を実行します。

前提条件

バックボーン キャリア コアを設定する前に、CSC コア ルータ上で次のプロトコルを設定します。

- IGP ルーティング プロトコル：BGP、OSPF、IS-IS、EIGRP、スタティックなど。
- ラベル配布プロトコル（LDP）。詳細については、『How to Configure MPLS LDP』を参照してください。

CSC コアにおける IP 接続と LDP 設定の確認

CSC コアにおける IP 接続と LDP 設定を確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [- *label*] | **interface***interface* |**next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
5. **show mpls ldp discovery** [**vrf***vrf-name* | **all**]
6. **show mpls ldp neighbor** [[**vrf***vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf***vrf-name*] [*interface*] [**detail**] | **all**]
9. **show ip route**
10. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**ping** [*protocol*] {*host-name* | *system-address*} 例： `Router# ping ip 10.1.0.0`	（任意）AppleTalk、CLNS、IP、Novell、Apollo、VINES、DECnet、または 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 ip** コマンドを使用して、CSC コア ルータから別の CSC コア ルータへの接続を確認します。
ステップ 3	**trace** [*protocol*] [*destination*] 例： `Router# trace ip 10.2.0.0`	（任意）パケットがその宛先に送信されるときに実際に取るルートを検出します。 • **trace** コマンドを使用して、パケットがその最終的な宛先に到達するまでに通過するパスを確認します。**trace** コマ

	コマンドまたはアクション	目的
		ンドは、2つのルータが通信できない場合に問題のある箇所を分離するのに役立ちます。
ステップ 4	**show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [- *label*] | **interface***interface* |**next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**] 例： `Router# show mpls forwarding-table`	（任意）MPLS ラベル転送情報ベース（LFIB）の内容を表示します。 • **show mpls forwarding-table** コマンドを使用して、MPLS パケットが転送されていることを確認します。
ステップ 5	**show mpls ldp discovery** [**vrf***vrf-name* | **all**] 例： `Router# show mpls ldp discovery`	（任意）LDP ディスカバリ プロセスのステータスを表示します。 • **show mpls ldp discovery** コマンドを使用して、LDP が CSC コアで動作していることを確認します。
ステップ 6	**show mpls ldp neighbor** [[**vrf***vrf-name*] [*address* | *interface*] [**detail**] | **all**] 例： `Router# show mpls ldp neighbor`	（任意）LDP セッションのステータスを表示します。 • **show mpls ldp neighbor** コマンドを使用して、CSC コアにおける LDP 設定を確認します。
ステップ 7	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef`	（任意）転送情報ベース（FIB）のエントリを表示します。 • **show ip cef** コマンドを使用して、転送テーブル（プレフィックス、ネクストホップ、およびインターフェイス）を確認します。
ステップ 8	**show mpls interfaces** [[**vrf***vrf-name*] [*interface*] [**detail**] | **all**] 例： `Router# show mpls interfaces`	（任意）ラベル スイッチングに設定されている 1 つ以上のインターフェイスまたはすべてのインターフェイスに関する情報を表示します。 • **show mpls interfaces** コマンドを使用して、LDP を使用するようにインターフェイスが設定されていることを確認します。
ステップ 9	**show ip route** 例： `Router# show ip route`	（任意）IP ルーティング テーブルのエントリを表示します。 • **show ip route** コマンドを使用して、ホスト IP アドレス、ネクストホップ、インターフェイスなどを含む、ルーティング テーブル全体を表示します。

	コマンドまたはアクション	目的
ステップ 10	**disable** 例： `Router# disable`	（任意）特権 EXEC モードに戻ります。

トラブルシューティングのヒント

ping コマンドと **trace** コマンドを使用して、コアにおける MPLS 接続の詳細を確認します。さらに **show** コマンドを使用して、有用なトラブルシューティング情報を入手することもできます。

CSC-PE ルータの VRF の設定

VPN ルーティング/転送（VRF）インスタンスをバックボーン キャリア エッジ（CSC-PE）ルータに設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map***route-map*
7. **exit**
8. **interface***typenumber*
9. **ip vrf forwarding***vrf-name*
10. **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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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 vpn1`	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-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。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。192.168.122.15:1 など。

ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target import 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、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 6	**import map***route-map* 例： `Router(config-vrf)# import map vpn1-route-map`	（任意）VRF のインポート ルート マップを設定します。 • *route-map* 引数には、VRF のインポート ルート マップとして使用されるルート マップを指定します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Router(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。
ステップ 8	**interface***typenumber* 例： `Router(config)# interface Ethernet5/0`	設定するインターフェイスを指定します。 • *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 9	**ip vrf forwarding***vrf-name* 例： `Router(config-if)# ip vrf forwarding vpn1`	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。
ステップ 10	**end** 例： `Router(config-if)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip vrf detail コマンドを入力し、MPLS VPN が稼働しており、適切なインターフェイスに関連付けられていることを確認します。

バックボーン キャリアにおける VPN 接続の Multiprotocol BGP の設定

バックボーン キャリアでマルチプロトコル BGP（MP-BGP）接続を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source***interface-type*
7. **address-family vpnv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**no bgp default ipv4-unicast** 例： `Router(config-router)# no bgp default ipv4-unicast`	（任意）IPv4 ユニキャスト アドレス ファミリをすべてのネイバーでディセーブルにします。 • ネイバーを MPLS ルートのみに使用している場合は、**no bgp default-unicast** コマンドを no 形式で使用します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor 10.5.5.5 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **update-source***interface-type* 例： `Router(config-router)# neighbor 10.2.0.0 update-source loopback0`	BGP セッションで、TCP 接続の特定の動作インターフェイスを使用できるようになります。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *interface-type* 引数には、ソースとして使用するインターフェイスを指定します。
ステップ 7	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ 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 プレフィックスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Router(config-router-af)# neighbor 10.0.0.1 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.4.0.0 activate`	ネイバー BGP ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip bgp neighbor コマンドを入力すると、ネイバーが稼働中であることを確認できます。このコマンドが成功しなかった場合は、**debug ip bgp x.x.x.x events** コマンドを入力します。ここで、*x.x.x.x* はネイバーの IP アドレスです。

CSC-PE ルータと CSC-CE ルータの設定

BGP を使用してルートと MPLS ラベルを配布する MPLS VPN CSC ネットワークの CSC-PE ルータとキャリア CSC-CE ルータとの間のリンクを設定および確認するには、次の作業を実行します。

次の図に、CSC-PE ルータと CSC-CE ルータ間を直接接続するインターフェイスによるピアリングの設定を示します。この設定は、次に説明する作業で例として使用します。

図 *22*：*CSC-PE* ルータと *CSC-CE* ルータ間を直接接続するインターフェイスによるピアリングの設定

CSC-PE ルータの設定

CSC-PE ルータを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor***ip-address***as-override**
8. **neighbor***ip-address***send-label**
9. **exit-address-family**
10. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Router(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。

	コマンドまたはアクション	目的
		• **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router-af)# neighbor 10.0.0.1 remote-as 200`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.0.0.2 activate`	ネイバー BGP ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**neighbor***ip-address***as-override** 例： `Router(config-router-af)# neighbor 10.0.0.2 as-override`	サイトの自律システム番号（ASN）をプロバイダーの ASN で上書きするように PE ルータを設定します。 • *ip-address* 引数には、指定した ASN で上書きされるルータの IP アドレスを指定します。
ステップ 8	**neighbor***ip-address***send-label** 例： `Router(config-router-af)# neighbor 10.0.0.2 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 • *ip-address* 引数には、ネイバー ルータの IP アドレスを指定します。
ステップ 9	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Router(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip bgp neighbor コマンドを入力して、ネイバーが稼働中であることを確認します。コマンド出力で、ネイバーの各機能の下に次の行が表示されていることを確認してください。

```
IPv4 MPLS Label capability:advertised and received
```

CSC-CE ルータの設定

CSC-CE ルータを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **redistribute***protocol*
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor***ip-address***send-label**
9. **exit-address-family**
10. **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。 • 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： `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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp***as-number* 例： `Router(config)# router bgp 200`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Router(config-router)# address-family ipv4`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。

ステップ 5	**redistribute***protocol*
	
	例：
	
	`Router(config-router-af)# redistribute static`
		ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
		
		• *protocol* 引数では、ルートの再配布元となるソース プロトコルを指定します。次のいずれかのキーワードを指定できます：**bgp**、**egp**、**igrp**、**isis**、**ospf**、**mobile**、**static** [**ip**]、**connected**、and **rip**。
		
		  • **static** [**ip**] キーワードを使用すると、IP スタティック ルートが再配布されます。省略可能な **ip** キーワードは、スタティック ルートを IS-IS に再配布する場合に使用します。
		
		  • **connected** キーワードは、IP がインターフェイスでイネーブルな場合に自動的に確立されるルートを示します。OSPF や IS-IS などのルーティング プロトコルの場合、これらのルートは自律システムに対して外部として再配布されます。

ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。

	コマンドまたはアクション	目的
	例： `Router(config-router-af)# neighbor 10.5.0.2 remote-as 100`	• *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.3.0.2 activate`	ネイバー BGP ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 8	**neighbor***ip-address***send-label** 例： `Router(config-router-af)# neighbor 10.0.0.2 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 • *ip-address* 引数には、ネイバー ルータの IP アドレスを指定します。
ステップ 9	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Router(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

CSC-PE ルータのラベルの確認

CSC-PE ルータのラベルを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**]
3. **show mpls interfaces** [**all**]
4. **show ip route vrf***vrf-name* [*prefix*]
5. **show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**]
6. **show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
7. **show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
8. **traceroute vrf** [*vrf-name*] *ip-address*
9. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**] 例： `Router# show ip bgp vpnv4 all summary`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • **show ip bgp vpnv4 all summary** コマンドを使用して、BGP セッションが CSC-PE ルータと CSC-CE ルータ間で稼働中であることを確認します。State/PfxRcd カラムのデータをチェックして、各セッション時にプレフィックスが学習されていることを確認します。
ステップ 3	**show mpls interfaces** [**all**] 例： `Router# show mpls interfaces all`	（任意）ラベルスイッチングに設定されている 1 つ以上のインターフェイスに関する情報を表示します。 • **show mpls interfaces all** コマンドを使用して、MPLS インターフェイスが稼働中であることを確認します。また、LDP 対応インターフェイスに、LDP が稼働中であることが示されていることを確認します。EBGP によってラベルが配布されるため、VRF では LDP がオフになっていることを確認してください。
ステップ 4	**show ip route vrf***vrf-name* [*prefix*] 例： `Router# show ip route vrf vpn1 10.5.5.5`	（任意）VRF 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。 • **show ip route vrf** コマンドを使用して、PE ルータのプレフィックスが CSC-PE ルータのルーティング テーブルに存在することを確認します。

	コマンドまたはアクション	目的
		（注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数ルートが、対応する VRF ルーティング テーブルにインストールされていることを確認します。
ステップ 5	**show ip bgp vpnv4** {**all** | **rd***route-distinguisher* | **vrf***vrf-name*} [**summary**] [**labels**] 例： `Router# show ip bgp vpnv4 vrf vpn1 labels`	（任意）BGP テーブルからの VPN アドレス情報を表示します。 • **show ip bgp vpnv4 vrf***vrf-name***labels** コマンドを使用して、カスタマー キャリア MPLS サービス プロバイダー ネットワークのプレフィックスが BGP テーブルに存在し、適切なラベルが付けられていることを確認します。 （注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数のラベルが、対応する VRF ルーティング テーブルにインストールされていることを確認します。
ステップ 6	**show ip cef** [**vrf***vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef vrf vpn1 10.1.0.0 detail`	（任意）転送情報ベース（FIB）のエントリを表示するか、または FIB のサマリーを表示します。 • **show ip cef vrf** コマンドと **show ip cef vrf detail** コマンドを使用して、PE ルータのプレフィックスが CEF テーブルに存在することを確認します。
ステップ 7	**show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**] 例： `Router# show mpls forwarding-table vrf vpn1 10.1.0.0 detail`	（任意）MPLS ラベル転送情報ベース（LFIB）の内容を表示します。 • **show mpls forwarding-table** コマンドに **vrf** キーワードを指定するか、または **vrf** と **detail** の両方のキーワードを指定して、ローカル カスタマー MPLS VPN サービス プロバイダーの PE ルータのプレフィックスが LFIB に含まれているかどうかを確認します。 （注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数のラベルが、対応する VRF テーブルにインストールされていることを確認します。
ステップ 8	**traceroute vrf** [*vrf-name*] *ip-address* 例： `Router# traceroute vrf vpn2 10.2.0.0`	パケットがその宛先に到達するまでにネットワークを通過するルートを表示します。 • **traceroute vrf** コマンドを使用して、PE から宛先 CE ルータへのデータ パスおよびトランスポート ラベルを確認します。 （注） このコマンドは、IP 存続可能時間（TTL）情報を伝播および生成するようにバックボーン ルータが設定されている場合にのみ、MPLS 認識 traceroute とともに機能します。詳細については、**mpls ip propagate-ttl** コマンドに関するマニュアルを参照してください。

	コマンドまたはアクション	目的
		（注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数ルートが、対応する VRF テーブルにインストールされていることを確認します。
ステップ 9	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

CSC-CE ルータでのラベルの確認

CSC-CE ルータのラベルを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip bgp summary**
3. **show ip route** [*address*]
4. **show mpls ldp bindings** [*network* {*mask* | *length*}]
5. **show ip cef** [*network* [*mask*]] [**longer-prefixes**] [**detail**]
6. **show mpls forwarding table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [- *label*] | **interface***interface* | **next-hop***address* |**lsp-tunnel** [*tunnel-id*]}] [**detail**]
7. **show ip bgp labels**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp summary** 例： `Router# show ip bgp summary`	（任意）BGP 接続すべての状況を表示します。 • **show ip bgp summary** コマンドを使用して、BGP セッションが CSC-CE ルータ上で稼働中であることを確認します。

	コマンドまたはアクション	目的
ステップ 3	**show ip route** [*address*] 例： `Router# show ip route 10.1.0.0`	（任意）IP ルーティング テーブルのエントリを表示します。 • **show ip route** コマンドを使用して、ローカルおよびリモートの PE ルータのループバック アドレスがルーティング テーブルに存在することを確認します。 （注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数ルートが、対応する VRF テーブルにインストールされていることを確認します。
ステップ 4	**show mpls ldp bindings** [*network* {*mask* | *length*}] 例： `Router# show mpls ldp bindings 10.2.0.0 255.255.255.255`	（任意）ラベル情報ベース（LIB）の内容を表示します。 • **show mpls ldp bindings** コマンドを使用して、ローカル PE ルータのプレフィックスが MPLS LDP バインディングに存在することを確認します。
ステップ 5	**show ip cef** [*network* [*mask*]] [**longer-prefixes**] [**detail**] 例： `Router# show ip cef 10.5.0.0 detail`	（任意）転送情報ベース（FIB）のエントリまたは FIB のサマリーを表示します。 • **show ip cef** コマンドと **show ip cef detail** コマンドを使用して、ローカルおよびリモートの PE ルータのプレフィックスが、Cisco Express Forwarding テーブルに存在することを確認します。 （注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数のルートとラベルが、対応する VRF テーブルにインストールされていることを確認します。
ステップ 6	**show mpls forwarding table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [- *label*] | **interface***interface* | **next-hop***address* |**lsp-tunnel** [*tunnel-id*]}] [**detail**] 例： `Router# show mpls forwarding-table 10.2.0.0 detail`	（任意）MPLS LFIB の内容を表示します。 • **show mpls forwarding-table** コマンドと **show mpls forwarding-table detail** コマンドを使用して、ローカルおよびリモートの PE ルータのプレフィックスが、MPLS 転送テーブルに存在することを確認します。 （注） CSC-PE と CSC-CE 間に複数パスを設定している場合は、CSC-CE から学習した同じ宛先への複数のルートとラベルが、対応する VRF ルーティング テーブルにインストールされていることを確認します。
ステップ 7	**show ip bgp labels** 例： `Router# show ip bgp labels`	（任意）EBGP ルート テーブルの MPLS ラベルに関する情報を表示します。 • **show ip bgp labels** コマンドを使用して、BGP ルーティング テーブルに、カスタマー キャリア MPLS VPN サービス プロバイダー

	コマンドまたはアクション	目的
		ネットワークのプレフィックスのラベルが含まれていることを確認します。

カスタマー キャリア ネットワークの設定

カスタマーキャリアネットワークを設定および確認するには、次の作業を実行します。手順を実行するには、カスタマーキャリアコア（P）ルータおよびカスタマーキャリアエッジ（PE）ルータに対して接続およびルーティング機能をセットアップする必要があります。

前提条件

BGP を使用してルートと MPLS ラベルを配布する MPLS VPN CSC ネットワークを設定する前に、カスタマー キャリア ルータで次のことを設定する必要があります。

- IGP ルーティング プロトコル：BGP、OSPF、IS-IS、EIGRP、スタティックなど。詳細については、『Configuring a Basic BGP Network』、『Configuring OSPF』、『Configuring a Basic IS-IS Network』、および『Configuring EIGRP』を参照してください。
- PE ルータ上での MPLS VPN 機能（階層型 VPN の場合のみ）。
- P ルータおよび PE ルータでのラベル配布プロトコル（LDP）（階層型 VPN の場合のみ）。詳細については、『How to Configure MPLS LDP』を参照してください。

（注） この項の作業を実行する前に、上のリストの項目を設定する必要があります。

カスタマー キャリアでの IP 接続の確認

カスタマー キャリアでの IP 接続を確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route**
5. **disable**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**ping** [*protocol*] {*host-name* | *system-address*} 例： `Router# ping ip 10.2.0.0`	AppleTalk、CLNS、IP、Novell、Apollo、VINES、DECnet、または 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、カスタマー キャリア コア ルータから別のカスタマー キャリア コア ルータへの接続を確認します。
ステップ 3	**trace** [*protocol*] [*destination*] 例： `Router# trace ip 10.1.0.0`	パケットがその宛先に送信されるときに実際に取るルートを検出します。 • **trace** コマンドを使用して、パケットがその最終的な宛先に到達するまでに通過するパスを確認します。**trace** コマンドは、2 つのルータが通信できない場合に問題のある箇所を分離するのに役立ちます。
ステップ 4	**show ip route** 例： `Router# show ip route`	IP ルーティング テーブルのエントリを表示します。 • **show ip route** コマンドを使用して、ホスト IP アドレス、ネクスト ホップ、インターフェイスなどを含む、ルーティング テーブル全体を表示します。
ステップ 5	**disable** 例： `Router# disable`	ユーザ モードに戻ります。

ルート リフレクタとしてのカスタマー キャリア コア ルータの設定

カスタマー キャリア コア（P）ルータをマルチプロトコル BGP プレフィックスのルート リフレクタとして設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
5. **address-family vpnv4** [**unicast**]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor***ip-address***route-reflector-client**
8. **exit-address-family**
9. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 200`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にラベルを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor 10.1.1.1 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。

	コマンドまたはアクション	目的
ステップ 5	**address-family vpnv4** [**unicast**] 例： `Router(config-router)# address-family vpnv4`	アドレス ファミリ 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 プレフィックスを使用する、BGP などのルーティング セッションを設定します。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.1.1.1 activate`	ネイバー BGP ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**neighbor***ip-address***route-reflector-client** 例： `Router(config-router-af)# neighbor 10.1.1.1 route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。 • *ip-address* 引数には、クライアントとして識別される BGP ネイバーの IP アドレスを指定します。
ステップ 8	**exit-address-family** 例： `Router(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Router(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーが、ユニキャストアドレスプレフィックスのみを交換します。ネイバーが、マルチキャストや VPNv4 などの他のアドレス プレフィックス タイプを交換できるようにするには、上で示しているように、アドレスファミリ コンフィギュレーションモードで **neighbor activate** コマンドを使用して、ネイバーをアクティブにする必要もあります。

ルータ コンフィギュレーション モードで **neighbor route-reflector-client** コマンドを使用して定義されたルート リフレクタとクライアント（ネイバーまたは内部 BGP ピア グループ）は、デフォ

ルトでこれらのクライアントとの間でユニキャストアドレスプレフィックスを反映します。ルートリフレクタおよびクライアントで、マルチキャストなどの他のアドレスファミリのプレフィックスを反映できるようにするには、上で示しているように、**neighbor route-reflector-client** コマンドを使用して、アドレス ファミリ コンフィギュレーション モードでリフレクタおよびクライアントを定義します。

階層型 VPN のカスタマー サイトの設定

（注） この項は、BGP を使用してルートおよび MPLS ラベルを配布するカスタマー キャリア ネットワークのみに適用されます。

階層型 VPN のカスタマー サイトを設定および確認するには、次の作業を実行します。

（注） ここで説明する内容は、階層型 VPN のみに適用されます。

階層型 VPN の PE ルータでの VPN の定義

PE ルータで VPN を定義するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map***route-map*
7. **ip vrf forwarding***vrf-name*
8. **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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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 vpn2`	VRF ルーティング テーブルとシスコ エクスプレス フォワーディング テーブルを作成し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF に割り当てられた名前です。
ステップ 4	**rd***route-distinguisher* 例： `Router(config-vrf)# rd 200:1`	VRF のルーティング 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。
ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Router(config-vrf)# route-target export 200:1`	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、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 6	**import map***route-map* 例： `Router(config-vrf)# import map map23`	VRF のインポート ルート マップを作成します。 • *route-map* 引数には、VRF のインポート ルート マップとして使用されるルート マップを指定します。
ステップ 7	**ip vrf forwarding***vrf-name* 例： `Router(config-vrf)# ip vrf forwarding vpn2`	VPN 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* 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 8	**exit** 例： `Router(config-vrf)# 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。

階層型 VPN の PE ルータでの BGP ルーティング セッションの設定

PE ルータで PE から CE へのルータ通信の BGP ルーティング セッションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **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。 • 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： `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 bgp***as-number* 例： `Router(config)# router bgp 200`	BGP プロセスを実行するようにルータを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネット

	コマンドまたはアクション	目的
		ワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Router(config-router)# address-family ipv4 multicast`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router-af)# neighbor 10.5.5.5 remote-as 300`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Router(config-router-af)# neighbor 10.1.0.0 activate`	ネイバー ルータとの情報交換をイネーブルにします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**end** 例： `Router(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

階層型 VPN の各 PE ルータでのラベルの確認

階層型 VPN の各 PE ルータでラベルを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip route vrf***vrf-name* [*prefix*]
3. **show mpls forwarding-table** [**vrf***vrf-name*] [*prefix*] [**detail**]
4. **show ip cef** [*network* [*mask* [**longer-prefix**]]] [**detail**]
5. **show ip cef vrf***vrf-name* [*ip-prefix*]
6. **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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip route vrf***vrf-name* [*prefix*] 例： `Router# show ip route vrf vpn2 10.5.5.5`	（任意）VRF 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。 • **show ip route vrf** コマンドを使用して、ローカルおよびリモートの CE ルータのループバック アドレスが、PE ルータのルーティング テーブルに存在することを確認します。
ステップ 3	**show mpls forwarding-table** [**vrf***vrf-name*] [*prefix*] [**detail**] 例： `Router# show mpls forwarding-table vrf vpn2 10.1.0.0`	（任意）LFIB の内容を表示します。 • **show mpls forwarding-table** コマンドを使用して、ローカルおよびリモートの CE ルータのプレフィックスが、MPLS 転送テーブルに存在し、指定したプレフィックスが非タグ付きであることを確認します。
ステップ 4	**show ip cef** [*network* [*mask* [**longer-prefix**]]] [**detail**] 例： `Router# show ip cef 10.2.0.0`	（任意）IP アドレス情報に基づく FIB 内に特定のエントリが表示されます。 • **show ip cef** コマンドを使用して、ローカルおよびリモートの PE ルータのプレフィックスが、Cisco Express Forwarding テーブルに存在することを確認します。
ステップ 5	**show ip cef vrf***vrf-name* [*ip-prefix*] 例： `Router# show ip cef vrf vpn2 10.3.0.0`	（任意）VRF に関連付けられているシスコ エクスプレス フォワーディング テーブルを表示します。 • **show ip cef vrf** コマンドを使用して、リモート CE ルータのプレフィックスが、Cisco Express Forwarding テーブルに存在することを確認します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router# exit`	（任意）終了して、ユーザ EXEC モードに戻ります。

階層型 VPN の CE ルータの設定

階層型 VPN の CE ルータを設定するには、次の作業を実行します。この設定は、階層型トポロジではない MPLS VPN の場合の設定と同じです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface***typenumber*
5. **ip addres***ip-addressmask* [**secondary**]
6. **exit**
7. **router bgp***as-number*
8. **redistribute***protocol*
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
10. **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。 • 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： `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。

	コマンドまたはアクション	目的
ステップ 3	**ip cef** [**distributed**] 例： `Router(config)# ip cef distributed`	ルート プロセッサ カードでシスコ エクスプレス フォワーディングをイネーブルにします。 • **distributed** キーワードを使用すると、分散型シスコ エクスプレス フォワーディング動作が有効になります。シスコエクスプレスフォワーディング情報は、複数のラインカードに分散されます。ラインカードが、エクスプレス フォワーディングを実行します。 （注） Cisco ASR 1000 シリーズのアグリゲーション サービス ルータの場合は、**distributed** キーワードは必須です。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 0`	インターフェイス タイプを設定し、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。 • *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。 • ループバック インターフェイスは、常に稼働状態にあるインターフェイスをエミュレートするソフトウェア専用インターフェイスを示します。これは、すべてのプラットフォームでサポートされている仮想インターフェイスです。 • *number* 引数は、作成または設定するループバック インターフェイスの数です。作成可能なループバック インターフェイスの数に制限はありません。
ステップ 5	**ip addres***ip-addressmask* [**secondary**] 例： `Router(config-if)# ip address 10.8.0.0 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IPアドレスになります。
ステップ 6	**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 モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	**router bgp***as-number* 例： `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 8	**redistribute***protocol* 例： `Router(config-router)# redistribute connected`	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。 • *protocol* 引数では、ルートの再配布元となるソース プロトコルを指定します。次のいずれかのキーワードを指定できます：**bgp**、**connected**、**egp**、**igrp**、**isis**、**mobile**、**ospf**、**static** [**ip**]、**rip**。 **connected** キーワードは、IP がインターフェイスでイネーブルな場合に自動的に確立されるルートを示します。Open Shortest Path First（OSPF）や IS-IS などのルーティング プロトコルの場合、これらのルートは自律システムに対して外部として再配布されます。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Router(config-router)# neighbor 10.8.0.0 remote-as 100`	リモート自律システムでのネイバーの IP アドレスを、ローカル ルータのマルチプロトコル BGP ネイバー テーブルに追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 10	**end** 例： `Router(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

カスタマー サイトでの IP 接続の確認

カスタマー サイトでの IP 接続を確認するには、次の作業を実行します。

手順の概要

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

手順の詳細

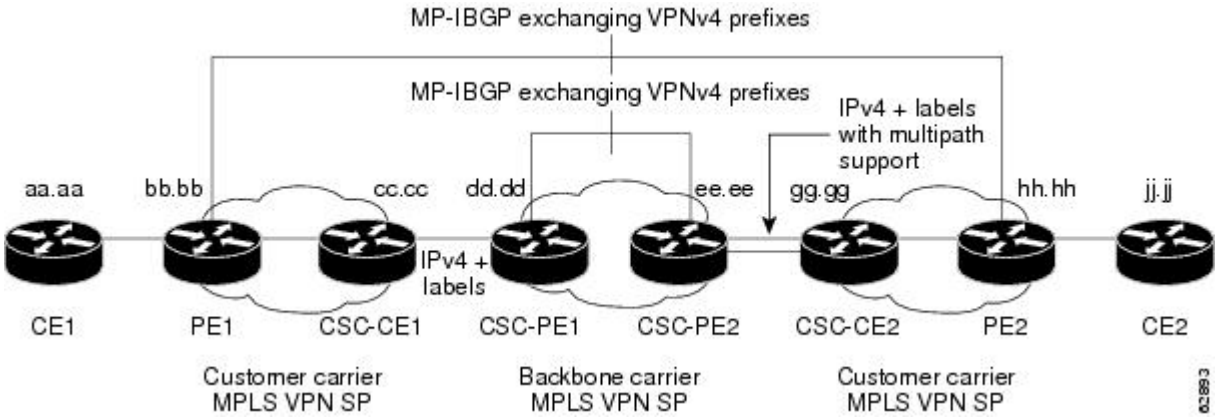
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip route** [*ip-address* [*mask*]] [**longer-prefixes**]	*protocol* [*process-id*]	**list** [*access-list-number*	*access-list-name*]	**static download** 例： `Router# show ip route 10.5.5.5`	（任意）ルーティング テーブルの現在の状態を表示します。 • **show ip route ip-address** コマンドを使用して、PE ルータを介して学習したリモート CE ルータのループバック アドレスが、ローカル CE ルータのルーティング テーブルに存在することを確認します。
ステップ 3	**ping** [*protocol*] {*host-name*	*system-address*} 例： `Router# ping 10.5.5.5`	Apollo、AppleTalk、コネクションレス型ネットワーク サービス（CLNS）、DECnet、IP、Novell IPX、VINES、または XNS ネットワーク上で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、カスタマー サイトのルータ間の接続を確認します。
ステップ 4	**trace** [*protocol*] [*destination*] 例： `Router# trace ip 10.5.5.5`	パケットがその宛先に送信されるときに実際に取るルートを検出します。 • **trace** コマンドを使用して、カスタマー サイトのパケットのパスを追跡します。 • デフォルト以外のパラメータを使用し、拡張 **trace** テストを呼び出すには、宛先の引数を指定せずに **trace** コマンドを入力します。ダイアログに従って手順を実行し、目的のパラメータを選択します。

	コマンドまたはアクション	目的
ステップ 5	**disable** 例： `Router# disable`	（任意）終了して、ユーザ EXEC モードに戻ります。

BGP を使用する MPLS VPN CSC の設定例

次の図に、IPv4 ルートと MPLS ラベルを交換するためのサンプル CSC トポロジを示します。この図は、IPv4 ルートおよび MPLS ラベルを交換するために Carrier Supporting Carrier ルータを設定および確認する場合の参照として使用します。

図 *23*：*IPv4* ルートと *MPLS* ラベルを交換するためのサンプル *CSC* トポロジ



次の表で、上記の図に示されているサンプル設定を説明します。

表 *9*：図 *1* に示すサンプル設定の説明

ルータ	説明
CE1 および CE2	エンドカスタマーに属しています。CE1 ルータと CE2 ルータは、PE ルータから学習したルートを交換します。 エンド カスタマーは、カスタマー キャリアから VPN サービスを購入します。

ルータ	説明
PE1 および PE2	MPLS VPN サービスを提供するように設定された、カスタマー キャリア ネットワークの一部です。PE1 および PE2 は、VPNv4 IBGP セッションを使用してピアリングして、MPLS VPN ネットワークを形成します。
CSC-CE1 おおび CSC-CE2	カスタマーキャリア ネットワークの一部です。CSC-CE1 ルータと CSC-CE2 ルータは、MPLS ラベルとともに IPv4 BGP アップデートを交換し、IGP（この例では OSPF）との間で PE ループバック アドレスを再配布します。 カスタマー キャリアは、バックボーン キャリアから Carrier Supporting Carrier VPN サービスを購入します。
CSC-PE1 および CSC-PE2	Carrier Supporting Carrier VPN サービスを提供するように設定された、バックボーン キャリアのネットワークの一部です。CSC-PE1 および CSC-PE2 は、VPNv4 IP BGP セッションを使用してピアリングして、MPLS VPN ネットワークを形成します。VRF では、CSC-PE1 と CSC-PE2 は、CSC-CE ルータを使用してピアリングします。CSC-CE ルータは、IPv4 EBGP セッションを使用して、ルートとともに MPLS ラベルを伝送するように設定されています。

バックボーン キャリア コアの設定：例

この項に含まれている、バックボーンキャリア コアの設定例および確認例は、次のとおりです。

CSC コアにおける IP 接続と LDP 設定の確認：例

CSC-CE1 で次のコマンドを入力して、CSC-PE2 が CSC-PE1 から到達可能であることを確認します。

```
Router# ping 10.5.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

CSC-CE1 で次のコマンドを入力して、CSC-PE1 から CSC-PE2 へのパスを確認します。

```
Router# trace 10.5.5.5
```

```
Type escape sequence to abort.
Tracing the route to 10.5.5.5
  1 10.5.5.5 0 msec 0 msec *
```

次に示すように、CSC-PE ルータ プレフィックスが、MPLS 転送テーブルに存在することを確認します。

```
Router# show mpls forwarding-table
Local     Outgoing     Prefix or          Bytes tag    Outgoing      Next Hop
tag       tag or VC    Tunnel Id          switched     interface
16        2/nn         dd.dd.dd.dd/32       0          AT2/1/0.1     point2point
17        16           bb.bb.bb.bb/32[V]    30204      Et1/0         pp.0.0.1
21        Pop tag      cc.cc.cc.cc/32[V]    0          Et1/0         pp.0.0.1
22        Pop tag      nn.0.0.0/8[V]        570        Et1/0         pp.0.0.1
23        Aggregate    pp.0.0.0/8[V]        0
2         2/nn         gg.gg.gg.gg/32[V]    0          AT3/0.1       point2point
8         2/nn         hh.hh.hh.hh/32[V]    15452      AT3/0.1       point2point
29        2/nn         qq.0.0.0/8[V]        0          AT3/0.1       point2point
30        2/nn         ss.0.0.0/8[V]        0          AT3/0.1       point2point
```

次に示すように、コアでの LDP ディスカバリ プロセスのステータスを確認します。

```
Router# show mpls ldp discovery
Local LDP Identifier:
  ee.ee.ee.ee:0
  Discovery Sources:
  Interfaces:
    ATM2/1/0.1 (ldp): xmit/recv
      TDP Id: dd.dd.dd.dd:1
```

次に示すように、コアでの LDP セッションのステータスを確認します。

```
Router# show mpls ldp neighbor
Peer LDP Ident: dd.dd.dd.dd:1; Local LDP Ident ee.ee.ee.ee:1
       TCP connection: dd.dd.dd.dd.646 - ee.ee.ee.ee.11007
       State: Oper; Msgs sent/rcvd: 20/21; Downstream on demand
       Up time: 00:14:56
       LDP discovery sources:
         ATM2/1/0.1, Src IP addr: dd.dd.dd.dd
```

次に示すように、転送テーブル（プレフィックス、ネクストホップ、およびインターフェイス）を確認します。

```
Router# show ip cef
Prefix             Next Hop          Interface
0.0.0.0/0          drop              Null0 (default route handler entry)
0.0.0.0/32         receive
dd.dd.dd.dd/32     dd.dd.dd.dd       ATM2/1/0.1
ee.ee.ee.ee/32     receive
224.0.0.0/4        drop
224.0.0.0/24       receive
255.255.255.255/32 receive
```

（注） CSC-CE ルータのラベルの確認：例，（240 ページ）も参照してください。

次に示すように、LDP を使用するようにインターフェイスが設定されていることを確認します。

```
Router# show mpls interfaces
Interface              IP            Tunnel   Operational
Ethernet0/1            Yes (ldp)     No       Yes
```

ホスト IP アドレス、ネクスト ホップ、インターフェイスなどを含む、ルーティング テーブル全体を表示します。

```
Router# show ip route
```

```
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
Gateway of last resort is not set
     dd.0.0.0/32 is subnetted, 1 subnets
O       dd.dd.dd.dd [110/7] via dd.dd.dd.dd, 00:16:42, ATM2/1/0.1
     ee.0.0.0/32 is subnetted, 1 subnets
C       ee.ee.ee.ee is directly connected, Loopback0
```

CSC-PE ルータの VRF の設定：例

次に、CSC-PE ルータの VPN ルーティングおよび転送（VRF）インスタンスを設定する例を示します。

```
ip cef distributed
ip vrf vpn1
rd 100:1
route target both 100:1
!
```

バックボーン キャリアにおける VPN 接続の Multiprotocol BGP の設定：例

次に、バックボーン キャリアにおける VPN 接続のマルチプロトコル BGP（MP-BGP）を設定する例を示します。

```
ip cef distributed
ip vrf vpn1
rd 100:1
route target both 100:1
hostname csc-pe1
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.ee.ee.ee remote-as 100
 neighbor ee.ee.ee.ee update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee send-community extended
 bgp dampening 30
 exit-address-family
 !
router bgp 100
. . .
! (BGP IPv4 to CSC-CE router from CSC-PE router)
!
 address-family ipv4 vrf vpn1
 neighbor ss.0.0.2 remote-as 200
 neighbor ss.0.0.2 activate
 neighbor ss.0.0.2 as-override
 neighbor ss.0.0.2 advertisement-interval 5
 neighbor ss.0.0.2 send-label
 no auto-summary
 no synchronization
 bgp dampening 30
 exit-address-family
!
```

CSC-PE ルータと CSC-CE ルータ間のリンクの設定：例

ここでは、次の例について説明します。

CSC-PE ルータの設定：例

次に、CSC-PE ルータを設定する例を示します。

```
ip cef
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
mpls label protocol ldp
!
interface Loopback0
 ip address dd.dd.dd.dd 255.255.255.255
!
interface Ethernet3/1
 ip vrf forwarding vpn1
 ip address pp.0.0.2 255.0.0.0
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
 ip unnumbered Loopback0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet3/1
 network dd.dd.dd.dd 0.0.0.0 area 100
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.ee.ee.ee remote-as 100
 neighbor ee.ee.ee.ee update-source Loopback0
!
address-family vpnv4                                !VPNv4 session with CSC-PE2
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee send-community extended
 bgp dampening 30
 exit-address-family
!
 address-family ipv4 vrf vpn1
 neighbor pp.0.0.1 remote-as 200
 neighbor pp.0.0.1 activate
 neighbor pp.0.0.1 as-override
 neighbor pp.0.0.1 advertisement-interval 5
 neighbor pp.0.0.1 send-label
 no auto-summary
```

```
 no synchronization
 bgp dampening 30
 exit-address-family
```

CSC-CE ルータの設定：例

次に、CSC-CE ルータを設定する例を示します。

```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address cc.cc.cc.cc 255.255.255.255
!
interface Ethernet3/0
 ip address pp.0.0.1 255.0.0.0
!
interface Ethernet4/0
 ip address nn.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets                    !Exchange routes
 redistribute bgp 200 metric 3 subnets             !learned from PE1
 passive-interface ATM1/0
 passive-interface Ethernet3/0
 network cc.cc.cc.cc 0.0.0.0 area 200
 network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor pp.0.0.2 remote-as 100
 neighbor pp.0.0.2 update-source Ethernet3/0
 no auto-summary
!
address-family ipv4
 redistribute connected
 redistribute ospf 200 metric 4 match internal
 neighbor pp.0.0.2 activate
 neighbor pp.0.0.2 send-label
 no auto-summary
 no synchronization
 bgp dampening 30
 exit-address-family
```

CSC-PE ルータのラベルの確認：例

次に、CSC-PE ルータの設定を確認する例を示します。

BGP セッションが、CSC-PE ルータと CSC-CE ルータ間で稼働中であることを確認します。State/PfxRcd カラムのデータをチェックして、各セッション時にプレフィックスが学習されていることを確認します。

```
Router# show ip bgp vpnv4 all summary
BBGP router identifier 10.5.5.5, local AS number 100
BGP table version is 52, main routing table version 52
```

```
12 network entries and 13 paths using 2232 bytes of memory
6 BGP path attribute entries using 336 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 16/4 prefixes, 27/14 paths, scan interval 5 secs
Neighbor        V   AS     MsgRcvd MsgSent  TblVer InQ  OutQ Up/Down  State/PfxRcd
10.5.5.5        4  100     7685    7686      52    0       0 21:17:04       6
10.0.0.2        4  200     7676    7678      52    0       0 21:16:43       7
```

MPLS インターフェイスが稼働中であることを確認します。また、LDP 対応インターフェイスで、LDP が稼働中であることが示されていることを確認します。EBGP によってラベルが配布されるため、VRF では LDP がオフになっています。

```
Router# show mpls interfaces all
Interface              IP            Tunnel   Operational
GigabitEthernet6/0     Yes (ldp)     No       Yes
VRF vpn1:
Ethernet3/1            No            No       Yes
```

次のように、ローカル PE ルータのプレフィックスが、CSC-PE ルータのルーティング テーブルに存在することを確認します。

```
Router# show ip route vrf vpn2 10.5.5.5
Routing entry for 10.5.5.5/32
  Known via "bgp 100", distance 20, metric 4
  Tag 200, type external
  Last update from pp.0.0.2 21:28:39 ago
  Routing Descriptor Blocks:
  * pp.0.0.2, from pp.0.0.2, 21:28:39 ago
      Route metric is 4, traffic share count is 1
      AS Hops 1, BGP network version 0
```

次のように、リモート PE ルータのプレフィックスが、CSC-PE ルータのルーティング テーブルに存在することを確認します。

```
Router# show ip route vrf vpn2 10.5.5.5
Routing entry for 10.5.5.5/32
  Known via "bgp 100", distance 200, metric 4
  Tag 200, type internal
  Last update from 10.1.0.0 21:27:39 ago
  Routing Descriptor Blocks:
  * 10.1.0.0 (Default-IP-Routing-Table), from 10.1.0.0, 21:27:39 ago
      Route metric is 4, traffic share count is 1
      AS Hops 1, BGP network version 0
```

カスタマー キャリア MPLS VPN サービス プロバイダー ネットワークのプレフィックスが、BGP テーブルに存在し、適切なラベルを持っていることを確認します。

```
Router# show ip bgp vpnv4 vrf vpn2 labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (vpn1)
   cc.cc.cc.cc/32   pp.0.0.2        22/imp-null
   bb.bb.bb.bb/32   pp.0.0.2        27/20
   hh.hh.hh.hh/32   ee.ee.ee.ee     34/35
   gg.gg.gg.gg/32   ee.ee.ee.ee     30/30
   nn.0.0.0         pp.0.0.2        23/imp-null
   ss.0.0.0         ee.ee.ee.ee     33/34
   pp.0.0.0         pp.0.0.2        25/aggregate(vpn1)
```

次のように、ローカル カスタマー キャリア MPLS VPN サービス プロバイダーの PE ルータ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。

```
Router# show ip cef vrf vpn2 10.1.0.0
10.1.0.0/32, version 19, cached adjacency pp.0.0.2
```

```
0 packets, 0 bytes
  tag information set
    local tag: 27
    fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
  via pp.0.0.2, 0 dependencies, recursive
    next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
    valid cached adjacency
    tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}

Router# show ip cef vrf vpn2 10.1.0.0 detail
10.1.0.0/32, version 19, cached adjacency pp.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: 27
    fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
  via pp.0.0.2, 0 dependencies, recursive
    next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
    valid cached adjacency
    tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
```

次のように、ローカル カスタマー キャリア MPLS VPN サービス プロバイダーの PE ルータのプレフィックスが、MPLS 転送テーブルに存在することを確認します。

```
Router# show mpls forwarding-table vrf vpn2 10.1.0.0
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
27     20          10.1.0.0/32[V]   958048     Et3/1       pp.0.0.2

Router# show mpls forwarding-table vrf vpn2 10.1.0.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
27     20 10.1.0.0/32[V]             958125     Et3/1      pp.0.0.2
        MAC/Encaps=14/18, MTU=1500, Tag Stack{20}
        00B04A74A05400B0C26E10558847 00014000
        VPN route: vpn1
        No output feature configured
    Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

次のように、リモート カスタマー キャリア MPLS VPN サービス プロバイダーの PE ルータ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。

```
Router# show ip cef vrf vpn2 10.3.0.0
10.3.0.0/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: 34
    fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
  via ee.ee.ee.ee, 0 dependencies, recursive
    next hop rr.0.0.2, GigabitEthernet6/0 via ee.ee.ee.ee/32
    valid cached adjacency
    tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}

Router# show ip cef vrf vpn2 10.3.0.0 detail
hh.hh.hh.hh/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: 34
    fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
  via ee.ee.ee.ee, 0 dependencies, recursive
    next hop rr.0.0.2, GigabitEthernet6/0 via ee.ee.ee.ee/32
    valid cached adjacency
    tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
```

次のように、リモート カスタマー キャリア MPLS VPN サービス プロバイダーの PE ルータのプレフィックスが、MPLS 転送テーブルに存在することを確認します。

```
Router# show mpls forwarding-table vrf vpn2 10.3.0.0
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
34     35          hh.hh.hh.hh/32[V] 139034     Gi6/0      rr.0.0.2
```

```
Router# show mpls forwarding-table vrf vpn2 10.3.0.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
34     35          hh.hh.hh.hh/32[V] 139034     Gi6/0      rr.0.0.2
        MAC/Encaps=14/18, MTU=1500, Tag Stack{35}
        00B0C26E447000B0C26E10A88847 00023000
        VPN route: vpn1
        No output feature configured
    Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

CSC-CE ルータのラベルの確認：例

次に、CSC-CE ルータの設定を確認する例を示します。

次のように、BGP セッションが稼働中であることを確認します。

```
Router# show ip bgp summary
BGP router identifier cc.cc.cc.cc, local AS number 200
BGP table version is 35, main routing table version 35
14 network entries and 14 paths using 2030 bytes of memory
3 BGP path attribute entries using 168 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 1 history paths, 0 dampened paths
BGP activity 17/67 prefixes, 29/15 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
pp.0.0.1        4   100    7615    7613       35    0    0 21:06:19        5
```

次のように、ローカル PE ルータのループバック アドレスがルーティング テーブルに存在すること確認します。

```
Router# show ip route 10.1.0.0
Routing entry for 10.1.0.0/32
  Known via "ospf 200", distance 110, metric 101, type intra area
  Redistributing via bgp 200
  Advertised by bgp 200 metric 4 match internal
  Last update from nn.0.0.1 on Ethernet4/0, 00:34:08 ago
  Routing Descriptor Blocks:
  * nn.0.0.1, from bb.bb.bb.bb, 00:34:08 ago, via Ethernet4/0
      Route metric is 101, traffic share count is 1
```

次のように、リモート PE ルータのループバック アドレスが、ルーティング テーブルに存在すること確認します。

```
Router# show ip route 10.5.5.5
Routing entry for 10.5.5.5/32
  Known via "bgp 200", distance 20, metric 0
  Tag 100, type external
  Redistributing via ospf 200
  Advertised by ospf 200 metric 3 subnets
  Last update from pp.0.0.1 00:45:16 ago
  Routing Descriptor Blocks:
  * pp.0.0.1, from pp.0.0.1, 00:45:16 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2, BGP network version 0
```

次のように、ローカル PE ルータのプレフィックスが、MPLS LDP バインディングに存在することを確認します。

```
Router# show mpls ldp bindings 10.1.0.0 255.255.255.255
  tib entry: 10.1.0.0/32, rev 20
        local binding:  tag: 20
        remote binding: tsr: 10.1.0.0:0, tag: imp-null
```

次のように、ローカル PE ルータ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。

```
Router# show ip cef 10.1.0.0
10.1.0.0/32, version 46, cached adjacency nn.0.0.1
0 packets, 0 bytes
  tag information set
    local tag: 20
  via nn.0.0.1, Ethernet4/0, 0 dependencies
    next hop nn.0.0.1, Ethernet4/0
    unresolved
    valid cached adjacency
    tag rewrite with Et4/0, nn.0.0.1, tags imposed {}
```

次のように、ローカル PE ルータのプレフィックスが、MPLS 転送テーブルに存在することを確認します。

```
Router# show mpls forwarding-table 10.1.0.0
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
20     Pop tag     bb.bb.bb.bb/32    893397     Et4/0      nn.0.0.1

Router# show mpls forwarding-table 10.1.0.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
20     Pop tag     bb.bb.bb.bb/32    893524     Et4/0      nn.0.0.1
        MAC/Encaps=14/14, MTU=1504, Tag Stack{}
        00074F83685400B04A74A0708847
        No output feature configured
    Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

次のように、BGP ルーティング テーブルに、カスタマー キャリア MPLS VPN サービス プロバイダー ネットワークのプレフィックスのラベルが含まれていることを確認します。

```
Router# show ip bgp labels
Network          Next Hop         In Label/Out Label
cc.cc.cc.cc/32   0.0.0.0          imp-null/exp-null
bb.bb.bb.bb/32   nn.0.0.1         20/exp-null
hh.hh.hh.hh/32   pp.0.0.1         26/34
gg.gg.gg.gg/32   pp.0.0.1         23/30
nn.0.0.0         0.0.0.0          imp-null/exp-null
ss.0.0.0         pp.0.0.1         25/33
pp.0.0.0         0.0.0.0          imp-null/exp-null
pp.0.0.1/32      0.0.0.0          16/exp-null
```

次のように、リモート PE ルータ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。

```
Router# show ip cef 10.5.5.5
10.5.5.5/32, version 54, cached adjacency pp.0.0.1
0 packets, 0 bytes
  tag information set
    local tag: 26
    fast tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}
  via pp.0.0.1, 0 dependencies, recursive
    next hop pp.0.0.1, Ethernet3/0 via pp.0.0.1/32
    valid cached adjacency
    tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}
```

次のように、リモート PE ルータのプレフィックスが、MPLS 転送テーブルに存在することを確認します。

```
Router# show mpls forwarding-table 10.5.5.5
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
26     34          hh.hh.hh.hh/32    81786      Et3/0      pp.0.0.1

Router# show mpls forwarding-table 10.5.5.5 detail
```

```
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
26     34          hh.hh.hh.hh/32    81863      Et3/0      pp.0.0.1
        MAC/Encaps=14/18, MTU=1500, Tag Stack{34}
        00B0C26E105500B04A74A0548847 00022000
        No output feature configured
    Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

カスタマー キャリア ネットワークの設定：例

この項のカスタマー キャリアの設定例と確認例には、次の設定と確認が含まれます。

カスタマー キャリアでの IP 接続の確認：例

次のコマンドを入力して、カスタマー キャリア コア ルータ間（CE1 から CE2）の接続を確認します。

```
Router# ping 10.2.0.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to jj.jj.jj.jj, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
```

次のように、パケットが、最終的な宛先（CE1 から CE2）に到達するまでに通過するパスを確認します。

```
Router# trace 10.2.0.0
Type escape sequence to abort.
Tracing the route to 10.2.0.0
  1 mm.0.0.2 0 msec 0 msec 4 msec
  2 nn.0.0.2 [MPLS: Labels 20/21 Exp 0] 8 msec 8 msec 12 msec
  3 pp.0.0.2 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 12 msec
  4 ss.0.0.1 [MPLS: Labels 17/21 Exp 0] 8 msec 8 msec 12 msec
  5 ss.0.0.2 [MPLS: Labels 16/21 Exp 0] 8 msec 8 msec 12 msec
  6 tt.0.0.1 [AS 200] [MPLS: Label 21 Exp 0] 8 msec 8 msec 8 msec
  7 tt.0.0.2 [AS 200] 8 msec 4 msec *
```

次のように、パケットが、最終的な宛先（CE2 から CE1）に到達するまでに通過するパスを確認します。

```
Router# trace 10.1.0.0
Type escape sequence to abort.
Tracing the route to 10.1.0.0
  1 tt.0.0.1 0 msec 0 msec 0 msec
  2 qq.0.0.2 [MPLS: Labels 18/21 Exp 0] 8 msec 12 msec 12 msec
  3 ss.0.0.1 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 8 msec
  4 pp.0.0.2 [MPLS: Labels 17/21 Exp 0] 12 msec 8 msec 8 msec
  5 pp.0.0.1 [MPLS: Labels 16/21 Exp 0] 12 msec 12 msec 8 msec
  6 mm.0.0.2 [AS 200] [MPLS: Label 21 Exp 0] 12 msec 8 msec 12 msec
  7 mm.0.0.1 [AS 200] 4 msec 4 msec *
```

ルート リフレクタとしてのカスタマー キャリア コア ルータの設定：例

次に、アドレス ファミリを使用して、内部 BGP ピア 10.1.1.1 をユニキャスト プレフィックスとマルチキャスト プレフィックスの両方のルート リフレクタ クライアントとして設定する例を示します。

```
router bgp 200
 address-family vpnv4
```

```
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 route-reflector-client

router bgp 100
 address-family vpnv4
  neighbor xx.xx.xx.xx activate
  neighbor xx.xx.xx.xx route-reflector-client
   ! xx.xx.xx,xx is a PE router
  neighbor xx.xx.xx.xx send-community extended
 exit address-family
! You need to configure your peer BGP neighbor.
```

階層型 VPN のカスタマー サイトの設定：例

ここでは、カスタマー サイトに関する次の設定例および確認例について説明します。

階層型 VPN の PE ルータの設定：例

次に、PE ルータを設定する例を示します。

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Ethernet3/0
 ip address nn.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/3
 ip vrf forwarding vpn2
 ip address mm.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet3/3
 network bb.bb.bb.bb 0.0.0.0 area 200
 network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor hh.hh.hh.hh remote-as 200
 neighbor hh.hh.hh.hh update-source Loopback0
!
address-family vpnv4                                !VPNv4 session with PE2
 neighbor hh.hh.hh.hh activate
 neighbor hh.hh.hh.hh send-community extended
 bgp dampening 30
 exit-address-family
!
 address-family ipv4 vrf vpn2
```

```
 neighbor mm.0.0.1 remote-as 300
 neighbor mm.0.0.1 activate
 neighbor mm.0.0.1 as-override
 neighbor mm.0.0.1 advertisement-interval 5
no auto-summary
 no synchronization
 bgp dampening 30
 exit-address-family
```

階層型 VPN の各 PE ルータでのラベルの確認：例

次に、階層型 VPN での PE ルータの設定を確認する例を示します。

次のように、ローカル CE ルータのループバック アドレスが、PE1 ルータのルーティング テーブルに存在することを確認します。

```
Router# show ip route vrf vpn2 10.2.2.2
Routing entry for 10.2.2.2/32
  Known via "bgp 200", distance 20, metric 0
  Tag 300, type external
  Last update from mm.0.0.2 20:36:59 ago
  Routing Descriptor Blocks:
  * mm.0.0.2, from mm.0.0.2, 20:36:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1, BGP network version 0
```

次のように、ローカルCEルータのプレフィックスが、MPLS転送テーブルに存在し、プレフィックスが非タグ付きであることを確認します。

```
Router# show mpls forwarding-table vrf vpn2 10.2.2.2
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
23     Untagged    aa.aa.aa.aa/32[V] 0          Et3/3      mm.0.0.2
```

次のように、リモート PE ルータ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。

```
Router# show ip cef 10.5.5.5

10.5.5.5/32, version 31, cached adjacency nn.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: 31
    fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}
  via nn.0.0.2, Ethernet3/0, 2 dependencies
    next hop nn.0.0.2, Ethernet3/0
    unresolved
    valid cached adjacency
    tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}
```

次のように、リモート CE ルータのループバック アドレスが、ルーティング テーブルに存在すること確認します。

```
Router# show ip route vrf vpn2 10.2.0.0
Routing entry for 10.2.0.0/32
  Known via "bgp 200", distance 200, metric 0
  Tag 300, type internal
  Last update from hh.hh.hh.hh 20:38:49 ago
  Routing Descriptor Blocks:
  * hh.hh.hh.hh (Default-IP-Routing-Table), from hh.hh.hh.hh, 20:38:49 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1, BGP network version 0
```

次のように、リモート CE ルータのプレフィックスが MPLS 転送テーブルに存在すること、および発信インターフェイスが存在することを確認します。

```
Router# show mpls forwarding-table vrf vpn2 10.2.0.0
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
None   26          jj.jj.jj.jj/32    0          Et3/0      nn.0.0.2
```

次のように、リモート CE ルータ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。

```
Router# show ip cef vrf vpn2 10.2.0.0
10.2.0.0/32, version 12, cached adjacency nn.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: VPN route head
    fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}
  via hh.hh.hh.hh, 0 dependencies, recursive
    next hop nn.0.0.2, Ethernet3/0 via hh.hh.hh.hh/32
    valid cached adjacency
    tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}
```

次のように、ローカル PE ルータ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。

```
Router# show ip cef 10.1.0.0
10.1.0.0/32, version 9, connected, receive
  tag information set
    local tag: implicit-null
```

階層型 VPN の CE ルータの設定：例

次に、CE ルータを設定する例を示します。

```
ip cef distributed
interface Loopback0
ip address 10.3.0.0 255.255.255.255
!
interface FastEthernet0/3/3
 ip address mm.0.0.1 255.0.0.0
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected                          !Redistributing routes into BGP
 neighbor mm.0.0.2 remote-as 200                 !to send to PE1
 neighbor mm.0.0.2 advertisement-interval 5
 no auto-summary
```

カスタマー サイトでの IP 接続の確認：例

次に、カスタマー サイトで IP 接続を確認する例を示します。

次のように、PE ルータから学習した、リモート CE ルータのループバック アドレスが、ローカル ルータのルーティング テーブルに存在することを確認します。

```
Router# show ip route 10.2.0.0
Routing entry for 10.2.0.0/32
  Known via "bgp 300", distance 20, metric 0
  Tag 200, type external
```

```
Redistributing via ospf 300
Advertised by ospf 300 subnets
Last update from mm.0.0.1 20:29:35 ago
Routing Descriptor Blocks:
* mm.0.0.1, from mm.0.0.1, 20:29:35 ago
    Route metric is 0, traffic share count is 1
    AS Hops 2
```

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
LDP	『MPLS Label Distribution Protocol』
MPLS	『MPLS Product Literature』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1164	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1171	『*A Border Gateway Protocol 4*』

RFC	タイトル
RFC 1700	『*Assigned Numbers*』
RFC 1966	『*BGP Route Reflection: An Alternative to Full Mesh IBGP*』
RFC 2283	『*Multiprotocol Extensions for BGP-4*』
RFC 2547	『*BGP/MPLS VPNs*』
RFC 2842	『*Capabilities Advertisement with BGP-4*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3107	『*Carrying Label Information in BGP-4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

BGP を使用する MPLS VPN CSC の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：*BGP* を使用する *MPLS VPN CSC* の機能情報

機能名	リリース	機能情報
MPLS VPN--Carrier Supporting Carrier--IPv4 BGP ラベル配布	12.0(21)ST 12.0(22)S 12.0(23)S 12.2(13)T 12.0(24)S 12.2(14)S 12.0(27)S 12.0(29)S Cisco IOS XE Release 2.2	この機能を使用すると、BGP を使用してルートおよびMPLS ラベルを転送する MPLS VPN CSC ネットワークを作成できます。 この機能は、12.0(21)ST で初めて導入されました。 この機能は、12.0(22)S で統合されました。 この機能は、12.0(23)S で統合されました。 この機能は、12.2(13)T で統合されました。 この機能は、12.0(24)S で統合されました。 この機能は、12.2(14)S で統合されました。 この機能は、12.0(27)S で統合されました。 この機能は、12.0(29)S で統合されました。 この機能は、Cisco IOS XE Release 2.2 で、Cisco ASR 1000 シリーズ ルータに実装されました。 この機能で使用される新しいコマンドまたは変更されたコマンドはありません。

用語集

ASBR：Autonomous System Boundary Router（自律システム境界ルータ）。自律システムを別の自律システムに接続するルータ。

自律システム：共通管理で共通のルーティング方針が共有される、ネットワークの集合。

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。他の BGP システムとネットワーク到達可能性情報を交換する、ドメイン間ルーティング プロトコル（同じ自律システム内の場合も、複数の自律システム間の場合もあります）。

CE ルータ：カスタマー エッジ ルータ。カスタマー ネットワークに属し、プロバイダー エッジ（PE）ルータとのインターフェイスとなるルータ。CE ルータは、関連する MPLS VPN を認識しません。

CSC：Carrier Supporting Carrier。小規模サービス プロバイダー（カスタマー キャリア）が MPLS バックボーンを経由してそれぞれの IP ネットワークまたは MPLS ネットワークを相互接続できる階層型 VPN モデル。これにより、カスタマー キャリアは独自の MPLS バックボーンを構築および維持する必要がなくなります。

eBGP：external Border Gateway Protocol（外部 Border Gateway Protocol）。異なる自律システムにあるルータ間の BGP。異なる自律システムにある 2 つのルータが互いに 2 ホップ以上離れている場合、これら 2 つのルータ間の eBGP セッションはマルチホップ BGP であると見なされます。

エッジ ルータ：ネットワークのエッジにあるルータ。MPLS ネットワークの境界を定義します。パケットを送受信します。エッジ ラベル スイッチ ルータおよびラベル エッジ ルータとも呼ばれます。

iBGP：internal Border Gateway Protocol（内部ボーダー ゲートウェイ プロトコル）。同じ自律システム内にあるルータ間の BGP。

IGP：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。単一の自律システム内でのルーティング情報の交換に使用されるインターネット プロトコル。インターネット IGP プロトコルの例として、IGRP、OSPF、IS-IS、RIP があります。

IP：Internet Protocol（インターネット プロトコル）。TCP/IP スタックにおいてコネクションレス型のネットワーク間サービスを提供するネットワーク層プロトコル。IP では、アドレッシング、タイプ オブ サービス指定、フラグメンテーションと再編成、セキュリティなどの機能が提供されます。RFC 791 に定義されています。

LDP：Label Distribution Protocol。パケットの転送に使用されるラベル（アドレス）をネゴシエーションするための、MPLS 対応ルータ間の標準プロトコル。

LFIB：Label Forwarding Information Base（ラベル転送情報ベース）。着信ラベルと発信ラベル、および関連する Forward Equivalence Class（FEC）パケットについての情報を保持するために MPLS で使用されるデータ構造。

MP-BGP：Multiprotocol BGP。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベル スイッチングを担当する IETF ワーキング グループの名前、およびそのワーキング グループで標準化されたラベル スイッチング アプローチの名前。

NLRI：Network Layer Reachability Information（ネットワーク層到達可能性情報）。BGP では、ルートおよびそのルートへのアクセス方法を記述した NLRI を含むルーティング アップデート メッセージが送信されます。この場合、NLRI がプレフィックスとなります。BGP アップデート メッセージでは、1 つ以上の NLRI プレフィックス、および NLRI プレフィックスのルートの属性が伝送されます。ルート属性には、BGP ネクスト ホップ ゲートウェイ アドレスおよび拡張コミュニティ値が含まれています。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）によって、ルータは、ルート プロセッサが他のルート プロセッサにテイクオーバーまたはスイッチオーバーされたあとでも継続して IP パケットを転送できます。NSF では、レイヤ 3 のルーティングおよび転送情報をバックアップルートプロセッサに保持および更新することによって、スイッチオーバーやルート収束のプロセス中にも継続して IP パケットおよびルーティングプロトコル情報が転送されることが保証されます。

PE ルータ：プロバイダー エッジ ルータ。サービス プロバイダーのネットワークの一部であるルータ。このルータは、カスタマー エッジ（CE）ルータに接続されます。すべての MPLS VPN 処理は PE ルータで実行されます。

QoS：Quality of Service。転送システムのパフォーマンスを測定したものであり、転送品質およびサービス アベイラビリティを示します。

RD：Route Distinguisher（ルート識別子）。IPv4 プレフィックスに連結される 8 バイトの値で、一意の VPN IPv4 プレフィックスを形成します。

RT：Route Target（ルート ターゲット）。プレフィックスのインポート先となる VRF ルーティング テーブルの識別に使用する拡張コミュニティ属性。

SLA：VPN 加入者に保証されるサービス レベル契約。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。1 つ以上の物理ネットワークのリソースを共有する、セキュアな MPLS ベースのネットワーク（一般的に1 つまたは複数のサービスプロバイダーによって実行されます）。VPNには地理的に分散したサイトが含まれており、共有バックボーン ネットワーク上で安全に通信できるようになっています。

VRF：VPN ルーティングおよび転送（VRF）インスタンス。PE ルータに付加される VPN サイトを定義するルーティング情報。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。

第 7 章

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポート

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポート機能により、MPLS VPN 相互自律（Inter-AS）ネットワークと MPLS VPN Carrier Supporting Carrier（CSC）ネットワークが、複数リンクで接続されている隣接ラベル スイッチ ルータ（LSR）間のトラフィックをロード シェアリングできます。LSR は、自律システム境界ルータ（ASBR）のペアまたは CSC プロバイダー エッジ（CSC-PE）デバイスと CSC カスタマー エッジ（CE）デバイスにすることができます。直接接続ループバック ピアリングを使用すると、内部ゲートウェイ プロトコル（IGP）レベルでロード シェアリングを実行できるため、LSR 間で必要な Border Gateway Protocol（BGP）セッションは 1 つのみです。BGP 以外の隣接 LSR の間に他のラベル配布メカニズムは不要です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートの前提条件

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）ネットワーク（MPLS VPN 相互自律システム（Inter-AS）、Carrier Supporting Carrier（CSC）を含む）が設定され、正しく動作していることを確認します。

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートの制約事項

直接接続ループバック ピアリングを使用したロード シェアリングは、Label Distribution Protocol（LDP）と内部ゲートウェイ プロトコル（IGP）を使用してルートとマルチプロトコル ラベル スイッチング（MPLS）ラベルを配布する Carrier Supporting Carrier（CSC）ネットワークには適用されません。

プロバイダー エッジ（PE）デバイスまたは自律システム境界ルータ（ASBR）デバイスの間に複数のリンクがある場合、このソフトウェアでは相互自律システム（Inter-AS）およびCSC でのロード バランシングはサポートされません。

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。これらのコマンドバリエーションは、タグ転送情報ベース（TFIB）をサポートする Cisco ソフトウェア リリースではサポートされていません。プレフィックスが通過する再帰ルートがいったん失われて再び現れる場合、TFIB はプレフィックスを解決できません。ただし、MPLS Forwarding Infrastructure（MFI）をサポートする Cisco ソフトウェア リリースでは、これらのコマンドバリエーションがサポートされています。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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1next-hop1*
- **ip route***destination-prefixmaskinterface2next-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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop-address*

MPLS VPN 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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop-address*

MPLS VPN 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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop1*
- **ip route***destination-prefixmasknext-hop2*

スタティック ルートを指定するときは、*interface* 引数および *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

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 Virtual Routing and Forwarding（VRF）インスタンスに関連付けられている場合は、次の **ip route vrf** コマンドがサポートされます。

- **ip route vrf***vrf-namedestination-prefixmasknext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmaskinterface1next-hop1*
- **ip route vrf***vrf-namedestination-prefixmaskinterface2next-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は、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-namedestination-prefixmasknext-hop-address***global**
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1next-hop1*
- **ip route***destination-prefixmaskinterface2next-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmasknext-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は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmasknext-hop1***global**
- **ip route vrf***destination-prefixmasknext-hop2***global**

MPLS VPN 環境でスタティック ルートを設定し、ネクストホップおよびインターフェイスが同じ VRF にある場合は、次の **ip route vrf** コマンドがサポートされません。

- **ip route vrf***vrf-namedestination-prefixmasknext-hop1*
- **ip route vrf***vrf-namedestination-prefixmasknext-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は、次の **ip route vrf** コマンドがサポートされます。たとえば、外部 Border Gateway Protocol（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-namedestination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1nexthop1*
- **ip route***destination-prefixmaskinterface2nexthop2*

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートに関する情報

直接接続ループバック ピアリングを使用したロード シェアリング

複数のリンクにより接続する隣接ラベル スイッチド ルータ（LSR）間のトラフィックをロード シェアリングするには、Inter-AS および CSC VPN の MPLS VPN ロード バランシング サポート機能を使用します。LSR は、自律システム境界ルータ（ASBR）のペアまたは Carrier Supporting Carrier プロバイダー エッジ（CSC-PE）と CSC カスタマー エッジ（CE）にすることができます。

直接接続ループバック ピアリングを使用すると、内部ゲートウェイ プロトコル（IGP）レベルでロード シェアリングを実行できるため、LSR 間で必要な Border Gateway Protocol（BGP）セッションは 1 つのみです。BGP 以外の隣接 LSR の間に他のラベル配布メカニズムは不要です。

直接接続ループバック ピアリングを使用すると、次のようにトラフィックをロードシェアリングできます。

- BGP セッションの確立時には LSR のループバック アドレスが使用されます。
- 接続リンク上でマルチプロトコル ラベル スイッチング（MPLS）が有効になります。
- 隣接 LSR のループバック アドレスへのスタティック ルーが複数あることで、IGP ロード シェアリングが可能になります。
- 隣接 LSR のループバック アドレスへの出ラベルは、暗黙的ヌル ラベルであり、LSR から推測されます。
- 隣接 LSR のループバック アドレスで IGP ロード シェアリングがイネーブルになるため、BGP セッションで学習される（さらにループバックに再帰する）プレフィックス宛てのトラフィックがロード シェアリングされます。

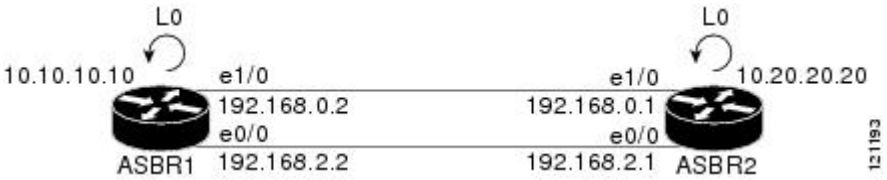
Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートの設定方法

VPN-IPv4 アドレスを交換する ASBR を使用した MPLS VPN Inter-AS の直接接続ループバック ピアリングの設定

ここでは、直接接続された自律システム境界ルータ（ASBR）のループバック インターフェイスのピアリングを設定する方法について説明します。

次の図は、直接接続された ASBR1 と ASBR2 のループバック設定を示します。この設定は、次に説明する作業で例として使用します。

図 *24*：直接接続 ***ASBR1*** および ***ASBR2*** のループバック インターフェイス設定



直接接続 ASBR のループバック インターフェイス アドレスの設定

直接接続自律システム境界ルータ（ASBR）のループバック インターフェイス アドレスを設定するには、この作業を実行します。

（注） 直接接続 ASBR ごとにループバック アドレスを設定する必要があります。つまり、上記の図の例では、ASBR1 と ASBR2 のそれぞれにループバック アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback***interface-number*
4. **ip address***ip-addressmask* [**secondary**]
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 モードをイネーブルにします。 • 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。

	コマンドまたはアクション	目的
ステップ 3	**interface loopback***interface-number* 例： `Device(config)# interface loopback 0`	常に稼働するインターフェイスをエミュレートするソフトウェア専用仮想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。 • **interface-number** 引数は、作成または設定するループバック インターフェイスの数です。作成可能なループバック インターフェイスの数に制限はありません。
ステップ 4	**ip address***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 10.10.10.10 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

eBGP ネイバー ループバックへの /32 スタティック ルートの設定

外部 Border Gateway Protocol（eBGP）ネイバー ループバックへの /32 スタティック ルートを設定するには、次の作業を実行します。

（注） 直接接続 ASBR ごとに /32 スタティック ルートを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route***prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*]
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**ip route***prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*] 例： `Device(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1`	スタティック ルートを確立します。 • *prefix* 引数は、宛先の IP ルート プレフィックスです。 • *mask* 引数は、宛先のプレフィックス マスクです。 • *ip-address* 引数は、指定されたネットワークに到達するのに使用できるネクスト ホップの IP アドレスです。 • *interface-type* 引数および *interface-number* 引数は、ネットワーク インターフェイス タイプおよびインターフェイス番号です。 • *distance* 引数はアドミニストレーティブ ディスタンスです。 • *name* 引数は、指定したルートに名前を適用します。 • **permanent** キーワードは、インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag***tag* キーワードおよび引数には、ルート マップを使用した再配布を制御するための「照合」値として使用できるタグ値を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

接続ループバック インターフェイスでの転送の設定

接続ループバック インターフェイスに転送を設定するには、この作業を実行します。

この作業を実行するには、ループバック間にセッションを確立する必要があります。「eBGP ネイバー ループバックへの /32 スタティック ルートの設定」の項では、Ethernet 1/0 と Ethernet 0/0 は接続インターフェイスです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***typeslot/port*
4. **mpls bgp forwarding**
5. **exit**
6. もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。
7. **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 モードをイネーブルにします。 • 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***typeslot/port* 例： `Device(config)# interface ethernet 1/0`	インターフェイス タイプを設定し、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。 • *type* 引数は、設定するインターフェイスのタイプです。 • *slot* 引数はスロット番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。 • */port* 引数はポート番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。

	コマンドまたはアクション	目的
ステップ 4	**mpls bgp forwarding** 例： `Device(config-if)# mpls bgp forwarding`	接続インターフェイスでマルチプロトコル ラベル スイッチング（MPLS）転送を有効にするように Border Gateway Protocol（BGP）を設定します。
ステップ 5	**exit** 例： `Device(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。
ステップ 6	もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ループバック間の eBGP セッションの設定

ループバック間の外部 Border Gateway Protocol（eBGP）セッションを設定するには、次の作業を実行します。

（注） 各直接接続自律システム境界ルータ（ASBR）のループバック間の eBGP セッションを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **no bgp default route-target filter**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
8. **address-family vpnv4** [**unicast**]
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standardextended**]
11. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 200`	BGP ルーティング プロセスを設定します。 • *as-number* は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。
ステップ 4	**no bgp default route-target filter** 例： `Device(config)# no bgp default route-target filter`	BGP の route-target フィルタリングを無効にし、ルータ コンフィギュレーション モードを開始します。 • 受信したすべての BGP VPN-IPv4 ルートがデバイスによって受け入れられます。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.20.20.20 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *as-number* 引数は、ネイバーが属する自律システムです。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check** 例： `Device(config-router)# neighbor 10.20.20.20 disable-connected-check`	ループバック間のピアリングを許可します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.20.20.20 update-source Loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • *ip-address* 引数は、BGP スピーキング ネイバーの IPv4 アドレスです。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *interface-type* 引数はインターフェイス タイプです。 • *interface-number* 引数は、インターフェイス番号です。
ステップ 8	**address-family vpnv4** [**unicast**] 例： `Device(config-router)# address-family vpnv4`	BGP、Routing Information Protocol（RIP）、スタティックなルーティングなどのルーティング プロトコルを設定するためにアドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードによって、ユニキャスト プレフィックスが指定されます。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**	BGP ネイバーとの情報交換をイネーブルにします。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。

	コマンドまたはアクション	目的
	例： `Device(config-router-af)# neighbor 10.20.20.20 activate`	• *peer-group-name* 引数は、BGP ピア グループの名前です。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 （注） この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standardextended**] 例： `Device(config-router-af)# neighbor 10.20.20.20 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • **both** キーワードは、標準コミュニティと拡張コミュニティの両方が送信されることを指定します。 • **standard** キーワードは、標準コミュニティのみを送信することを指定します。 • **extended** キーワードは、拡張コミュニティのみを送信することを指定します。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ループバック間でロード シェアリングが発生することの確認

ループバック間でロード シェアリングが発生することを確認するには、次の作業を実行します。ネイバールートのマルチプロトコル ラベル スイッチング（MPLS）ラベル転送情報ベース（LFIB）エントリが、使用可能なパスとインターフェイスをリストしていることを確認する必要があります。

手順の概要

1. **enable**
2. **show mpls forwarding-table** {*mask* | *length*} | **labels***label* [*networklabel*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**]
3. **disable**

手順の詳細

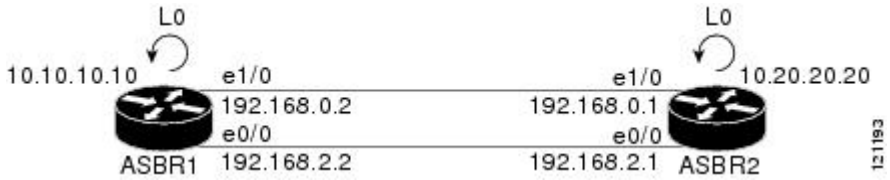
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	（任意）特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show mpls forwarding-table** {*mask* | *length*} | **labels***label* [*networklabel*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**] 例： `Device# show mpls forwarding-table`	MPLS LFIB の内容を表示します。 • 必要に応じて任意のキーワードまたは引数を入力します。
ステップ 3	**disable** 例： `Device# disable`	ユーザ EXEC モードに戻ります。

IPv4 のルートおよびアドレスを交換する ASBR を使用した MPLS VPN Inter-AS の直接接続ループバック ピアリングの設定

ここでは、相互自律システムネットワークでロードシェアリングを実現するために、直接接続している自律システム境界ルータ（ASBR）のループバック インターフェイスのピアリングを設定する方法について説明します。

次の図は、直接接続された ASBR1 と ASBR2 のループバック設定を示します。この設定は、次に説明する作業で例として使用します。

図 *25*：直接接続 ***ASBR1*** および ***ASBR2*** のループバック インターフェイス設定



直接接続 ASBR のループバック インターフェイス アドレスの設定

（注） 直接接続自律システム境界ルータ（ASBR）ごとにループバック アドレスを設定する必要があります。つまり、上記の図の例では、ASBR1 と ASBR2 のそれぞれにループバック アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback***interfacenumber*
4. **ip address***ip-address* [*mask* [**secondary**]]
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 モードをイネーブルにします。 • 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 loopback***interfacenumber* 例： `Device(config)# interface loopback 0`	常に稼働するインターフェイスをエミュレートするソフトウェア専用仮想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。 • *interface-number* 引数は、作成または設定するループバック インターフェイスの数です。作成可能なループバック インターフェイスの数に制限はありません。
ステップ 4	**ip address***ip-address* [*mask* [**secondary**]] 例： `Device(config-if)# ip address 10.10.10.10 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。

	コマンドまたはアクション	目的
		• **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

eBGP ネイバー ループバックへの /32 スタティック ルートの設定

外部 Border Gateway Protocol（eBGP）ネイバー ループバックへの /32 スタティック ルートを設定するには、次の作業を実行します。

（注） 直接接続自律システム境界ルータ（ASBR）ごとに /32 スタティック ルートを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route***prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*]
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**ip route***prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*] 例： `Device(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1`	スタティック ルートを確立します。 • *prefix* 引数は、宛先の IP ルート プレフィックスです。 • *mask* 引数は、宛先のプレフィックス マスクです。 • *ip-address* 引数は、指定されたネットワークに到達するのに使用できるネクスト ホップの IP アドレスです。 • *interface-type* 引数および *interface-number* 引数は、ネットワーク インターフェイス タイプおよびインターフェイス番号です。 • *distance* 引数はアドミニストレーティブ ディスタンスです。 • *name* 引数は、指定したルートに名前を適用します。 • **permanent** キーワードは、インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag***tag* キーワードおよび引数には、ルート マップを使用した再配布を制御するための「照合」値として使用できるタグ値を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

接続ループバック インターフェイスでの転送の設定

この作業を実行するには、ループバック間にセッションを確立する必要があります。「eBGP ネイバー ループバックへの /32 スタティック ルートの設定」タスクでは、Ethernet1/0 と Ethernet0/0 は接続インターフェイスです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***typeslot/port*
4. **mpls bgp forwarding**
5. **exit**
6. もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。
7. **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 モードをイネーブルにします。 • 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***typeslot/port* 例： `Device(config)# interface ethernet 1/0`	インターフェイス タイプを設定し、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。 • *type* 引数は、設定するインターフェイスのタイプです。 • *slot* 引数はスロット番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。 • */port* 引数はポート番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。
ステップ 4	**mpls bgp forwarding** 例： `Device(config-if)# mpls bgp forwarding`	接続インターフェイスに MPLS 転送をイネーブルにするように BGP 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	**exit** 例： `Device(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。
ステップ 6	もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ループバック間の eBGP セッションの設定

（注） 各直接接続自律システム境界ルータ（ASBR）のループバック間の外部 Border Gateway Protocol（eBGP）セッションを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
9. **address-family ipv4** [**unicast**] **vrf***vrf-name*
10. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
11. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**
12. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 200`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.20.20.20 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *as-number* 引数は、ネイバーが属する自律システムの番号です。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check** 例： `Device(config-router)# neighbor 10.20.20.20 disable-connected-check`	ループバック間のピアリングを許可します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `Device(config-router)# neighbor bb.bb.bb.bb ebgp-multihop 255`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *ttl* 引数には、1 ～ 255 ホップの範囲の存続可能時間を指定します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.20.20.20 update-source Loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • *ip-address* 引数は、BGP スピーキング ネイバーの IPv4 アドレスです。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 （注） この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *interface-type* 引数はインターフェイス タイプです。 • *interface-number* 引数は、インターフェイス番号です。
ステップ 9	**address-family ipv4** [**unicast**] **vrf***vrf-name* 例： `Device(config-router)# address-family ipv4`	BGP、Routing Information Protocol（RIP）、スタティックなルーティングなどのルーティング プロトコルを設定するためにアドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードによって、ユニキャストプレフィックスが指定されます。 • **vrf***vrf-name* キーワードおよび引数では、サブモードコマンドに関連付ける VPN ルーティング/転送インスタンス（VRF）の名前を指定します。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**	BGP ネイバーとの情報交換をイネーブルにします。 • *ip-address* 引数は、ネイバーデバイスの IP アドレスです。

	コマンドまたはアクション	目的
	例： `Device(config-router-af)# neighbor 10.20.20.20 activate`	• *peer-group-name* 引数は、BGP ピア グループの名前です。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 （注） この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended** 例： `Device(config-router-af)# neighbor 10.20.20.20 send-community extended`	コミュニティ属性が BGP ネイバーに送信されるように指定します。 • *ip-address* 引数は、ネイバーデバイスの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • **both** キーワードは、標準コミュニティと拡張コミュニティの両方が送信されることを指定します。 • **standard** キーワードは、標準コミュニティのみを送信することを指定します。 • **extended** キーワードは、拡張コミュニティのみを送信することを指定します。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ループバック間でロード シェアリングが発生することの確認

ループバック間でロードシェアリングが発生することを確認するには、ネイバールートのマルチプロトコル ラベル スイッチング（MPLS）ラベル転送情報ベース（LFIB）エントリに、使用可能なパスとインターフェイスがリストされていることを確認します。

手順の概要

1. **enable**
2. **show mpls forwarding-table** [*network* {*mask* |*length*} |**labels***label* [*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**]
3. **disable**

手順の詳細

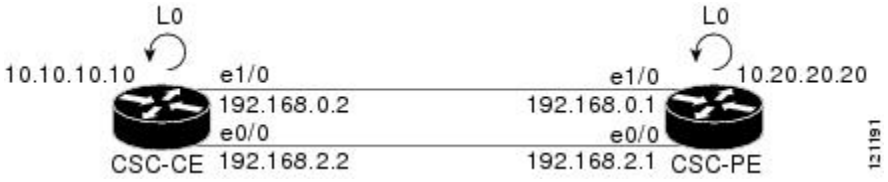
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels***label* [*label*] | **interface***interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]] [**vrf***vrf-name*] [**detail**] 例： `Device# show mpls forwarding-table`	MPLS LFIB の内容を表示します。 • 必要に応じてキーワードまたは引数を入力します。
ステップ 3	**disable** 例： `Device# disable`	ユーザ EXEC モードに戻ります。

MPLS VPN Carrier Supporting Carrier での直接接続ループバック ピアリングの設定

ここでは、直接接続 Carrier Supporting Carrier（CSC）プロバイダー エッジ（PE）デバイスと CSC カスタマー エッジ（CE）デバイスのループバック インターフェイスをピアリングして CSC トラフィックのロード バランシングを実行する方法について説明します。

次の図に、直接接続 CSC-PE デバイスおよび CSC-CE デバイスのループバック設定を示します。この設定は、次に説明する作業で例として使用します。

図 *26*：直接接続 *CSC-PE* デバイスおよび *CSC-CE* デバイスのループバック インターフェイス設定



CSC-PE デバイスでのループバック インターフェイス アドレスの設定

（注） Carrier Supporting Carrier（CSC）- プロバイダー エッジ（PE）デバイスでループバック インターフェイス アドレスを設定するには、Virtual Routing and Forwarding（VRF）インスタンスを有効にする必要があります。CSC- カスタマー エッジ（CE）デバイス ループバック インターフェイスでは、VRF を有効にする必要はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback***interfacenumber*
4. **ip vrf forwarding***vrf-name*
5. **ip address***ip-addressmask* [**secondary**]
6. **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 モードをイネーブルにします。 • 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 loopback***interfacenumber* 例： `Device(config)# interface loopback 0`	常に稼働するインターフェイスをエミュレートするソフトウェア専用仮想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。 • *interface-number* 引数は、作成または設定するループバック インターフェイスの数です。作成可能なループバック インターフェイスの数に制限はありません。

	コマンドまたはアクション	目的
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	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。
ステップ 5	**ip address***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 10.20.20.20 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-CE ルータでのループバック インターフェイス アドレスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface loopback***interface-number*
4. **ip address***ip-addressmask* [**secondary**]
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 モードをイネーブルにします。 • 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 loopback***interface-number* 例： `Device(config)# interface loopback 0`	常に動作しているインターフェイスをエミュレートするソフトウェア専用仮想インターフェイスを設定します。 • *interface-number* 引数は、作成または設定するループバック インターフェイスの数です。作成可能なループバック インターフェイスの数に制限はありません。
ステップ 4	**ip address***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 10.10.10.10 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

CSC-PE デバイスでの eBGP ネイバー ループバックへの /32 スタティック ルートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route vrf***vrf-nameprefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [**global**] [*distance*] [*name*] [**permanent**] [**tag***tag*]
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**ip route vrf***vrf-nameprefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [**global**] [*distance*] [*name*] [**permanent**] [**tag***tag*] 例： `Device(config)# ip route vrf vpn1 10.10.10.10 255.255.255.255 Ethernet 1/0 172.16.0.2`	Virtual Routing and Forwarding（VRF）インスタンスのスタティック ルートを確立します。 • *vrf-name* 引数は、スタティック ルートの VRF の名前です。 • *prefix* 引数は、宛先の IP ルート プレフィックスです。 • *mask* 引数は、宛先のプレフィックス マスクです。 • *ip-address* 引数は、宛先ネットワークに到達するのに使用できるネクスト ホップの IP アドレスです。 • *interface-type* 引数および *interface-number* 引数は、ネットワーク インターフェイス タイプおよびインターフェイス番号です。 • **global** キーワードは、指定されたネクスト ホップ アドレスが非 VRF ルーティング テーブルに登録されていることを指定します。 • *distance* 引数はアドミニストレーティブ ディスタンスです。 • *name* 引数は、指定したルートに名前を適用します。

	コマンドまたはアクション	目的
		• **permanent** キーワードは、インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag***tag* キーワードおよび引数には、ルート マップを使用した再配布を制御するための「照合」値として使用できるタグ値を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-CE デバイスでの eBGP ネイバー ループバックへの /32 スタティック ルートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip route***prefixmask* {*ip-address* | *interface-typeinterface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*]
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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**ip route***prefixmask* {*ip-address* | *interface-typeinterface-number*	スタティック ルートを確立します。 • *prefix* 引数は、宛先の IP ルート プレフィックスです。

	コマンドまたはアクション	目的
	[*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag***tag*] 例： `Device(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1`	• *mask* 引数は、宛先のプレフィックス マスクです。 • *ip-address* 引数は、宛先ネットワークに到達するのに使用できるネクスト ホップの IP アドレスです。 • *interface-type* 引数および *interface-number* 引数は、ネットワーク インターフェイス タイプおよびインターフェイス番号です。 • *distance* 引数はアドミニストレーティブ ディスタンスです。 • *name* 引数は、指定したルートに名前を適用します。 • **permanent** キーワードは、インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag***tag* キーワードおよび引数には、ルート マップを使用した再配布を制御するための「照合」値として使用できるタグ値を指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-CE ループバックに接続する CSC-PE インターフェイスでの転送の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***typeslot*/*port*
4. **ip vrf forwarding***vrf-name*
5. **ip address***ip-addressmask* [**secondary**]
6. **mpls bgp forwarding**
7. **exit**
8. もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 ～ 6 を繰り返します。
9. **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 モードをイネーブルにします。 • 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***typeslot/port* 例： `Device(config)# interface ethernet 1/0`	インターフェイスタイプを設定し、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。 • *type* 引数は、設定するインターフェイスのタイプです。 • *slot* 引数はスロット番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。 • */port* 引数はポート番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	インターフェイスまたはサブインターフェイスに Virtual Routing and Forwarding（VRF）インスタンスを関連付けます。 • *vrf-name* 引数は、VRF に割り当てる名前です。
ステップ 5	**ip address***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 172.16.0.1 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

	コマンドまたはアクション	目的
ステップ 6	**mpls bgp forwarding** 例： `Device(config-if)# mpls bgp forwarding`	接続インターフェイスでマルチプロトコル ラベル スイッチング（MPLS）転送を有効にするように Border Gateway Protocol（BGP）を設定します。
ステップ 7	**exit** 例： `Device(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。
ステップ 8	もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 ～ 6 を繰り返します。	
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-PE ループバックに接続する CSC-CE インターフェイスでの転送の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***typeslot*/*port*
4. **mpls bgp forwarding**
5. **exit**
6. もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。
7. **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 モードをイネーブルにします。 • 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***typeslot*/*port* 例： `Device(config)# interface ethernet 1/0`	インターフェイス タイプを設定し、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。 • *type* 引数は、設定するインターフェイスのタイプです。 • *slot* 引数はスロット番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。 • */port* 引数はポート番号です。スロット情報およびポート情報については、該当するハードウェア マニュアルを参照してください。
ステップ 4	**mpls bgp forwarding** 例： `Device(config-if)# mpls bgp forwarding`	接続インターフェイスでマルチプロトコル ラベル スイッチング（MPLS）転送を有効にするように Border Gateway Protocol（BGP）を設定します。
ステップ 5	**exit** 例： `Device(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。
ステップ 6	もう 1 つの接続インターフェイス（Ethernet 0/0）に対して、ステップ 3 および 4 を繰り返します。	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-PE デバイスと CSC-CE ループバック間での eBGP セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
8. **address-family ipv4** [**unicast**] **vrf***vrf-name*
9. **ip vrf forwarding***vrf-name*
10. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
11. **neighbor***ip-address***send-label**
12. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 200`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。

	コマンドまたはアクション	目的
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.10.10.10 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *as-number* 引数は、ネイバーが属する自律システムです。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check** 例： `Device(config-router)# neighbor 10.10.10.10 disable-connected-check`	ループバック間のピアリングを許可します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.10.10.10 update-source Loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • *ip-address* 引数は、BGP スピーキング ネイバーの IPv4 アドレスです。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *interface-type* 引数はインターフェイス タイプです。 • *interface-number* 引数は、インターフェイス番号です。
ステップ 8	**address-family ipv4** [**unicast**] **vrf***vrf-name* 例： `Device(config-router)# address-family ipv4 vrf vpn1`	BGP、Routing Information Protocol（RIP）、スタティックなルーティングなどのルーティング プロトコルを設定するためにアドレス ファミリ コンフィギュレーション モードを開始します。 • **ipv4** キーワードは、標準 IPv4 アドレス プレフィックスを伝送するセッションを設定します。

	コマンドまたはアクション	目的
		• **unicast** キーワードによって、ユニキャスト プレフィックスが指定されます。 • **vrf***vrf-name* キーワードおよび引数では、サブモード コマンドに関連付ける Virtual Routing and Forwarding（VPF）インスタンスの名前を指定します。
ステップ 9	**ip vrf forwarding***vrf-name* 例： `Device(config-router-af)# ip vrf forwarding vpn1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • *vrf-name* 引数は、VRF に割り当てる名前です。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 10.10.10.10 activate`	BGP ネイバーとの情報交換をイネーブルにします。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 （注） この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
ステップ 11	**neighbor***ip-address***send-label** 例： `Device(config-router-af)# neighbor 10.10.10.10 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定します。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

CSC-CE デバイスと CSC-PE ループバック間での eBGP セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
8. **address-family ipv4** [**unicast**] [**vrf***vrf-name*]
9. **neighbor** {*ip-address* | *peer-group-name*|*ipv6-address*] **activate**
10. **neighbor***ip-address***send-label**
11. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 200`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。
ステップ 4	**bgp log-neighbor-changes** 例： `Device(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.20.20.20 remote-as 100`	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *as-number* 引数は、ネイバーが属する自律システムです。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check** 例： `Device(config-router)# neighbor 10.20.20.20 disable-connected-check`	ループバック間のピアリングを許可します。 • *ip-address* 引数はネイバーの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.20.20.20 update-source Loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。 • *ip-address* 引数は、BGP スピーキング ネイバーの IPv4 アドレスです。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *interface-type* 引数はインターフェイス タイプです。 • *interface-number* 引数は、インターフェイス番号です。
ステップ 8	**address-family ipv4** [**unicast**] [**vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4`	BGP、RIP、スタティックなルーティングなどのルーティング プロトコルを設定するためにアドレス ファミリ コンフィギュレーション モードを開始します。 • **ipv4** キーワードは、標準 IPv4 アドレス プレフィックスを伝送するセッションを設定します。 • **unicast** キーワードによって、ユニキャスト プレフィックスが指定されます。 • **vrf***vrf-name* キーワードおよび引数では、サブモード コマンドに関連付ける Virtual Routing and Forwarding（VPF）インスタンスの名前を指定します。

	コマンドまたはアクション	目的
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*|*ipv6-address*] **activate** 例： `Device(config-router-af)# neighbor 10.20.20.20 activate`	BGP ネイバーとの情報交換をイネーブルにします。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。 • *peer-group-name* 引数は、BGP ピア グループの名前です。 • *ipv6-address* 引数は、BGP スピーキング ネイバーの IPv6 アドレスです。 （注） この引数は、RFC 2373 に記載されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
ステップ 10	**neighbor***ip-address***send-label** 例： `Device(config-router-af)# neighbor 10.20.20.20 send-label`	BGP ルートとともにマルチプロトコル ラベル スイッチング（MPLS）ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定します。 • *ip-address* 引数は、ネイバー デバイスの IP アドレスです。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ループバック間でロード シェアリングが発生することの確認

ループバック間でロードシェアリングが発生することを確認するには、ネイバールートのマルチプロトコル ラベル スイッチング（MPLS）ラベル転送情報ベース（LFIB）エントリが、使用可能なパスとインターフェイスをリストしていることを確認します。

手順の概要

1. **enable**
2. **show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [-*label*] | [**interface**] *interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
3. **disable**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show mpls forwarding-table** [**vrf***vrf-name*] [{*network* {*mask* | *length*} | **labels***label* [-*label*] | [**interface**] *interface* | **next-hop***address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**] 例： `Device# show mpls forwarding-table`	MPLS LFIB の内容を表示します。
ステップ 3	**disable** 例： `Device# disable`	ユーザ EXEC モードに戻ります。

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートの設定例

例：ASBR から別の ASBR のループバック アドレスへの 32 スタティック ルートの設定

次の例では、ASBR1 から ASBR2 のループバック アドレスに至る /32 スタティック ルートを設定します。

```
Device# configure terminal
Device(config)# ip route 10.20.20.20 255.255.255 e1/0 168.192.0.1
Device(config)# ip route 10.20.20.20 255.255.255 e0/0 168.192.2.1
```

次の例では、ASBR2 から ASBR1 のループバック アドレスに至る /32 スタティック ルートを設定します。

```
Device# configure terminal
Device(config)# ip route vrf vpn1 10.10.10.10 255.255.255 e1/0 168.192.0.2
Device(config)# ip route vrf vpn1 10.10.10.10 255.255.255 e0/0 168.192.2.2
```

例：ASBR を接続するインターフェイスでの BGP MPLS 転送の設定

次の例では、ASBR2 と ASBR1 を接続するインターフェイスで Border Gateway Protocol（BGP）およびマルチプロトコル ラベル スイッチング（MPLS）転送を設定します。

```
Device# configure terminal
Device(config)# interface ethernet 1/0
Device(config-if)# ip vrf forwarding vpn1
Device(config-if)# ip address 168.192.0.1 255.255.255.255
Device(config-if)# mpls bgp forwarding
Device(config-if)# exit
Device(config)# interface ethernet 0/0
Device(config-if)# ip vrf forwarding vpn1
Device(config-if)# ip address 168.192.2.1 255.255.255.255
Device(config-if)# mpls bgp forwarding
Device(config-if)# exit
```

例：ASBR での VPNv4 セッションの設定

次の例では、ASBR2 で VPNv4 セッションを設定します。

```
Device# configure terminal
Device(config)# router bgp 200
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# neighbor 10.10.10.10 remote-as 100
Device(config-router)# neighbor 10.10.10.10 disable-connected-check
Device(config-router)# neighbor bb.bb.bb.bb ebgp-multihop 255
Device(config-router)# neighbor 10.10.10.10 update-source Loopback0
!
Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor 10.10.10.10 activate
Device(config-router-af)# neighbor 10.10.10.10 send-community extended
Device(config-router-af)# end
```

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
BGP を使用する MPLS VPN CSC の設定	『*MPLS: Layer 3 VPNs: Inter-AS and CSC Configuration Guide*』の「MPLS VPN Carrier Supporting Carrier with BGP」モジュール

関連項目	マニュアル タイトル
BGP の設定	『*IP Routing: BGP Configuration Guide*』の「Configuring BGP」モジュール
MPLS VPN での eBGP と iBGP の両方に対する BGP マルチパス ロード シェアリングの設定	『*IP Routing: BGP Configuration Guide*』の「BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN」モジュール

RFC

RFC	タイトル
RFC 1164	『Application of the Border Gateway Protocol in the Internet』
RFC 1171	『A Border Gateway Protocol 4』
RFC 1700	『Assigned Numbers』
RFC 1966	『BGP Route Reflection: An Alternative to Full Mesh IBGP』
RFC 2283	『Multiprotocol Extensions for BGP-4』
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2547	『BGP/MPLS VPNs』
RFC 2842	『Capabilities Advertisement with BGP-4』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3107	『Carrying Label Information in BGP-4』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11* : *Inter-AS* および *CSN VPN* の *MPLS VPN* ロード バランシング サポートの機能情報

機能名	リリース	機能情報
Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポート	12.0(29)S 12.4(20)T 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.2	Inter-AS および CSN VPN の MPLS VPN ロード バランシング サポート機能により、MPLS VPN Inter-AS ネットワークと MPLS VPN CSC ネットワークが、複数リンクで接続されている隣接 LSR 間でトラフィックをロード シェアリングできます。LSR は、ASBR のペアまたは CSC-PE と CSC-CE にすることができます。直接接続ループバック ピアリングを使用すると、IGP レベルでロードシェアリングを実行できるため、LSR 間に複数の BGP セッションは不要です。BGP 以外の隣接 LSR の間に他のラベル配布メカニズムは不要です。 この機能は、Cisco IOS Release 12.0(29)S で導入されました。 この機能は、Cisco IOS Release 12.4(20)T、12.2(33)SRA、および 12.2(33)SXH で統合されました。 この機能は、Cisco IOS XE Release 2.2 で、Cisco ASR 1000 シリーズ ルータに実装されました。 追加または変更されたコマンドはありません。

第 8 章

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポート

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポート機能では、IPv4 ラベルを使用して外部 Border Gateway Protocol（eBGP）マルチパスを設定できます。これにより、マルチプロトコル ラベル スイッチング（MPLS）転送テーブルに、ルーティング テーブルにインストールされている各発信パスのラベル情報のエントリが作成され、冗長接続とロード バランシングが可能になります。この機能を使用しない場合は、ルーティングテーブルにそのプレフィックスのパスが複数ある場合でも、MPLS 転送テーブルには BGP ベスト パスのラベルのみが含まれます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの前提条件

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）ネットワーク（MPLS VPN 相互自律システム（Inter-AS）、Carrier Supporting Carrier（CSC）を含む）が設定され、正しく動作していることを確認します。

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの制約事項

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポート機能は、VPNv4 ルートを交換する自律システム境界ルータ（ASBR）が接続されたマルチプロトコル 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）相互自律システム（Inter-AS）ではサポートされていません。

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。これらのコマンドバリエーションは、タグ転送情報ベース（TFIB）をサポートする Cisco ソフトウェア リリースではサポートされていません。プレフィックスが通過する再帰ルートがいったん失われて再び現れる場合、TFIB はプレフィックスを解決できません。ただし、MPLS Forwarding Infrastructure（MFI）をサポートする Cisco ソフトウェア リリースでは、これらのコマンドバリエーションがサポートされています。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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1next-hop1*
- **ip route***destination-prefixmaskinterface2next-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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop-address*

MPLS VPN 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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop-address*

MPLS VPN 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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-hop1*
- **ip route***destination-prefixmasknext-hop2*

スタティック ルートを指定するときは、*interface* 引数および *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

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 Virtual Routing and Forwarding（VRF）インスタンスに関連付けられている場合は、次の **ip route vrf** コマンドがサポートされます。

- **ip route vrf***vrf-namedestination-prefixmasknext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmaskinterface1next-hop1*
- **ip route vrf***vrf-namedestination-prefixmaskinterface2next-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は、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-namedestination-prefixmasknext-hop-address***global**
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1next-hop1*
- **ip route***destination-prefixmaskinterface2next-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmasknext-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は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmasknext-hop1***global**
- **ip route vrf***destination-prefixmasknext-hop2***global**

MPLS VPN 環境でスタティック ルートを設定し、ネクスト ホップおよびインターフェイスが同じ VRF にある場合は、次の **ip route vrf** コマンドがサポートされません。

- **ip route vrf***vrf-namedestination-prefixmasknext-hop1*
- **ip route vrf***vrf-namedestination-prefixmasknext-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は、次の **ip route vrf** コマンドがサポートされます。たとえば、外部 Border Gateway Protocol（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-namedestination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterface1nexthop1*
- **ip route***destination-prefixmaskinterface2nexthop2*

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートに関する情報

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの概要

デバイスは、特定のプレフィックスの 2 つの同一外部 Border Gateway Protocol（eBGP）パスをネイバー自律システムから学習すると、ルータ ID が小さいパスをベスト パスとして選択します。このベスト パスが IP ルーティング テーブルにインストールされます。eBGP マルチパスを有効にすると、ネイバー自律システムから eBGP パスが学習されたときに、1 つのベスト パスが選択されるのではなく、複数のパスが IP ルーティング テーブルにインストールされます。

パケット スイッチング中、複数のパス間ではスイッチング モードに応じてパケット単位または宛先単位のロード シェアリングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。デフォルトでは、BGP は IP ルーティング テーブルへのパスを 1 つのみインストールします。

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの設定方法

Inter-AS MPLS VPN での MPLS VPN eBGP マルチパス ロード シェアリングの設定

自律システム境界ルータ（ASBR）で IPv4 ルートと MPLS ラベルを交換するマルチプロトコル 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）相互自律システムの外部 Border Gateway Protocol（eBGP）マルチパスを設定するには、ASBR で次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
6. **maximum-paths***number-paths*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor***ip-address***send-label**
9. **exit-address-family**
10. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定し、デバイスでルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。指定できる範囲は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 200`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4`	標準 IPv4 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 6	**maximum-paths***number-paths* 例： `Device(config-router-af)# maximum-paths 2`	（任意）IP ルーティング プロトコルがサポートできる並列ルートの最大数を制御します。 • *number-paths* 引数には、IP ルーティング プロトコルがルーティング テーブルにインストールする並列ルートの最大数を指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	ネイバー デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 8	**neighbor***ip-address***send-label** 例： `Device(config-router-af)# neighbor 10.0.0.1 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定します。 • *ip-address* 引数には、ネイバー デバイスの IP アドレスを指定します。
ステップ 9	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ 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	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

CSC-PE デバイスでの Carrier Supporting Carrier による MPLS VPN eBGP マルチパス ロード シェアリングの設定

マルチプロトコル ラベル スイッチング（MPLS）ラベルを使用して BGP ルートを配布する Carrier Supporting Carrier - プロバイダーエッジ（CSC-PE）デバイスで外部 Border Gateway Protocol（eBGP）マルチパス ロード シェアリングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **maximum-paths***number-paths*
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor***ip-address***as-override**
9. **neighbor***ip-address***send-label**
10. **exit-address-family**
11. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システ

	コマンドまたはアクション	目的
		ムの番号を示します。指定できる範囲は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 5	**maximum-paths***number-paths* 例： `Device(config-router-af)# maximum-paths 2`	（任意）IP ルーティング プロトコルがサポートできる並列ルートの最大数を制御します。 • CSC-PE デバイスでは、アドレス ファミリ コンフィギュレーション モードでこのコマンドが有効になります。 • *number-paths* 引数には、IP ルーティング プロトコルがルーティング テーブルにインストールする並列ルートの最大数を指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router-af)# neighbor 10.0.0.1 remote-as 200`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	ネイバー BGP デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 8	**neighbor***ip-address***as-override** 例： `Device(config-router-af)# neighbor 10.0.0.1 as-override`	サイトの自律システム番号（ASN）をプロバイダーの ASN で上書きするように PE デバイスを設定します。 • *ip-address* 引数には、指定した ASN で上書きされるデバイスの IP アドレスを指定します。
ステップ 9	**neighbor***ip-address***send-label** 例： `Device(config-router-af)# neighbor 10.0.0.1 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定します。 • *ip-address* 引数には、ネイバー デバイスの IP アドレスを指定します。
ステップ 10	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 11	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

CSC-CE デバイスでの Carrier Supporting Carrier による MPLS VPN eBGP マルチパス ロード シェアリングの設定

Carrier Supporting Carrier - カスタマー エッジ（CSC-CE）デバイスでの外部 Border Gateway Protocol（eBGP）マルチパス ロード シェアリングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp***as-number*
4. **maximum-paths***number-paths*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
6. **redistribute***protocol*
7. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
9. **neighbor***ip-address***send-label**
10. **exit-address-family**
11. **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 モードをイネーブルにします。 • 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	**router bgp***as-number* 例： `Device(config)# router bgp 200`	BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 • *as-number* 引数は、デバイスを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。指定できる範囲は 0 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。
ステップ 4	**maximum-paths***number-paths* 例： `Device(config-router)# maximum-paths 2`	（任意）IP ルーティング プロトコルがサポートできる並列ルートの最大数を制御します。 • CSC-CE ルータでは、ルータ コンフィギュレーション モードでこのコマンドが発行されます。

	コマンドまたはアクション	目的
		• *number-paths* 引数には、IP ルーティング プロトコルがルーティング テーブルにインストールする並列ルートの最大数を指定します。
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4`	IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **multicast** キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。 • **unicast** キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。 • **vrf***vrf-name* キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VRF の名前を指定します。
ステップ 6	**redistribute***protocol* 例： `Device(config-router-af)# redistribute static`	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。 • *protocol* 引数では、ルートの再配布元となるソース プロトコルを指定します。次のいずれかのキーワードを指定できます：**bgp**、**connected**、**egp**、**igrp**、**isis**、**mobile**、**ospf**、**rip**、および **static** [**ip**]。 • **static** [**ip**] キーワードを使用すると、IP スタティック ルートが再配布されます。 （注） 任意の **ip** キーワードは、スタティック ルートを System-to-Intermediate System（IS-IS）に再配布するときに使用します。 • **connected** キーワードは、IP がインターフェイスでイネーブルな場合に自動的に確立されるルートを示します。 • Open Shortest Path First（OSPF）や Intermediate System-to-Intermediate System（IS-IS）などのルーティング プロトコルの場合、これらのルートは自律システムの外部として再配布されます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。

	コマンドまたはアクション	目的
	例： `Device(config-router-af)# neighbor 10.0.0.2 remote-as 100`	• *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *as-number* 引数には、ネイバーが属している自律システムを指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.2 activate`	ネイバー BGP デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**neighbor***ip-address***send-label** 例： `Device(config-router-af)# neighbor 10.0.0.2 send-label`	BGP ルートとともにマルチプロトコル ラベル スイッチング（MPLS）ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定します。 • *ip-address* 引数には、ネイバー デバイスの IP アドレスを指定します。
ステップ 10	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 11	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの設定例

例：MPLS VPN Inter-AS での MPLS VPN eBGP マルチパス ロード シェアリングの設定

次に、自律システム境界ルータ（ASBR）で IPv4 ルートと MPLS ラベルを交換するマルチプロトコル 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）相互自律システムの外部 Border Gateway Protocol（eBGP）マルチパスを設定する例を示します。

```
Device# configure terminal
Device(config)# router bgp 100
Device(config-router)# neighbor 10.0.0.1 remote-as 200
Device(config-router)# address-family ipv4
Device(config-router-af)# maximum-paths 2
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 send-label
Device(config-router-af)# exit-address-family
Device(config-router-af)# end
```

例：CSC-PE デバイスでの MPLS VPN Carrier Supporting Carrier による MPLS VPN eBGP マルチパス ロード シェアリングの設定

次に、マルチプロトコル ラベル スイッチング（MPLS）ラベルを使用して BGP ルートを配布する Carrier Supporting Carrier - プロバイダーエッジ（CSC-PE）デバイスでの外部 Border Gateway Protocol（eBGP）マルチパス ロード シェアリングを設定する例を示します。

```
Device# configure terminal
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 vrf vpn1
Device(config-router-af)# maximum-paths 2
Device(config-router-af)# neighbor 10.0.0.1 remote-as 200
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 as-override
Device(config-router-af)# neighbor 10.0.0.1 send-label
Device(config-router-af)# exit-address-family
Device(config-router)# end
```

例：CSC-CE デバイスでの MPLS VPN Carrier Supporting Carrier による MPLS VPN eBGP マルチパス ロード シェアリングの設定

次に、Carrier Supporting Carrier - カスタマー エッジ（CSC-CE）デバイスでの外部 Border Gateway Protocol（eBGP）マルチパス ロード シェアリングを設定する例を示します。

```
Device# configure terminal
Device(config)# router bgp 200
```

```
Device(config-router)# maximum-paths 2
Device(config-router)# address-family ipv4
Device(config-router-af)# redistribute static
Device(config-router-af)# neighbor 10.0.0.2 remote-as 100
Device(config-router-af)# neighbor 10.0.0.2 activate
Device(config-router-af)# neighbor 10.0.0.2 send-label
Device(config-router-af)# exit-address-family
Device(config-router)# end
```

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
BGP を使用する MPLS VPN CSC の設定	『*MPLS: Layer 3 VPNs: Inter-AS and CSC Configuration Guide*』の「MPLS VPN Carrier Supporting Carrier with BGP」モジュール
BGP の設定	『*IP Routing: BGP Configuration Guide*』の「Configuring BGP」モジュール
MPLS VPN での eBGP と iBGP の両方に対する BGP マルチパス ロード シェアリングの設定	『*IP Routing: BGP Configuration Guide*』の「BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN」モジュール

RFC

RFC	タイトル
RFC 1164	『Application of the Border Gateway Protocol in the Internet』
RFC 1171	『A Border Gateway Protocol 4』
RFC 1700	『Assigned Numbers』
RFC 1966	『BGP Route Reflection: An Alternative to Full Mesh IBGP』
RFC 2283	『Multiprotocol Extensions for BGP-4』

RFC	タイトル
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2547	『BGP/MPLS VPNs』
RFC 2842	『Capabilities Advertisement with BGP-4』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3107	『Carrying Label Information in BGP-4』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *12*：*CSC* および *Inter-AS MPLS VPN* の *MPLS VPN eBGP* マルチパス サポートの機能情報

機能名	リリース	機能情報
CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポート	12.0(27)S 12.2(30)S 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.2	CSC および Inter-AS MPLS VPN の MPLS VPN eBGP マルチパス サポート機能により、ネイバー自律システム（AS）から eBGP パスが学習されたときに、ベスト パスが 1 つ選択されるのではなく、複数のパスが IP ルーティングテーブルにインストールされます。 この機能は、Cisco IOS Release 12.0(27)S で導入されました。 この機能は、Cisco IOS Release 12.2(30)S、12.2(33)SRA、および 12.2(33)SXH で統合されました。 この機能は、Cisco IOS XE Release 2.2 で、Cisco ASR 1000 シリーズ ルータに実装されました。 追加または変更されたコマンドはありません。

第 9 章

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポート

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポート機能により、Border Gateway Protocol（BGP）ラベル セッションで Carrier Supporting Carrier（CSC）カスタマー エッジ（CE）デバイスの明示的ヌルをアドバタイズできます。

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの前提条件

- ご使用のネットワークでマルチプロトコル 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）を設定する必要があります。
- Carrier Supporting Carrier（CSC）カスタマー エッジ（CE）デバイス（CSC-CE）と CSC プロバイダー エッジ（PE）デバイス間でラベルを配布するため、Border Gateway Protocol（BGP）を設定する必要があります。

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの制約事項

- 明示的ヌル ラベルは、Carrier Supporting Carrier（CSC）カスタマー エッジ（CE）デバイス（CSC-CE）トポロジでのみ設定します。
- 明示的ヌル ラベルはネイバーのみに基づいて設定します。

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートに関する情報

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの機能設計

Border Gateway Protocol（BGP）IPv4 ラベル配布機能を備えた Carrier Supporting Carrier（CSC）カスタマーエッジ（CE）デバイス（CSC-CE）では、BGP が直接接続ルートの暗黙的ヌル ラベルをアドバタイズします。これにより、前のホップ（直前の）デバイスが PHP（Penultimate Hop Popping）を実行します。

MPLS VPN 明示的ヌル ラベル サポート BGP IPv4 ラベル セッション機能により、直前のデバイスが着信ラベルを明示的ヌル ラベルに交換（または追加）します。このアクションにより、出力デバイスは強制的に、明示的ヌル ラベルをポップし、残りのパケットを調べることでこの明示的ヌル ラベルを処理します。

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの利点

明示的ヌル ラベルは、パケットがその Carrier Supporting Carrier（CSC）カスタマー エッジ（CE）宛先に到達するまで、サービス レベル契約（SLA）間で Quality of Service（QoS）ビットを維持できるようにします。

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの設定方法

BGP を使用する CSC の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast**]
5. **neighbor** *ip-address* **send-label explicit-null**
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **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 モードをイネーブルにします。 • 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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 100`	ルータ コンフィギュレーション モードを開始して、Border Gateway Protocol（BGP）プロセスを実行するようにデバイスを設定します。
ステップ 4	**address-family ipv4** [**unicast**] 例： `Device(config-router)# address-family ipv4`	IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードを開始します。このモードでは、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定できます。
ステップ 5	**neighbor** *ip-address* **send-label explicit-null** 例： `Device(config-router-af)# neighbor 10.0.0.2 send-label explicit-null`	BGP ルートとともにマルチプロトコル ラベル スイッチング（MPLS）ラベルを送信するデバイスの機能をアドバタイズします。 • explicit-null キーワードを指定すると、Carrier Supporting Carrier（CSC）カスタマーエッジ（CE）デバイスが、値が 0 のラベルをネイバーに送信できます。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.99.70 activate`	ネイバーが IPv4 アドレス ファミリのプレフィックスをローカル デバイスと交換できるようにします。
ステップ 7	**end** 例： `Device(config-router-af)# end`	特権 EXEC モードに戻ります。

明示的ヌル設定の確認

手順の概要

1. イネーブル化
2. **show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*regexp*] | **received prefix-filter** | **received-routes** | **routes**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*regexp*] | **received prefix-filter** | **received-routes** | **routes**]] 例： `Device# show ip bgp neighbors`	ネイバーへの TCP および Border Gateway Protocol（BGP）接続に関する情報（明示的ヌルを含む）を表示します。 • 任意の *ip-address* 引数を指定すると、ルートを学習したネイバーの IP アドレスが表示されます。この引数を省略すると、すべてのネイバーが表示されます。 • 任意の **advertised-routes** キーワードを指定すると、デバイスがネイバーにアドバタイズしたルートがすべて表示されます。 • 任意の **dampened-routes** キーワードを指定すると、指定された IP アドレスのネイバーへのダンプ ルートが表示されます。 • 任意の **flap-statistics** キーワードを指定すると、指定されたネイバーから学習したルートのフラップ統計情報が表示されます（外部BGP（eBGP）ピアのみ）。 • 任意の **path** *regexp* キーワードおよび引数を指定すると、指定されたネイバーから学習した自律システム パスが表示されます。オプションの正規表現を使用して、出力をフィルタ処理できます。 • 任意の **received prefix-filter** キーワードを指定すると、指定された IP アドレスに対して設定されているプレフィックス リスト フィルタが表示されます。 • 任意の **received-routes** キーワードを指定すると、指定したネイバーから受信したすべてのルート（受け入れられたルートと拒否されたルートの両方）が表示されます。 • 任意の **routes** キーワードを指定すると、受信され、受け入れられたすべてのルートが表示されます。これは **received-routes** キーワードの出力のサブセットです。

次の作業

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの設定例

例：BGP を使用する CSC-CE の設定

次の例では、ラベルを配布し、またそのすべての接続ルートについて明示的ヌルをアドバタイズするため、Carrier Supporting Carrier（CSC）が Border Gateway Protocol（BGP）を使用して設定されています。

```
neighbor 10.0.0.0 send-label explicit-null
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.0.0.0 remote-as 200
 !
address-family ipv4
 neighbor 10.0.0.0 activate
 neighbor 10.0.0.0 send-label explicit-null
 no auto-summary
 no synchronization
 exit-address-family
```

例：明示的ヌル設定の確認

この例では、**show ip bgp neighbors** コマンドにより、接続 Border Gateway Protocol（BGP）ネイバーに関する情報（IP アドレス、バージョン番号、ネイバーの機能、メッセージ統計情報、および（明示的ヌルが設定されている場合に表示される）アドレス ファミリ統計情報など）が表示されます。

```
Device# show ip bgp neighbors

BGP neighbor is 10.0.0.2,  remote AS 300, external link
  BGP version 4, remote router ID 10.0.0.20
  BGP state = Established, up for 00:45:16
  Last read 00:00:16, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    ipv4 MPLS Label capability: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          2
    Keepalives:            47         47
    Route Refresh:          0          0
    Total:                 49         50
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 9, neighbor version 9/0
  Output queue sizes : 0 self, 0 replicated
  Index 1, Offset 0, Mask 0x2
```

```
Member of update-group 1
My AS number is allowed for 3 number of times
AF-dependant capabilities:
  Outbound Route Filter (ORF) type (128) Prefix-list:
Sending Prefix & Label(advertise explicit-null set)       !Explicit null is configured
                                Sent       Rcvd
Prefix activity:                ----       ----
  Prefixes Current:               3          3 (Consumes 144 bytes)
  Prefixes Total:                 3          6
  Implicit Withdraw:              0          3
  Explicit Withdraw:              0          0
  .........
  .........
```

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートのその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
BGP 設定作業	『*IP Routing: BGP Configuration Guide*』
BGP コマンド	『Cisco IOS IP Routing: BGP Command Reference』

RFC

RFC	タイトル
RFC 1163	『*A Border Gateway Protocol*』
RFC 1164	『*Application of the Border Gateway Protocol in the Internet*』
RFC 2283	『*Multiprotocol Extensions for BGP-4*』
RFC 2547	『*BGP/MPLS VPNs*』
RFC 3107	『*Carrying Label Information in BGP-4*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13* : ***BGP IPv4*** ラベル セッションによる ***MPLS VPN*** 明示的ヌル ラベル サポートの機能情報

機能名	リリース	機能情報
BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポート	12.0(27)S 12.0(27)S1 12.2(27)SBA 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.3	BGP IPv4 ラベル セッションによる MPLS VPN 明示的ヌル ラベル サポート機能により、Carrier Supporting Carrier（CSC）カスタマー エッジ（CE）デバイスの BGP ラベル セッションで明示的ヌルをアドバタイズできます。 この機能は、12.0(27)S で導入されました。 12.0(27)S1 では、Cisco 12000 シリーズ インターネット ルータのサポートが追加されました。 Cisco 10000 シリーズ ルータのサポートは、12.2(27)SBA で追加されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ ルータのサポートが追加されました。 次のコマンドが導入または変更されました：**debug ip bgp**、**neighbor send-label explicit-null**、**show ip bgp neighbors**、**show ip bgp vpnv4**、**show mpls forwarding-table**

用語集

BGP

ボーダー ゲートウェイ プロトコル。別々の自律システムに属するデバイス間でのルーティング情報交換に使用する外部ボーダー ゲートウェイ プロトコル。BGP は TCP を使用します。TCP は信頼性の高いプロトコルであるため、BGP ではデータ パケットのドロップまたはフラグメント化の問題が発生しません。

CE デバイス

カスタマーエッジデバイスVPNプロバイダーとVPNカスタマーの境界にあり、カスタマーに属するデバイス。

eBGP

外部ボーダー ゲートウェイ プロトコル。別々の自律システムに属するデバイス間で行われる BGP セッション。異なる自律システムに属するデバイス ペアが互いに複数 IP ホップ離れている場合、この 2 台のデバイス間で行われる外部 BGP セッションをマルチホップ外部 BGP と呼びます。

label

スイッチング ノードに対してデータの転送方法（パケットまたはセル）を指示する短い固定長のデータ ID。

ラベル配布

標準のルーティング方式が使用されていた場合に選択されたであろうパス以外のパス上のネットワーク経由でトラフィックを転送するために使用されるテクニックとプロセス。

LDP

Label Distribution Protocol。ラベルとネットワーク プレフィックスの間のバインディングを配布することによって、MPLS ホップバイホップ転送をサポートするプロトコル。このプロトコルのシスコ独自のバージョンは、タグ配布プロトコル（TDP）です。

LSP

Label Switched Path（ラベル スイッチド パス）。パケットの伝送に MPLS が使用される、2 台のデバイス間に設定された接続。1 つ以上のラベル スイッチド ホップを連結して作成されたパスです。これにより、MPLS ノードからのラベルを別の MPLS ノードにスワップして、パケットを転送できます。

MPLS

Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。レイヤ 3 スイッチングではなくレイヤ 2 スイッチング経由で主にパケットを送信する方式。MPLS では、Forwarding Equivalence Class という概念に基づいて、MPLS クラウドに入るときにパケットに短い固定長のラベルが割り当てられます。MPLS ドメイン内では、元のパケット ヘッダーにほとんど頼ることなく、ラベルに基づいて転送判断が行われます（これまではタグ スイッチングと呼ばれていました）。

NLRI

Network Layer Reachability Information（ネットワーク層到達可能性情報）。BGP は NLRI を含むルーティング アップデート メッセージを送信します。ルートは NLRI に記述されています。この場合、NLRI がプレフィックスとなります。BGP アップデート メッセージは、1 つまたは複数の NLRI プレフィックス、およびこの NLRI プレフィックスのルートの属性を伝送します。ルート属性には、BGP ネクストホップ ゲートウェイ アドレス、コミュニティ値、およびその他の情報が格納されています。

PE デバイス

プロバイダー エッジ デバイス。VPN プロバイダーと VPN カスタマーの境界にあり、プロバイダーに属するデバイス。

QoS

Quality of Service。転送システムのパフォーマンスの尺度の 1 つであり、転送品質とサービスのアベイラビリティを反映したものです。

ルータ

1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層デバイス。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

VPN

Virtual Private Network（バーチャル プライベート ネットワーク）。1 つまたは複数の物理ネットワーク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。VPN には、共有のバックボーンで安全に通信できる地理的に分散したサイトが含まれます。