Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ MPLS レイヤ 3 VPN コンフィギュレーション ガイド

Text Part Number: OL-24668-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

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

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

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

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

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

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ MPLS レイヤ 3 VPN コンフィギュレーション ガイド
© 2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2011–2012, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

はじめに VPC-vii

MPLS レイヤ 3 VPN の実装 VPC-9

内容 VPC-10

MPLS L3VPN の実装の前提条件 VPC-10

MPLS L3VPN の制限 VPC-11

MPLS レイヤ 3 VPN の概要 VPC-11

MPLS L3VPN の概要 VPC-11

MPLS L3VPN の利点 VPC-12

MPLS L3VPN の機能 VPC-13

仮想ルーティングおよび転送テーブル VPC-13

VPN ルーティング情報：配信 VPC-13

BGP による VPN ルーティング情報の配布 VPC-14

MPLS 転送 VPC-14

自動ルート識別子の割り当て VPC-15

MPLS L3VPN の主要コンポーネント VPC-15

L3VPN の Inter-AS サポート VPC-16

Inter-AS サポート：概要 VPC-16

Inter-AS および ASBR VPC-16

連合 VPC-17

MPLS VPN Inter-AS BGP ラベル配布 VPC-18

MPLS ラベル付き IPv4 ルートの交換 VPC-19

BGP ルーティング情報 VPC-20

BGP メッセージおよび MPLS ラベル VPC-20

MPLS ラベルとルートの送信 VPC-21

L3VPN の Carrier Supporting Carrier サポート VPC-21

CSC の前提条件 VPC-21

CSC の利点 VPC-22

バックボーン キャリアとカスタマー キャリアの設定オプション VPC-22

カスタマー キャリア：IP コアを持つ ISP VPC-23

カスタマー キャリア：MPLS サービス プロバイダー VPC-23

MPLS レイヤ 3 VPN の実装方法 VPC-24

コア ネットワークの設定 VPC-24
MPLS VPN カスタマーのニーズの評価 VPC-24
コアにおけるルーティング プロトコルの設定 VPC-25
コアにおける MPLS の設定 VPC-25
FIB がコア上でイネーブルになっているかどうかの確認 VPC-25
PE ルータおよびルート リフレクタでのマルチプロトコル BGP の設定 VPC-26
MPLS VPN カスタマーの接続 VPC-27
カスタマーの接続を可能にするための、PE ルータでの VRF の定義 VPC-28
各 VPN カスタマー用の PE ルータでの VRF インスタンスの設定 VPC-30
BGP を PE ルータと CE ルータ間のルーティング プロトコルに設定 VPC-32
RIPv2 を PE ルータと CE ルータ間のルーティング プロトコルに設定 VPC-36
PE ルータと CE ルータ間のスタティック ルートの設定 VPC-39
OSPF を PE ルータと CE ルータ間のルーティング プロトコルに設定 VPC-40
EIGRP を PE ルータと CE ルータ間のルーティング プロトコルに設定 VPC-43
MPLS VPN における EIGRP 再配布の設定 VPC-46
ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供 VPC-49
IPv4 ルートおよび MPLS ラベルを交換する ASBR の設定 VPC-49
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 VPC-52
ルート リフレクタが AS 内でリモート ルートを反映するように設定する VPC-55
ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供 VPC-58
VPN-IPv4 アドレスを交換するように ASBR を設定する VPC-58
ASBR ピアへのスタティック ルートの設定 VPC-61
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 VPC-63
ASBR 連合での MPLS 転送の設定 VPC-65
ASBR 連合ピアへのスタティック ルートの設定 VPC-67
Carrier Supporting Carrier の設定 VPC-68
Carrier Supporting Carrier トポロジの識別 VPC-68
バックボーン キャリア コアの設定 VPC-69
CSC-PE ルータと CSC-CE ルータの設定 VPC-69
ピアへのスタティック ルートの設定 VPC-76
MPLS レイヤ 3 VPN 設定の確認 VPC-77
MPLS レイヤ 3 VPN 実装の設定例 VPC-81
BGP を使用する MPLS VPN の設定：例 VPC-81
PE ルータでの Routing Information Protocol の設定：例 VPC-82

EIGRP を使用した PE ルータの設定：例 VPC-82
MPLS VPN CSC の設定例 VPC-83
バックボーン キャリア コアの設定：例 VPC-83
CSC-PE ルータと CSC-CE ルータ間のリンクの設定：例 VPC-83
ピアへのスタティック ルートの設定：例 VPC-84
その他の参考資料 VPC-85
関連資料 VPC-85
標準 VPC-85
MIB VPC-85
RFC VPC-86
シスコのテクニカル サポート VPC-86
IPv6 VPN プロバイダー エッジ転送 over MPLS VPC-87
内容 VPC-87
6PE/VPE 設定の前提条件 VPC-88
6PE/VPE に関する情報 VPC-88
6PE/VPE の概要 VPC-88
6PE/VPE の利点 VPC-89
IPv6 over MPLS バックボーンの導入 VPC-89
プロバイダー エッジ ルータおよびカスタマー エッジ ルータ上の IPv6 VPC-89
IPv6 プロバイダー エッジ マルチ パス VPC-90
OSPFv3 6VPE VPC-90
複数の VRF のサポート VPC-90
OSPFv3 PE-CE 拡張 VPC-91
VRF Lite VPC-91
6PE/VPE の実装方法 VPC-91
6PE/VPE の設定 VPC-91
PE から PE コアの設定 VPC-93
CE から PE コアの設定 VPC-97
OSPFv3 を PE ルータと CE ルータ間のルーティング プロトコルに設定 VPC-100
6PE の設定例 VPC-104
PE ルータでの 6PE の設定：例 VPC-104
PE ルータでの 6VPE の設定：例 VPC-104
PE から CE 間の OSPFv3 の設定：例 VPC-105
その他の参考資料 VPC-106
関連資料 VPC-106
標準 VPC-106
MIB VPC-106
RFC VPC-106

シスコのテクニカル サポート VPC-107

INDEX

はじめに

「はじめに」の内容は、次のとおりです。

- 「マニュアルの変更履歴」（P.VPC-vii）
- 「マニュアルの入手方法およびテクニカル サポート」（P.VPC-vii）

マニュアルの変更履歴

表 1 に、初版後、このマニュアルに加えられた技術的な変更の履歴を示します。

表 1　　マニュアルの変更履歴

リビジョン	日付	変更点
OL-24668-01-J	2011 年 4 月	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

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

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

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

MPLS レイヤ 3 VPN の実装

マルチプロトコル ラベル スイッチング（MPLS）レイヤ 3 バーチャル プライベート ネットワーク（VPN）は、MPLS プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1 つ以上のカスタマー エッジ（CE）ルータが、1 つ以上のプロバイダー エッジ（PE）ルータに接続されます。

このモジュールでは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの MPLS レイヤ 3 VPN の概念および設定情報を提供します。

（注） MPLS レイヤ 3 VPN 機能を使用するには、評価ライセンスまたは永久ライセンスを取得する必要があります。ただし、以前のソフトウェア バージョンからアップグレードする場合は、MPLS レイヤ 3 VPN 機能は 90 日間暗黙ライセンスを使用して動作し続けます（この期間中に永久ライセンスを購入できます）。ライセンスの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』の「*Software Entitlement on Cisco ASR 9000 Series Routers*」モジュールを参照してください。

（注） このモジュールに記載されているコマンドの詳細については、「*Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference*」を参照してください。この章で使用されている他のコマンドの説明については、コマンド リファレンスのマスター索引を参照するか、またはオンラインで検索してください。

MPLS レイヤ 3 VPN の実装の機能履歴：Cisco ASR 9000 シリーズ ルータ

リリース	変更箇所
リリース 3.7.2	この機能が導入されました。

内容

- 「MPLS L3VPN の実装の前提条件」（P.VPC-10）
- 「MPLS L3VPN の制限」（P.VPC-11）
- 「MPLS レイヤ 3 VPN の概要」（P.VPC-11）
- 「MPLS レイヤ 3 VPN の実装方法」（P.VPC-24）
- 「MPLS レイヤ 3 VPN 実装の設定例」（P.VPC-81）
- 「その他の参考資料」（P.VPC-85）

MPLS L3VPN の実装の前提条件

MPLS レイヤ 3 VPN を設定するには、次の前提条件を満たす必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。

  ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

VPN-IPV4 アドレスまたは IPv4 ルートおよび MPLS ラベルを交換する自律システム境界ルータ（ASBR）に MPLS VPN Inter-AS を設定するには、次の前提条件を満たす必要があります。

- MPLS VPN の自律システムまたはサブ自律システム間に外部ボーダー ゲートウェイ プロトコル（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が正しく設定されていることを確認します（手順については「MPLS レイヤ 3 VPN の実装方法」（P.VPC-24）、を参照してください）。
- 次の作業を実行する必要があります。
  - 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 PE-to-PE ルーティング セッションの設定
  - BGP の PE から CE へのルーティング セッションの設定
  - 直接接続された ASBR 間の VPN-IPv4 eBGP セッションの設定

MPLS レイヤ 3 VPN を設定するには、ルータは MPLS 転送および転送情報ベース（FIB）をサポートしている必要があります。

MPLS L3VPN の制限

次に、MPLS レイヤ 3 VPN の実装に関する制約事項を示します。

- MPLS VPN の自律システムまたはサブ自律システム間に eBGP ルーティングを設定する場合は、マルチホップ VPN-IPv4 eBGP はサポートされません。
- MPLS VPN は、IPv4 アドレス ファミリだけをサポートします。

IPv4 ルートおよび MPLS ラベルを交換する ASBR に MPLS VPN Inter-AS を設定する場合は、次の制約事項が適用されます。

- 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。
- Inter-AS は IPv4 ルートだけをサポートします。IPv6 はサポートされていません。

（注） BGP スピーカーに接続する物理インターフェイスは FIB および MPLS をサポートする必要があります。

次の制約事項がルーティング プロトコル OSPF および RIP に適用されます。

- OSPF および RIP では IPv6 はサポートされません。

MPLS レイヤ 3 VPN の概要

MPLS レイヤ 3 VPN を実装するには、次の概念を理解する必要があります。

- 「MPLS L3VPN の概要」（P.VPC-11）
- 「MPLS L3VPN の利点」（P.VPC-12）
- 「MPLS L3VPN の機能」（P.VPC-13）
- 「MPLS L3VPN の主要コンポーネント」（P.VPC-15）

MPLS L3VPN の概要

MPLS VPN を定義する前に、VPN の全般を定義する必要があります。VPN の説明を次に示します。

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

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

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

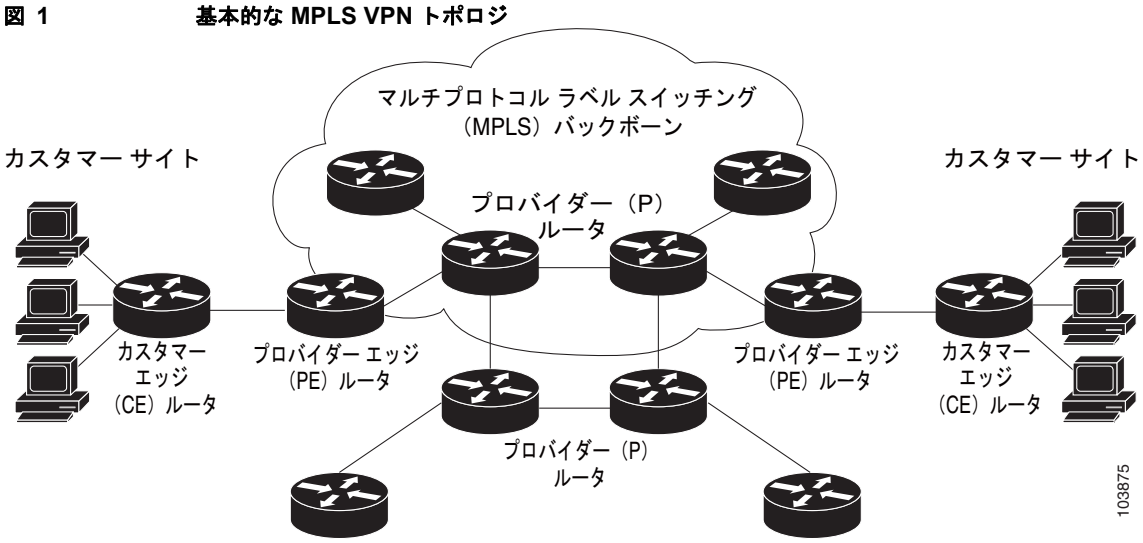
MPLS VPN の管理や拡張は、従来の VPN よりも簡単です。新しいサイトが MPLS VPN に追加された場合、更新する必要があるのは、カスタマー サイトにサービスを提供するサービス プロバイダーのエッジ ルータだけです。

MPLS VPN コンポーネントは次のとおりです。

- プロバイダー（P）ルータ：プロバイダー ネットワークのコア内のルータ。PE ルータは MPLS スイッチングを実行し、ルーティングされるパケットに VPN ラベルを付加しません。VPN ラベルは正しいプライベート ネットワークまたはカスタマー エッジ ルータにデータ パケットを送信するために使用されます。
- PE ルータ：着信パケットを受信するインターフェイスまたはサブインターフェイスに基づいて、着信パケットに VPN ラベルを付加するルータ。MPLS コア ラベルも付加します。PE ルータは、CE ルータに直接接続します。
- カスタマー（C）ルータ：インターネット サービス プロバイダー（ISP）または企業ネットワークのルータ。
- カスタマー エッジ（CE）ルータ：ネットワーク上の PE ルータに接続する、ISP のネットワーク上のエッジ ルータ。CE ルータは、PE ルータとインターフェイスする必要があります。

図 1 に、基本的な MPLS VP N トポロジを示します。

図 1　　基本的な MPLS VPN トポロジ



MPLS L3VPN の利点

MPLS L3VPN は次の利点があります。

- サービス プロバイダーは、スケーラブルな VPN を展開し、付加価値サービスを提供できます。
- コネクションレス型サービスでは、ホスト間の通信を確立するために上記のアクションは必要はないことを保証します。
- 集中型サービス：レイヤ 3 に VPN を構築すると、VPN に代表されるユーザ グループに目的のサービスを配布できます。
- スケーラビリティ：コネクション型ポイントツーポイント オーバーレイ、フレーム リレー、または ATM 仮想接続を使用して、スケーラブルな VPN を作成します。
- セキュリティ：セキュリティは、（カスタマーから受信したパケットを確実に正しい VPN に配置するように）プロバイダー ネットワークのエッジとバックボーンに提供されます。

- 統合 Quality of Service（QoS）サポート：QoS は、予測可能なパフォーマンスおよびポリシーの実装に対処し、MPLS VPN のさまざまなレベルのサービスをサポートする機能を提供します。
- 単純な移行：サービス プロバイダーは、単純な移行パスを使用して VPN サービスを導入できます。
- エンド カスタマーの移行が簡素化されます。CE ルータ上で MPLS をサポートする必要がなく、カスタマーのイントラネットに変更は必要ありません。

MPLS L3VPN の機能

MPLS VPN 機能は、MPLS ネットワークのエッジでイネーブルになっています。PE ルータは、次のタスクを実行します。

- CE ルータとルーティング アップデートを交換する
- VPN バージョン 4（VPNv4）ルートに CE ルーティング情報を変換する
- マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を介して、他の PE ルータと VPNv4 ルートを交換する

仮想ルーティングおよび転送テーブル

各 VPN は、1 つ以上の VPN ルーティングおよび転送（VRF）インスタンスに関連付けられています。VRF では、PE ルータに接続されているカスタマー サイトの VPN メンバーシップを定義します。VRF は、次のコンポーネントで構成されています。

- IP バージョン 4（IPv4）ユニキャスト ルーティング テーブル
- 取得された FIB テーブル
- 転送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 テーブルに格納されている情報を制御するための一連のルールおよびルーティング プロトコル パラメータ

これらのコンポーネントは一括して VRF インスタンスと呼ばれます。

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

パケット転送情報は、VRF ごとに IP ルーティング テーブルおよび FIB テーブルに格納されます。各 VRF の一連のルーティング テーブルと FIB テーブルは別々に維持されます。これらのテーブルにより、VPN の外側に情報が転送されないようになっているほか、VPN の外側のパケットも VPN 内のルータに転送されないようになっています。

VPN ルーティング情報：配信

VPN ルーティング情報の配布は、BGP 拡張コミュニティによって実装される VPN ルート ターゲット コミュニティを使用して制御されます。VPN ルーティング情報は、次のように配布されます。

- CE ルータから学習した VPN ルートが BGP に注入されると、VPN ルート ターゲット拡張コミュニティ属性のリストが、そのルートに関連付けられます。通常、ルート ターゲット コミュニティ拡張値のリストは、ルートの学習元の VRF に関連付けられているルート ターゲットのエクスポート リストから設定されます。

- ルート ターゲット拡張コミュニティのインポート リストは、各 VRF に関連付けられています。インポート リストには、ルートが VRF にインポートされるために、ルートに設定されている必要のある、ルート ターゲット拡張コミュニティ属性が定義されています。たとえば、ある特定の VRF のインポート リストにルート ターゲット拡張コミュニティ A、B、および C が含まれている場合、これらのルート ターゲット拡張コミュニティ A、B、または C のいずれかを伝送するすべての VPN ルートが VRF にインポートされます。

BGP による VPN ルーティング情報の配布

PE ルータは、次のソースから IP プレフィクスを学習します。

- 静的設定の CE ルータ
- CE ルータとの eBGP セッション
- CE ルータと交換する Routing Information Protocol（RIP）
- Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、および Interior Gateway Protocol（IGP）としての RIP

IP プレフィクスは、IPv4 アドレス ファミリのメンバです。PE ルータは、IP プレフィクスを学習した後、その IP プレフィクスを 64 ビットのルート識別子に結合することで、VPN-IPv4 プレフィクスに変換します。生成されたプレフィクスは、VPN-IPv4 アドレス ファミリのメンバです。このプレフィクスによって、カスタマー サイトでグローバルに一意でない（登録されていないプライベート）IP アドレスが使用される場合でも、カスタマーのアドレスが一意に識別されます。VPN-IPv4 プレフィクスを生成するために使用されるルート識別子は、**rd** コマンドによって指定し、PE ルータ上で VRF に関連付けられます。

BGP は、各 VPN の VPN-IPv4 プレフィクスに関する到達可能性情報を配布します。BGP 通信は、次の 2 つのレベルで行われます。

- 自律システムと呼ばれる IP ドメイン内。
- 自律システム間。

PE から PE または PE からルート リフレクタ（RR）へのセッションは iBGP セッション、PE から CE へのセッションは eBGP セッションです。PE から CE への eBGP セッションは、直接または間接的に接続できます（eBGP マルチホップ）。

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 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だけ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。

MPLS 転送

VRF IP ルーティング テーブルおよび VRF FIB テーブルに格納されているルーティング情報に基づき、MPLS を使用してパケットが宛先に転送されます。

PE ルータでは、CE ルータから学習した各カスタマー プレフィクスにラベルをバインドし、他の PE ルータにアドバタイズするプレフィクスのネットワーク到達可能性情報に、そのラベルを含めます。PE ルータは、プロバイダー ネットワークを介して CE ルータから受信したパケットを転送するときに、宛先 PE ルータから学習したラベルを使用してパケットにラベルを付けます。宛先 PE ルータは、ラベルの付いたパケットを受信すると、そのラベルをポップし、パケットを正しい CE ルータに誘導するために使用します。プロバイダー バックボーン経由のラベル転送は、ダイナミック ラベル スイッチングまたはトラフィック エンジニアリング パスのいずれかに基づきます。バックボーンを通過するカスタマー データ パケットが伝達するラベルには、2 つのレベルがあります。

- 最上位ラベルによって、パケットが正しい PE ルータに誘導されます。

- 2 番めのラベルは、PE ルータがパケットを CE ルータに転送する方法を示します。

他の機能がイネーブルの場合、より多くのラベルがスタックできます。たとえば、高速再ルーティング（FRR）が可能なトラフィック エンジニアリング（TE）トンネルがイネーブルの場合、PE で付加される総ラベル数は 4 です（レイヤ 3 VPN、ラベル配布プロトコル（LDP）、TE、FRR）。

自動ルート識別子の割り当て

iBGP ロード バランシングを利用するには、各ネットワークの VRF には一意のルート識別子を割り当てる必要があります。VRF では、異なる VPN から受信した潜在的に同一のプレフィクスを BGP が区別できるように、ルート識別子が必要です。

それぞれが複数の VRF をサポートするネットワークに多くのルータが存在する場合、ネットワーク全体でルート識別子を設定および管理すると、問題になる可能性があります。Cisco IOS XR ソフトウェアでは、**rd auto** コマンドを使用して VRF に一意のルート識別子を割り当てて、このプロセスが簡略化されます。

各ルータに一意のルート識別子を割り当てるには、各ルータは一意の BGP router-id を持つようにする必要があります。その場合、**rd auto** コマンドは、*ip-address:number* の形式を使用して VRF にタイプ 1 ルート識別子を割り当てます。IP アドレスは、BGP router-id ステートメントで指定し、数値（0 ～ 65535 の範囲の未使用インデックスとして取得）は VRF 全体で一意です。

最後に、フェールオーバーまたはプロセス再起動後も VRF へのルート識別子の割り当てが保持されるように、ルート識別子の値はチェックポイントされます。ルート識別子が VRF 用に明示的に設定されている場合、この値は自動ルート識別子によって上書きされることはありません。

MPLS L3VPN の主要コンポーネント

MPLS ベースの VPN ネットワークには、次の 3 つの主要コンポーネントがあります。

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

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

L3VPN の Inter-AS サポート

この項は次のトピックで構成されています。

- 「Inter-AS サポート：概要」（P.VPC-16）
- 「Inter-AS および ASBR」（P.VPC-16）
- 「連合」（P.VPC-17）
- 「MPLS VPN Inter-AS BGP ラベル配布」（P.VPC-18）
- 「MPLS ラベル付き IPv4 ルートの交換」（P.VPC-19）

Inter-AS サポート：概要

自律システム（AS）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 の複雑性および場所に関係なく、自律システム間の接続はシームレスでなければなりません。

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 バックボーンをまたがることが可能。

  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、共同で同じエンド 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 BGP 自律システム サービス プロバイダー バックボーンだけを通過できました。この機能は、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 が異なるエリアに存在可能。

  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。

- iBGP メッシングを最適化するための連合が可能。

  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た後、それらを単一の連合に分類できます。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。

Inter-AS および ASBR

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 NLRI を交換することによって通信できます。ASBR は、eBGP を使用してその情報を交換します。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。ルーティング情報は、次のプロトコルを使用して共有されます。

- 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 を使用することで、サービス プロバイダーは異なる自律システム間でのルーティング情報のループフリー交換を保証するドメイン間ルーティング システムを設定できます。

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 ルータを使用してラベル 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 ルータでは、ネクスト ホップおよび MPLS ラベルが書き換えられます。

MPLS VPN でサポートされている Inter-AS 設定には次のものがあります。

- プロバイダー間 VPN：異なるボーダー エッジ ルータ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、それらを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。

連合

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 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 eBGP 接続もあります。連合 eBGP（CEBGP）ボーダー エッジ ルータは、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、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。

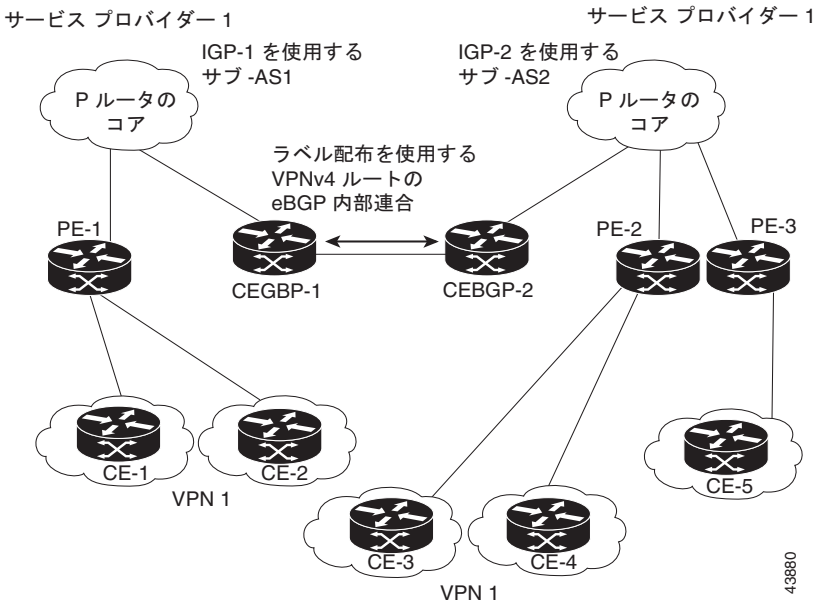
次の 2 つの方法で、異なるサブ自律システムに連合を設定できます。

- next-hop-self アドレスが CEBGP ボーダー エッジ ルータ間でだけ転送されるようにルータを設定します（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 ルータ 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 ルータ間（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ルータを設定します。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 ルータ間で next-hop-self アドレスの転送もします。CEBGP ボーダー エッジ ルータ アドレスは、IGP ドメイン内で認識されます。

図 2 に、一般的な MPLS VPN 連合設定を示します。この設定では、次のことが行われます。

- 2 つの CEBGP ボーダー エッジ ルータは、2 つの自律システム間で VPN-IPv4 アドレスおよびラベルを交換します。
- 配布元ルータはネクスト 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 2　　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 ルータは、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 ルータ（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、ルータのラベルを割り当てます。CEBGP ボーダー エッジ ルータは、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、NLRI の一部として符号化されます。
- 各 PE および CEBGP ボーダー エッジ ルータは、ルートを再配布する前に、各 VPN-IPv4 アドレス プレフィクスに独自のラベルを割り当てます。CEBGP ボーダー エッジ ルータは、ラベル付き IPV-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 ルータ 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 ルータが両方の連合で認識されます。

連合を設定する方法の詳細については、「ASBR 連合での MPLS 転送の設定」（P.MPC-65）を参照してください。

MPLS VPN Inter-AS BGP ラベル配布

（注）　このセクションは、Inter-AS over IP トンネルの場合には適用されません。

ASBR が、プロバイダー エッジ（PE）ルータの MPLS ラベル付き IPv4 ルートを交換するように MPLS VPN Inter-AS ネットワークを設定できます。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 BGP ラベル配布と呼ばれます。

ASBR が IPv4 ルートおよび MPLS ラベルを交換するように Inter-AS システムを設定することには次の利点があります。

- 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 リフレクタが VPN-IPv4 ルートを持つようにすることでも、ネットワーク境界での設定は簡素化されます。
- 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。
- 隣接ラベル スイッチ ルータ（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 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。

MPLS ラベル付き IPv4 ルートの交換

（注） このセクションは、Inter-AS over IP トンネルの場合には適用されません。

VPN サービス プロバイダー ネットワークを設定して、MPLS ラベル付き IPv4 ルートを交換できます。次のように VPN サービス プロバイダー ネットワークを設定できます。

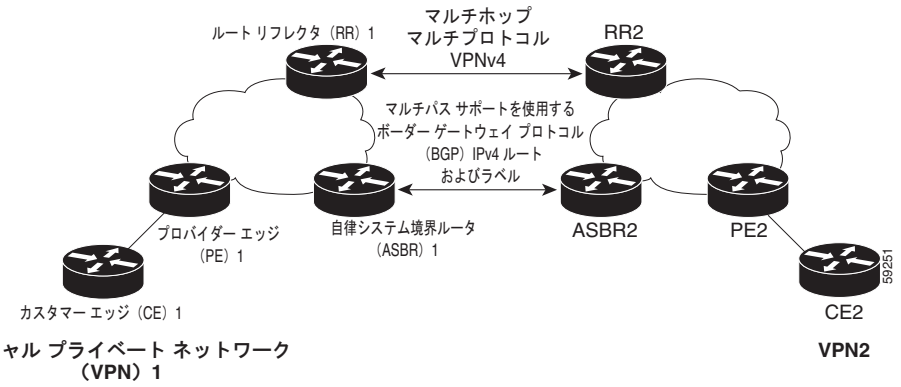
- ルート リフレクタは、マルチホップ マルチプロトコル eBGP を使用して VPN-IPv4 ルートを交換します。この設定では、自律システムをまたがってネクストホップ情報および VPN ラベルが維持されます。
- ローカル PE ルータ（たとえば図 3 の PE1）は、リモート PE ルータ（PE2）のルートおよびラベル情報を把握する必要があります。

  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。IGP および LDP から eBGP への再配布も可能です。
  - 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。この学習した IPv4 ルートおよび MPLS ラベルの反映は、ルート リフレクタと IPv4 ルートおよび MPLS ラベルを交換するように ASBR をイネーブルにすることで実現します。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、VPN1 では、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。

図 3　eBGP および iBGP を使用してルートと MPLS ラベルを配布する VPN



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 AS のリスト（自律システム（AS）パス）。リスト内の最初の AS 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 AS 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 AS です。
- ネクスト ホップなどの、AS パスについての他の情報を提供するパス属性。

BGP メッセージおよび 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。ルータでは、次のタイプの BGP メッセージが交換されます。

- 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。
- 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。（Cisco 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 ヘッダーだけが含まれています。
- 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。

MPLS ラベルとルートの送信

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 **show bgp neighbors** *ip-address* 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。

L3VPN の Carrier Supporting Carrier サポート

ここでは、MPLS VPN Carrier Supporting Carrier（CSC）機能に関する概念的な情報を説明します。次のトピックで構成されます。

- 「CSC の前提条件」（P.VPC-21）
- 「CSC の利点」（P.VPC-22）
- 「バックボーン キャリアとカスタマー キャリアの設定オプション」（P.VPC-22）

このマニュアルでは、次の用語は、CSC の文脈で使用されています。

バックボーン キャリア：別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。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：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。カスタマー キャリアは、インターネット サービス プロバイダー（ISP）または BGP/MPLS VPN サービス プロバイダーです。

CE ルータ：カスタマー エッジ ルータはカスタマー ネットワークの一部であり、プロバイダー エッジ（PE）ルータへのインターフェイスになります。このマニュアルでは、CE ルータはカスタマー キャリア ネットワークのエッジにあります。

PE ルータ：プロバイダー エッジ ルータはカスタマー エッジ（CE）ルータに接続されているサービス プロバイダーのネットワークの一部です。このマニュアルでは、PE ルータは、バックボーン キャリア ネットワークのエッジにあります。

ASBR：自律システム境界ルータは、ある自律システムを別の自律システムに接続します。

CSC の前提条件

CSC を設定するには、次の前提条件を満たす必要があります。

- 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。
- Interior Gateway Protocol（IGP）、MPLS ラベル配布プロトコル（LDP）、マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を設定できる必要があります。
- CSC-PE と CSC-CE ルータが、BGP ラベル配布をサポートしていることを確認する必要があります。

（注） BGP は、CE と PE 間のリンクでサポートされている唯一のラベル配布プロトコルです。

CSC の利点

ここでは、バックボーン キャリアとカスタマー キャリアにとっての CSC の利点について説明します。

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。
- MPLS VPN Carrier Supporting Carrier 機能は、スケーラブルです。
- MPLS VPN Carrier Supporting Carrier 機能は、柔軟なソリューションです。

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。
- 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。
- カスタマー キャリアは、任意のリンク層テクノロジーを使用して、CE ルータを PE ルータに接続します。
- 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。

BGP を使用する MPLS VPN CSC の実装の利点

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 は 2 つの ISP を接続する優先ルーティング プロトコルです。

バックボーン キャリアとカスタマー キャリアの設定オプション

CSC をイネーブルにするには、バックボーン キャリアとカスタマー キャリアは次の内容に従って設定されている必要があります。

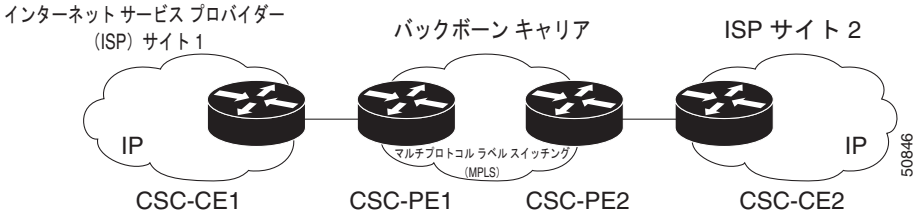
- バックボーン キャリアは、BGP と MPLS VPN サービスを提供する必要があります。
- カスタマー キャリアには、複数のネット ワーキングの形式があります。カスタマー キャリアは、次のものがあります。
  - IP コアを持つ ISP（「カスタマー キャリア：IP コアを持つ ISP」（P.MPC-23）を参照）。
  - VPN サービスを使用または使用しない MPLS サービス プロバイダー（「カスタマー キャリア：MPLS サービス プロバイダー」（P.MPC-23）を参照）。

（注） カスタマー キャリア ネットワークの IGP は CSC-CE にネクスト ホップおよびループバックを配布するために使用します。ラベル セッション付き IBGP は、CSC-CE にネクスト ホップおよびループバックを配布するためにカスタマー キャリア ネットワークで使用します。

カスタマー キャリア：IP コアを持つ ISP

図 4 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 または IP トンネルを使用して VPN サービスを提供します。ISP サイトは IP を使用します。

図 4　　ネットワーク：カスタマー キャリアが ISP

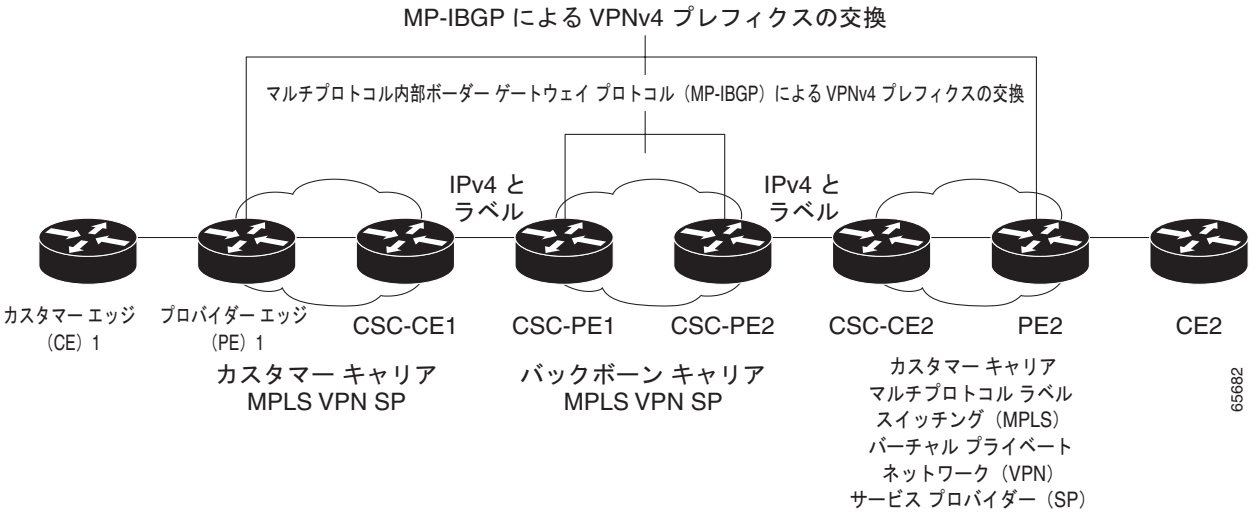


CE ルータと PE ルータ間のリンクでは、eBGP を使用して、IPv4 ルートと MPLS ラベルを配布します。これらのリンク間では、PE ルータはマルチプロトコル iBGP を使用して、VPNv4 ルートを配布します。

カスタマー キャリア：MPLS サービス プロバイダー

図 5 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。カスタマー キャリアには 2 つのサイトがあります。カスタマー キャリアは、ネットワークで MPLS を使用しますが、バックボーン キャリアはネットワークで MPLS または IP トンネルを使用します。

図 5　　ネットワーク：カスタマー キャリアが MPLS VPN サービス プロバイダー



この設定（図 5）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。

MPLS レイヤ 3 VPN の実装方法

ここでは、次のタスクの手順を説明します。

- 「コア ネットワークの設定」（P.VPC-24）
- 「MPLS VPN カスタマーの接続」（P.VPC-27）
- 「ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供」（P.VPC-49）（任意）
- 「ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供」（P.VPC-58）（任意）
- 「Carrier Supporting Carrier の設定」（P.VPC-68）（任意）
- 「MPLS レイヤ 3 VPN 設定の確認」（P.VPC-77）

コア ネットワークの設定

コア ネットワーク設定には、次の手順が含まれます。

- 「MPLS VPN カスタマーのニーズの評価」（P.VPC-24）
- 「コアにおけるルーティング プロトコルの設定」（P.VPC-25）
- 「コアにおける MPLS の設定」（P.VPC-25）
- 「FIB がコア上でイネーブルになっているかどうかの確認」（P.VPC-25）
- 「PE ルータおよびルート リフレクタでのマルチプロトコル BGP の設定」（P.VPC-26）

MPLS VPN カスタマーのニーズの評価

MPLS VPN を設定する前に、コア ネットワーク トポロジは最良のサービスを MPLS VPN カスタマーに提供できるように識別される必要があります。コア ネットワーク トポロジを識別するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ネットワークのサイズを識別します。	次の内容を特定して、必要なルータとポート数を決定します。 • サポートされるカスタマー数 • カスタマーごとに必要な VPN 数 • 各 VPN に存在する、仮想ルーティングおよび転送インスタンス（VRF）の数
ステップ 2	コアにおけるルーティング プロトコルを識別します。	コア ネットワークで必要なルーティング プロトコルを決定します。
ステップ 3	MPLS ハイ アベイラビリティのサポートが必要かどうかを決定します。	MPLS VPN ノンストップ フォワーディングおよびグレースフル リスタートは、選択ルータおよび Cisco IOS XR ソフトウェア リリースでサポートされています。
ステップ 4	BGP ロード シェアリングおよび冗長パスが必要かどうかを決定します。	MPLS VPN コアで BGP ロード シェアリングおよび冗長パスが必要であるかどうかを決定します。

コアにおけるルーティング プロトコルの設定

ルーティング プロトコルを設定するには、『*Cisco ASR 9000 Series Aggregation Services Routers Routing Configuration Guide*』を参照してください。

コアにおける MPLS の設定

コアのすべてのルータで MPLS をイネーブルにするには、ラベル配布プロトコル（LDP）を設定する必要があります。LDP として次のいずれかを使用しできます。

- MPLS LDP：設定の詳細については、『*Implementing MPLS Label Distribution Protocol on Cisco ASR 9000 Series Routers*』を参照してください。
- MPLS トラフィック エンジニアリング リソース予約プロトコル（RSVP）：設定の詳細については、このマニュアルの「*Implementing RSVP for MPLS-TE on Cisco ASR 9000 Series Routers*」を参照してください。

FIB がコア上でイネーブルになっているかどうかの確認

転送情報ベース（FIB）は、プロバイダー エッジ（PE）ルータを含むコア内のすべてのルータでイネーブルにする必要があります。FIB が使用可能かどうかを確認する方法については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』の「*Implementing Cisco Express Forwarding on Cisco ASR 9000 Series Routers*」モジュールを参照してください。

PE ルータおよびルート リフレクタでのマルチプロトコル BGP の設定

PE ルータおよびルート リフレクタ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. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family vpnv4 unicast**
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family vpnv4 unicast**
   end
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 120`	BGP 設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。
ステップ 3	**address-family vpnv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast`	VPNv4 アドレス ファミリに対応する VPNv4 アドレス ファミリ設定モードを開始します。
ステップ 4	**neighbor** *ip-address* **remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.168.40.24 remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**address-family vpnv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast`	VPNv4 アドレス ファミリに対応する VPNv4 アドレス ファミリ設定モードを開始します。

ステップ 6	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

MPLS VPN カスタマーの接続

MPLS VPN カスタマーを VPN に接続するには、次の作業を行います。

- 「カスタマーの接続を可能にするための、PE ルータでの VRF の定義」（P.VPC-28）
- 「各 VPN カスタマー用の PE ルータでの VRF インスタンスの設定」（P.VPC-30）
- 「BGP を PE ルータと CE ルータ間のルーティング プロトコルに設定」（P.VPC-32）（任意）
- 「RIPv2 を PE ルータと CE ルータ間のルーティング プロトコルに設定」（P.VPC-36）（任意）
- 「PE ルータと CE ルータ間のスタティック ルートの設定」（P.VPC-39）（任意）
- 「OSPF を PE ルータと CE ルータ間のルーティング プロトコルに設定」（P.VPC-40）（任意）
- 「EIGRP を PE ルータと CE ルータ間のルーティング プロトコルに設定」（P.VPC-43）（任意）
- 「MPLS VPN における EIGRP 再配布の設定」（P.VPC-46）（任意）

カスタマーの接続を可能にするための、PE ルータでの VRF の定義

VPN ルーティングおよび転送（VRF）インスタンスを定義するには、次の作業を実行します。

手順の概要

1. **configure**
2. **vrf** *vrf-name*
3. **address-family ipv4 unicast**
4. **import route-policy** *policy-name*
5. **import route-target** [*as-number:nn* | *ip-address:nn*]
6. **export route-policy** *policy-name*
7. **export route-target** [*as-number:nn* | *ip-address:nn*]
8. **exit**
9. **exit**
10. **router bgp** *autonomous-system-number*
11. **vrf** *vrf-name*
12. **rd** {*as-number* | *ip-address* | **auto**}
13. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config)# vrf vrf_1`	VRF インスタンスを設定し、VRF 設定モードを開始します。
ステップ 3	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast`	VRF アドレス ファミリに対応する IPv4 アドレス ファミリ設定モードを開始します。
ステップ 4	**import route-policy** *policy-name* **例：** `RP/0/RSP0/CPU0:router(config-vrf-af)# import route-policy policy_A`	ローカル VPN にインポートできるルート ポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 5	**import route-target** [*as-number:nn* | *ip-address:nn*] **例：** `RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 120:1`	エクスポートされたルートのルート ターゲットの 1 つが、ローカル VPN のインポート ルート ターゲットの 1 つと一致する場合に、エクスポートされた VPN ルートを VPN にインポートできるようにします。
ステップ 6	**export route-policy** *policy-name* **例：** `RP/0/RSP0/CPU0:router(config-vrf-af)# export route-policy policy_B`	ローカル VPN からエクスポートできるルート ポリシーを指定します。
ステップ 7	**export route-target** [*as-number:nn* | *ip-address:nn*] **例：** `RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 120:2`	ローカル VPN をルート ターゲットに関連付けます。ルートが他のプロバイダー エッジ（PE）ルータにアドバタイズされる際に、エクスポート ルート ターゲットが拡張コミュニティとしてルートとともに送信されます。
ステップ 8	**exit** **例：** `RP/0/RSP0/CPU0:router(config-vrf-af)# exit`	VRF アドレス ファミリ設定モードを終了し、ルータを VRF 設定モードに戻します。
ステップ 9	**exit** **例：** `RP/0/RSP0/CPU0:router(config-vrf)# exit`	VRF 設定モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**router bgp** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 120`	BGP 設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。
ステップ 11	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf_1`	VRF インスタンスを設定し、BGP ルーティングの VRF 設定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 12	**rd** {*as-number* | *ip-address* | **auto**} **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd auto`	自動的に vrf_1 に一意のルート識別子（RD）を割り当てます。

ステップ 13	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

各 VPN カスタマー用の PE ルータでの VRF インスタンスの設定

VPN ルーティングおよび転送（VRF）インスタンスを PE ルータのインターフェイスまたはサブ インターフェイスを割り当てるには、次の作業を実行します。

（注） インターフェイスの VRF の割り当て、削除、または変更を行う前に、IPv4/IPv6 アドレスをインターフェイスから削除する必要があります。これを事前に行わない場合、IP インターフェイス上での VRF 変更はすべて拒否されます。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **vrf** *vrf-name*
4. **ipv4 address** *ipv4-address mask*
5. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/3/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-if)# vrf vrf_A`	VRF インスタンスを設定し、VRF 設定モードを開始します。
ステップ 4	**ipv4 address** *ipv4-address mask* **例：** `RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0`	指定したインターフェイスのプライマリ IPv4 アドレスを設定します。

ステップ 5	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

BGP を PE ルータと CE ルータ間のルーティング プロトコルに設定

BGP を使用して PE-to-CE 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. **configure**
2. **router bgp** *autonomous-system-number*
3. **bgp router-id** {*ip-address*}
4. **vrf** *vrf-name*
5. **label-allocation-mode** *per-ce*
6. **address-family ipv4 unicast**
7. **redistribute connected** [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   または
   redistribute isis *process-id* [**level** {**1** | **1-inter-area** | **2**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   または
   redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   または
   redistribute static [**metric** *metric-value*] [**route-policy** *route-policy-name*]
8. **aggregate-address** *address/mask-length* [**as-set**] [**as-confed-set**] [**summary-only**] [**route-policy** *route-policy-name*]
9. **network** {*ip-address/prefix-length* | *ip-address mask*} [**route-policy** *route-policy-name*]
10. **exit**
11. **neighbor** *ip-address*
12. **remote-as** *autonomous-system-number*
13. **password** {**clear** | **encrypted**} *password*
14. **ebgp-multihop** [*ttl-value*]
15. **address-family ipv4 unicast**
16. **allowas-in** [*as-occurrence-number*]
17. **route-policy** *route-policy-name* **in**
18. **route-policy** *route-policy-name* **out**
19. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 120`	ボーダー ゲートウェイ プロトコル（BGP）設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。
ステップ 3	**bgp router-id** {*ip-address*} **例：** `RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 192.168.70.24`	ローカル ルータに 192.168.70.24 のルータ ID を設定します。
ステップ 4	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、BGP ルーティングの VRF 設定モードを開始します。
ステップ 5	**label-allocation-mode per-ce** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# label-allocation-mode per-ce`	各カスタマー エッジ（CE）ラベル モードに MPLS VPN ラベル割り当てモードを設定します。プロバイダー エッジ（PE）ルータは、このモードで、即時ネクストホップ 1 つにつき 1 つのラベルを割り当てることができます。
ステップ 6	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 unicast`	VRF アドレス ファミリに対応する IPv4 アドレス ファミリ設定モードを開始します。
ステップ 7	**redistribute connected** [**metric** *metric-value*] [**route-policy** *route-policy-name*] または **redistribute isis** *process-id* [**level** {**1** | **1-inter-area** | **2**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*] または **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** route-policy-name] または **redistribute static** [**metric** *metric-value*] [**route-policy** *route-policy-name*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute connected`	ルートが BGP に再配布されるようにします。BGP に再配布できるルートは次のとおりです。 • 接続 • Intermediate System-to-Intermediate System（IS-IS） • Open Shortest Path First（OSPF） • スタティック

	コマンドまたはアクション	目的
ステップ 8	**aggregate-address** *address/mask-length* [**as-set**] [**as-confed-set**] [**summary-only**] [**route-policy** *route-policy-name*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# aggregate-address 10.0.0.0/8 as-set`	集約アドレスを作成します。このルートにアドバタイズされたパスは、集約されるすべてのパスに含まれるすべての要素で構成された自律システム セットです。 • **as-set** キーワードで、自律システム セット パス情報および関係するパスに基づくコミュニティ情報が生成されます。 • **as-confed-set** キーワードで、関係するパスから自律システム連合セット パス情報が生成されます。 • **summary-only** キーワードによって、アップデートから固有性の強いルートがすべてフィルタリングされます。 • **route-policy** *route-policy-name* キーワードと引数は集約ルートの属性を設定するために使用されるルート ポリシーを指定します。
ステップ 9	**network** {*ip-address/prefix-length* | *ip-address mask*} [**route-policy** *route-policy-name*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# network 172.20.0.0/16`	指定されたネットワークを開始し、アドバタイズするようにローカル ルータを設定します。
ステップ 10	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# exit`	VRF アドレス ファミリ設定モードを終了し、ルータを BGP ルーティングの VRF 設定モードに戻します。
ステップ 11	**neighbor** *ip-address* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# neighbor 172.168.40.24`	ルータを BGP ルーティングの VRF ネイバー設定モードにして、ネイバーの IP アドレス 172.168.40.24 を BGP ピアとして設定します。
ステップ 12	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。
ステップ 13	**password** {**clear** | **encrypted**} *password* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# password clear pswd123`	ネイバー 172.168.40.24 を、パスワード pswd123 で MD5 認証を使用するように設定します。
ステップ 14	**ebgp-multihop** [*ttl-value*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# ebgp-multihop`	ネイバー 172.168.40.24 への BGP 接続を許可します。

	コマンドまたはアクション	目的
ステップ 15	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# address-family ipv4 unicast`	BGP ルーティングの VRF ネイバー アドレス ファミリ設定モードを開始します。
ステップ 16	**allowas-in** [*as-occurrence-number*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# allowas-in 3`	ネイバーの自律システム番号（ASN）を、AS パスの PE ASN に 3 回置き換えます。
ステップ 17	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy In-Ipv4 in`	インバウンド IPv4 ユニキャスト ルートに In-Ipv4 ポリシーを適用します。
ステップ 18	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy In-Ipv4 in`	アウトバウンド IPv4 ユニキャスト ルートに In-Ipv4 ポリシーを適用します。

ステップ 19	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

RIPv2 を PE ルータと CE ルータ間のルーティング プロトコルに設定

Routing Information Protocol version 2（RIPv2）を使用してプロバイダー エッジ（PE）からカスタマー エッジ（CE）へのルーティング 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. **configure**
2. **router rip**
3. **vrf** *vrf-name*
4. **interface** *type instance*
5. **site-of-origin** {*as-number*:*number* | *ip-address*:*number*}
6. **exit**
7. **redistribute bgp** *as-number* [[**external** | **internal** | **local**] [**route-policy** *name*]
   または
   redistribute connected [**route-policy** *name*]
   または
   redistribute isis *process-id* [**level-1** | **level-1-2** | **level-2**] [**route-policy** *name*]
   または
   redistribute eigrp *as-number* [**route-policy** *name*]
   または
   redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**route-policy** *name*]
   または
   redistribute static [**route-policy** *name*]
8. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router rip** **例：** `RP/0/RSP0/CPU0:router(config)# router rip`	Routing Information Protocol（RIP）設定モードを開始します。このモードでは、RIP ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-rip)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、RIP ルーティングの VRF 設定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 4	**interface** *type instance* **例：** `RP/0/RSP0/CPU0:router(config-rip-vrf)# interface GigabitEthernet 0/3/0/0`	VRF インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**site-of-origin** {*as-number:number* | *ip-address:number*} **例：** `RP/0/RSP0/CPU0:router(config-rip-vrf-if)# site-of-origin 200:1`	送信元サイトへのプレフィクスの再アドバタイズメントを回避するために、サイトから生じたルートを特定します。PE ルータがルートを学習したサイトを一意に識別します。
ステップ 6	**exit** **例：** `RP/0/RSP0/CPU0:router(config-rip-vrf-if)# exit`	VRF 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、ルータを RIP ルーティングの VRF 設定モードに戻します。

	コマンドまたはアクション	目的
ステップ 7	**redistribute bgp** *as-number* [[**external** | **internal** | **local**] [**route-policy** *name*] または **redistribute connected** [**route-policy** *name*] または **redistribute eigrp** *as-number* [**route-policy** *name*] または **redistribute isis** *process-id* [**level-1** | **level-1-2** | **level-2**] [**route-policy** *name*] または **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**route-policy** *name*] または **redistribute static** [**route-policy** *name*] **例：** `RP/0/RSP0/CPU0:router(config-rip-vrf)# redistribute connected`	ルートが RIP に再配布されるようにします。RIP に再配布できるルートは次のとおりです。 • ボーダー ゲートウェイ プロトコル（BGP） • 接続 • Enhanced Interior Gateway Routing Protocol（EIGRP） • Intermediate System-to-Intermediate System（IS-IS） • Open Shortest Path First（OSPF） • スタティック

ステップ 8	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-rip-vrf)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rip-vrf)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

PE ルータと CE ルータ間のスタティック ルートの設定

プロバイダー エッジ（PE）からカスタマー エッジ（CE）へスタティック ルートを使用するルーティング セッションを設定するには、次の作業を実行します。

（注） インターフェイスの VRF の割り当て、削除、または変更を行う前に、IPv4/IPv6 アドレスをインターフェイスから削除する必要があります。これを事前に行わない場合、IP インターフェイス上での VRF 変更はすべて拒否されます。

手順の概要

1. **configure**
2. **router static**
3. **vrf** *vrf-name*
4. **address-family ipv4 unicast**
5. *prefix/mask* [**vrf** *vrf-name*] {*ip-address* | *type interface-path-id*}
6. *prefix/mask* [**vrf** *vrf-name*] **bfd fast-detect**
7. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router static** **例：** `RP/0/RSP0/CPU0:router(config)# router static`	スタティック ルーティング設定モードを開始します。このモードでは、スタティック ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-static)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、スタティック ルーティングの VRF 設定モードを開始します。
ステップ 4	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-static-vrf)# address-family ipv4 unicast`	VRF アドレス ファミリに対応する IPv4 アドレス ファミリ設定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 5	*prefix/mask* [**vrf** *vrf-name*] {*ip-address* | type interface-path-id} **例：** RP/0/RSP0/CPU0:router(config-static-vrf-afi)# 172.168.40.24/24 vrf vrf_1 10.1.1.1	vrf_1 にスタティック ルートを割り当てます。
ステップ 6	*prefix/mask* [**vrf** *vrf-name*] **bfd fast-detect** **例：** RP/0/RSP0/CPU0:router(config-static-vrf-afi)# 172.168.40.24/24 vrf vrf_1 bfd fast-detect	隣接する転送エンジン間のパスで障害を検出するために、双方向フォワーディング検出（BFD）をイネーブルにします。 このオプションは、ステップ 5 で転送ルータのアドレスを指定した場合に使用できます。
ステップ 7	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-static-vrf-afi)# end または RP/0/RSP0/CPU0:router(config-static-vrf-afi)# commit	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

OSPF を PE ルータと CE ルータ間のルーティング プロトコルに設定

プロバイダー エッジ（PE）からカスタマー エッジ（CE）へ Open Shortest Path First（OSPF）を使用するルーティング 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. **configure**
2. **router ospf** *process-name*
3. **vrf** *vrf-name*
4. **router-id** {*router-id* | *type interface-path-id*}
5. **redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または

redistribute connected [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
または
redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
または
redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
または
redistribute eigrp *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
または
redistribute rip [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

6. **area** *area-id*
7. **interface** *type interface-path-id*
8. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-name* **例：** `RP/0/RSP0/CPU0:router(config)# router ospf 109`	OSPF 設定モードを開始します。このモードでは、OSPF ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-ospf)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、OSPF ルーティングの VRF 設定モードを開始します。
ステップ 4	**router-id** {*router-id* | type interface-path-id} **例：** `RP/0/RSP0/CPU0:router(config-ospf-vrf)# router-id 172.20.10.10`	OSPF ルーティング プロセスのルータ ID 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	**redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute connected** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute static** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute eigrp** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}][**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute rip** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] **例：** `RP/0/RSP0/CPU0:router(config-ospf-vrf)# redistribute connected`	ルートが OSPF に再配布されるようにします。OSPF に再配布できるルートは次のとおりです。 • ボーダー ゲートウェイ プロトコル（BGP） • 接続 • Enhanced Interior Gateway Routing Protocol（EIGRP） • OSPF • スタティック • Routing Information Protocol（RIP; ルーティング情報プロトコル）
ステップ 6	**area** *area-id* **例：** `RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 0`	OSPF エリアをエリア 0 として設定します。

	コマンドまたはアクション	目的
ステップ 7	**interface** type interface-path-id **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf-ar)# interface GigabitEthernet 0/3/0/0	インターフェイス GigabitEthernet 0/3/0/0 をエリア 0 に関連付けます。
ステップ 8	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf-ar-if)# end または RP/0/RSP0/CPU0:router(config-ospf-vrf-ar-if)# commit	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

EIGRP を PE ルータと CE ルータ間のルーティング プロトコルに設定

プロバイダー エッジ（PE）からカスタマー エッジ（CE）へ Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するルーティング セッションを設定するには、次の作業を実行します。

PE ルータと CE ルータ間で EIGRP を使用すると、MPLS 対応ボーダー ゲートウェイ プロトコル（BGP）コア ネットワークを介して EIGRP カスタマー ネットワークを透過的に接続できるため、EIGRP ルートは、内部 BGP（iBGP）として BGP ネットワーク全体で VPN を介して再配布されます。

前提条件

BGP は、ネットワークで設定されている必要があります。『*Cisco ASR 9000 Series Aggregation Services Routers Routing Configuration Guide*』の「*Implementing BGP on Cisco ASR 9000 Series Routers*」モジュールを参照してください。

（注） インターフェイスの VRF の割り当て、削除、または変更を行う前に、IPv4/IPv6 アドレスをインターフェイスから削除する必要があります。これを事前に行わない場合、IP インターフェイス上での VRF 変更はすべて拒否されます。

手順の概要

1. **configure**
2. **router eigrp** *as-number*
3. **vrf** *vrf-name*
4. **address-family ipv4**
5. **router-id** *router-id*
6. **autonomous-system** *as-number*
7. **default-metric** *bandwidth delay reliability loading mtu*
8. **redistribute** {{**bgp** | **connected** | **isis** | **ospf**| **rip** | **static**} [*as-number* | *instance-name*]} [**route-policy** *name*]
9. **interface** *type interface-path-id*
10. **site-of-origin** {*as-number:number* | *ip-address:number*}
11. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router eigrp 24`	EIGRP 設定モードを開始します。このモードでは、EIGRP ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-eigrp)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、EIGRP ルーティングの VRF 設定モードを開始します。
ステップ 4	**address-family ipv4** **例：** `RP/0/RSP0/CPU0:router(config-eigrp-vrf)# address family ipv4`	VRF アドレス ファミリに対応する IPv4 アドレス ファミリ設定モードを開始します。
ステップ 5	**router-id** *router-id* **例：** `RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# router-id 172.20.0.0`	Enhanced Interior Gateway Routing Protocol（EIGRP）ルーティング プロセスのルータ ID を設定します。

	コマンドまたはアクション	目的
ステップ 6	**autonomous-system** *as-number* **例：** RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# autonomous-system 6	VRF 内で実行する EIGRP ルーティング プロセスを設定します。
ステップ 7	**default-metric** *bandwidth delay reliability loading mtu* **例：** RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# default-metric 100000 4000 200 45 4470	EIGRP のメトリックを設定します。
ステップ 8	**redistribute** {{**bgp** | **connected** | **isis** | **ospf**| **rip** | **static**} [*as-number* | *instance-name*]} [**route-policy** *name*] **例：** RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# redistribute connected	接続ルートが EIGRP に再配布されるようにします。
ステップ 9	**interface** type interface-path-id **例：** RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# interface GigabitEthernet 0/3/0/0	インターフェイス GigabitEthernet 0/3/0/0 を EIGRP ルーティング プロセスに関連付けます。

	コマンドまたはアクション	目的
ステップ 10	**site-of-origin** {*as-number:number* | *ip-address:number*} **例：** `RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# site-of-origin 201:1`	インターフェイス GigabitEthernet 0/3/0/0 に Site of Origin（SoO）を設定します。

ステップ 11	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

MPLS VPN における EIGRP 再配布の設定

VPN サービスを提供する各プロバイダー エッジ（PE）ルータに対して次の作業を行い、MPLS VPN での Enhanced Interior Gateway Routing Protocol（EIGRP）再配布をイネーブルにします。

前提条件

メトリックは、**redistribute** コマンドの route-policy 設定で設定（または **default-metric** コマンドで設定）できます。別の EIGRP 自律システムまたはメトリックが設定されていない非 EIGRP ネットワークから外部ルートを受信した場合、ルートは EIGRP データベースにインストールされません。別の EIGRP 自律システムまたはメトリックが設定されていない非 EIGRP ネットワークから外部ルートを受信した場合、ルートは CE ルータにアドバタイズされません。『*Cisco ASR 9000 Series Aggregation Services Routers Routing Configuration Guide*』の「*Implementing EIGRP on Cisco ASR 9000 Series Routers*」モジュールを参照してください。

制約事項

ネイティブ EIGRP VPN ルーティングおよび転送（VRF）インスタンス間の再配布はサポートされません。この動作は意図的なものです。

手順の概要

1. **configure**
2. **router eigrp** as-number
3. **vrf** *vrf-name*
4. **address-family ipv4**
5. **redistribute bgp** [*as-number*] [**route-policy** *policy-name*]
6. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router eigrp 24`	EIGRP 設定モードを開始します。このモードでは、EIGRP ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-eigrp)# vrf vrf_1`	VRF インスタンスを設定し、EIGRP ルーティングの VRF 設定モードを開始します。
ステップ 4	**address-family ipv4** **例：** `RP/0/RSP0/CPU0:router(config-eigrp-vrf)# address family ipv4`	VRF アドレス ファミリに対応する IPv4 アドレス ファミリ設定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 5	**redistribute bgp** [*as-number*] [**route-policy** *policy-name*] **例：** `RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# redistribute bgp 24 route-policy policy_A`	ボーダー ゲートウェイ プロトコル（BGP）ルートが EIGRP に再配布されるようにします。

ステップ 6	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASBR で IPv4 ルートおよび MPLS ラベルを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供

（注） このセクションは、Inter-AS over IP トンネルの場合には適用されません。

ここでは、次のタスクの手順を説明します。

- 「IPv4 ルートおよび MPLS ラベルを交換する ASBR の設定」（P.VPC-49）
- 「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」（P.VPC-52）
- 「ルート リフレクタが AS 内でリモート ルートを反映するように設定する」（P.VPC-55）

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。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family ipv4 unicast**
4. **allocate-label all**
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **address-family ipv4 labeled-unicast**
8. **route-policy** *route-policy-name* **in**
9. **route-policy** *route-policy-name* **out**
10. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *autonomous-system-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 120`
	`RP/0/RSP0/CPU0:router(config-bgp)#`
		ボーダー ゲートウェイ プロトコル（BGP）設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

	コマンドまたはアクション	目的

ステップ 3	**address-family ipv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-af)#`
		IPv4 ユニキャスト アドレス ファミリに対応するグローバル アドレス ファミリ設定モードを開始します。

ステップ 4	**allocate-label all** **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# allocate-label all`	MPLS ラベルを特定の IPv4 ユニキャストまたは VPN ルーティングおよび転送（VRF）IPv4 ユニキャスト ルートに割り当て、BGP ルータがラベル付きユニキャスト セッションを設定した隣接ルータに BGP ルートとともにラベルを送信できるようにします。

ステップ 5	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 172.168.40.24 を BGP ピアとして設定します。

ステップ 6	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

ステップ 7	**address-family ipv4 labeled-unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)`
		IPv4 ラベル付きユニキャスト アドレス ファミリに対応するネイバー アドレス ファミリ設定モードを開始します。

ステップ 8	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in`	BGP ネイバーから受信されるアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • インバウンド ルートのポリシーを定義するために、**in** 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 9	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out`	BGP ネイバーに送信されるアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • アウトバウンド ルートのポリシーを定義するために **out** キーワードを使用します。

ステップ 10	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

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。ここでは、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。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *ip-address*
4. **remote-as** *autonomous-system-number*
5. **ebgp-multihop** [*ttl-value*]
6. **update-source** *type interface-path-id*
7. **address-family vpnv4 unicast**
8. **route-policy** *route-policy-name* **in**
9. **route-policy** *route-policy-name* **out**
10. **next-hop-unchanged**
11. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *autonomous-system-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 120`
	`RP/0/RSP0/CPU0:router(config-bgp)#`
		ボーダー ゲートウェイ プロトコル（BGP）設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

ステップ 3	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.168.40.24`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 172.168.40.24 を BGP ピアとして設定します。

ステップ 4	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**ebgp-multihop** [*ttl-value*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# ebgp-multihop`	外部 BGP ネイバーとのマルチホップ ピアリングをイネーブルにします。
ステップ 6	**update-source** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0`	BGP セッションが、特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。

ステップ 7	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 8	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in`	BGP ネイバーから受信されるアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • インバウンド ルートのポリシーを定義するために、**in** キーワードを使用します。
ステップ 9	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out`	BGP ネイバーに送信されるアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • アウトバウンド ルートのポリシーを定義するために **out** 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 10	**next-hop-unchanged** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-unchanged`	外部ボーダー ゲートウェイ プロトコル（eBGP）ピアにアドバタイズする前に、ネクスト ホップの上書きをディセーブルにします。

ステップ 11	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ルート リフレクタが AS 内でリモート ルートを反映するように設定する

ルート リフレクタ（RR）が、自律システム境界ルータから学習した IPv4 ルートおよびラベルを、自律システム内のプロバイダー エッジ（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 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。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family ipv4 unicast**
4. **allocate-label all**
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **update-source** *type interface-path-id*
8. **address-family ipv4 labeled-unicast**
9. **route-reflector-client**
10. **neighbor** *ip-address*
11. **remote-as** *autonomous-system-number*
12. **update-source** *type interface-path-id*
13. **address-family ipv4 labeled-unicast**
14. **route-reflector-client**
15. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 120`	ボーダー ゲートウェイ プロトコル（BGP）設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

ステップ 3	**address-family ipv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-af)#`
		IPv4 ユニキャスト アドレス ファミリに対応するグローバル アドレス ファミリ設定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 4	**allocate-label all** **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# allocate-label all`	MPLS ラベルを特定の IPv4 ユニキャストまたは VPN ルーティングおよび転送（VRF）IPv4 ユニキャスト ルートに割り当て、BGP ルータがラベル付きユニキャスト セッションを設定した隣接ルータに BGP ルートとともにラベルを送信できるようにします。

ステップ 5	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 172.168.40.24 を ASBR eBGP ピアとして設定します。

ステップ 6	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。
ステップ 7	**update-source** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0`	BGP セッションが、特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。

ステップ 8	**address-family ipv4 labeled-unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		IPv4 ラベル付きユニキャスト アドレス ファミリに対応するネイバー アドレス ファミリ設定モードを開始します。

ステップ 9	**route-reflector-client** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、ネイバー 172.168.40.24 をそのクライアントとして設定します。

ステップ 10	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# neighbor 10.40.25.2`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 10.40.25.2 を VPNv4 iBGP ピアとして設定します。

ステップ 11	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

	コマンドまたはアクション	目的
ステップ 12	**update-source** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0`	BGP セッションが、特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。

ステップ 13	**address-family ipv4 labeled-unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		IPv4 ラベル付きユニキャスト アドレス ファミリに対応するネイバー アドレス ファミリ設定モードを開始します。

ステップ 14	**route-reflector-client** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client`	ネイバーをルート リフレクタ クライアントとして設定します。

ステップ 15	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASBR で VPN-IPv4 アドレスを交換する MPLS VPN Inter-AS を使用する複数の自律システム間への VPN 接続性の提供

ここでは、次のタスクの手順を説明します。

- 「VPN-IPv4 アドレスを交換するように ASBR を設定する」（P.VPC-58）
- 「ASBR ピアへのスタティック ルートの設定」（P.VPC-61）
- 「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」（P.VPC-63）
- 「ASBR 連合での MPLS 転送の設定」（P.VPC-65）
- 「ASBR 連合ピアへのスタティック ルートの設定」（P.VPC-67）

VPN-IPv4 アドレスを交換するように ASBR を設定する

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、他の自律システムと VPN-IPv4 ルートを交換するように設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family vpnv4 unicast**
4. **retain route-target {all | route-policy** *route-policy-name*}
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **address-family vpnv4 unicast**
8. **route-policy** *route-policy-name* **in**
9. **route-policy** *route-policy-name* **out**
10. **neighbor** *ip-address*
11. **remote-as** *autonomous-system-number*
12. **update-source** *type interface-path-id*
13. **address-family vpnv4 unicast**
14. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *autonomous-system-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 120`
	`RP/0/RSP0/CPU0:router(config-bgp)#`
		ボーダー ゲートウェイ プロトコル（BGP）設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

ステップ 3	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)#`
	`address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 4	**retain route-target** {**all** | **route-policy** *route-policy-name*} **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# retain route-target route-policy policy1`	PE ルータから VPNv4 テーブルを取得します。 Inter-AS オプション B ASBR で **retain route-target** コマンドが必要です。**all** または **route-policy** キーワードと一緒にこのコマンドを使用できます。

ステップ 5	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 172.168.40.24 を ASBR eBGP ピアとして設定します。

ステップ 6	**remote-as** *autonomous-system-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
	`remote-as 2002`
		ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

ステップ 7	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
	`address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		VPNv4 アドレス ファミリを設定します。

	コマンドまたはアクション	目的
ステップ 8	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in`	BGP ネイバーから受信されるアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • インバウンド ルートのポリシーを定義するために、**in** キーワードを使用します。
ステップ 9	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out`	BGP ネイバーから送信されたアップデートに、ルーティング ポリシーを適用します。 • ルート ポリシーの名前を定義するために *route-policy-name* 引数を使用します。例では、ルート ポリシーの名前が pass-all として定義されていることを示します。 • アウトバウンド ルートのポリシーを定義するために **out** キーワードを使用します。

ステップ 10	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# neighbor 10.40.25.2`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 10.40.25.2 を VPNv4 iBGP ピアとして設定します。

ステップ 11	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。
ステップ 12	**update-source** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0`	BGP セッションが、特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。

	コマンドまたはアクション	目的

ステップ 13	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 14	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASBR ピアへのスタティック ルートの設定

ASBR ピアにスタティック ルートを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*
5. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router static**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router static`
	`RP/0/RSP0/CPU0:router(config-static)#`
		ルータ スタティック コンフィギュレーション モードを開始します。

ステップ 3	**address-family ipv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-static)#`
	`address-family ipv4 unicast`
	`RP/0/RSP0/CPU0:router(config-static-afi)#`
		IPv4 アドレス ファミリをイネーブルにします。

ステップ 4	***A.B.C.D/length*** *next-hop*
	
	例：
	`RP/0/RSP0/CPU0:router(config-static-afi)#`
	`10.10.10.10/32 10.9.9.9`
		宛先ルータのアドレスを入力します（IPv4 サブネット マスクを含む）。

ステップ 5	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-static-afi)# end`
	または
	`RP/0/RSP0/CPU0:router(config-static-afi)#`
	`commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?`
		`[cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

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 ルートを交換する外部ボーダー ゲートウェイ プロトコル（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 ルートが他のルータおよび PE ルータに（Interior Gateway Protocol（IGP）を使用して）伝播されるようにするには、連合 eBGP（CEBGP）の IGP 設定部分で **redistribute connected** コマンドを指定します。Open Shortest Path First（OSPF）を使用する場合、「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されていないことを確認します。

手順の概要

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **bgp confederation peers** *peer autonomous-system-number*
4. **bgp confederation identifier** *autonomous-system-number*
5. **address-family vpnv4 unicast**
6. **neighbor** *ip-address*
7. **remote-as** *autonomous-system-number*
8. **address-family vpnv4 unicast**
9. **route-policy** *route-policy-name* **in**
10. **route-policy** *route-policy-name* **out**
11. **next-hop-self**
12. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *autonomous-system-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 120`
	`RP/0/RSP0/CPU0:router(config-bgp)#`
		BGP 設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

	コマンドまたはアクション	目的
ステップ 3	**bgp confederation peers** *peer autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# bgp confederation peers 8`	連合に属するピアの自律システム番号を設定します。
ステップ 4	**bgp confederation identifier** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# bgp confederation identifier 5`	連合 ID の自律システム番号を指定します。

ステップ 5	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 6	**neighbor** *ip-address*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 10.168.40.24`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		ルータを BGP ルーティングのネイバー設定モードにして、ネイバーの IP アドレス 10.168.40.24 を BGP ピアとして設定します。

ステップ 7	**remote-as** *autonomous-system-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002`	ネイバーを作成し、そのネイバーをリモート自律システム番号に割り当てます。

ステップ 8	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 9	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy In-Ipv4 in`	BGP ネイバーから受信されるアップデートに、ルーティング ポリシーを適用します。
ステップ 10	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy Out-Ipv4 out`	BGP ネイバーにアドバタイズされるアップデートに、ルーティング ポリシーを適用します。

	コマンドまたはアクション	目的
ステップ 11	**next-hop-self** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-self`	ネクストホップ計算をディセーブルにし、BGP アップデートのネクストホップ フィールドにユーザ自身のアドレスの挿入を許可します。

ステップ 12	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASBR 連合での MPLS 転送の設定

指定したインターフェイスで自律システム境界ルータ（ASBR）連合（BGP 内）への MPLS 転送を設定するには、次の作業を実行します。

（注） この設定は、インターフェイスに関連付けられたピアに対応する暗黙のヌル書き換えを追加します。これは、（マルチホップ インスタンスで）BGP が LDP によって自動的にリライトをインストールしないようにするために必要です。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **mpls activate**
4. **interface** *type interface-path-id*
5. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *as-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 120`
	`RP/0/RSP0/CPU0:router(config-bgp)`
		BGP 設定モードを開始します。このモードでは、BGP ルーティング プロセスの設定を行えます。

ステップ 3	**mpls activate**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# mpls activate`
	`RP/0/RSP0/CPU0:router(config-bgp-mpls)#`
		BGP MPLS アクティブ化設定モードを開始します。

ステップ 4	**interface** *type interface-path-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-mpls)# interface GigabitEthernet 0/3/0/0`	インターフェイスで MPLS をイネーブルにします。

ステップ 5	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-mpls)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-mpls)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ASBR 連合ピアへのスタティック ルートの設定

Inter-AS 連合ピアにスタティック ルートを設定するには、次の作業を実行します。詳細については、「ピアへのスタティック ルートの設定」（P.MPC-76）を参照してください。

手順の概要

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*
5. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router static**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router static`
	`RP/0/RSP0/CPU0:router(config-static)#`
		ルータ スタティック コンフィギュレーション モードを開始します。

ステップ 3	**address-family ipv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-static)#`
	`address-family ipv4 unicast`
	`RP/0/RSP0/CPU0:router(config-static-afi)#`
		IPv4 アドレス ファミリ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 4	***A.B.C.D/length*** *next-hop* **例：** `RP/0/RSP0/CPU0:router(config-static-afi)# 10.10.10.10/32 10.9.9.9`	宛先ルータのアドレスを入力します（IPv4 サブネット マスクを含む）。

ステップ 5	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-static-afi)# end`
	または
	`RP/0/RSP0/CPU0:router(config-static-afi)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

Carrier Supporting Carrier の設定

Carrier Supporting Carrier（CSC）を設定するには、このセクションの作業を実行します。

- 「Carrier Supporting Carrier トポロジの識別」（P.VPC-68）
- 「バックボーン キャリア コアの設定」（P.VPC-69）
- 「CSC-PE ルータと CSC-CE ルータの設定」（P.VPC-69）
- 「ピアへのスタティック ルートの設定」（P.VPC-76）

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。

（注） 複数の CSC-CE 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. CE ルータを識別します。
3. カスタマー キャリア 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。
ステップ 2	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	カスタマー キャリア コア ルータの設定を識別します。	コア（P）ルータ間、および P ルータとエッジ ルータ（PE ルータと CSC-CE ルータ）間の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）間の設定に関する要件を設定します。

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。これを行うには、次の高レベルのタスクを完了する必要があります。

- CSC コアの IP 接続を確認します。
- CSC コアの LDP 設定を確認します。

（注） この作業は、CSC over IP トンネルの場合には適用されません。

- CSC-PE ルータの VRF を設定します。
- バックボーン キャリアで VPN 接続用のマルチ プロトコル BGP を設定します。

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するには、次の作業を実行します。

- CSC-PE の設定
- CSC-CE の設定

図 6 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 6　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 の設定

CSC-PE を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **address-family vpnv4 unicast**
4. **neighbor** *A.B.C.D*
5. **remote-as** *as-number*
6. **update-source** *type interface-path-id*
7. **address-family vpnv4 unicast**
8. **vrf** *vrf-name*
9. **rd** {*as-number:nn* | *ip-address:nn* | **auto**}
10. **address-family ipv4 unicast**
11. **allocate-label all**
12. **neighbor** *A.B.C.D*
13. **remote-as** *as-number*
14. **address-family ipv4 labeled-unicast**
15. **route-policy** *route-policy-name* **in**
16. **route-policy** *route-policy-name* **out**
17. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**router bgp** *as-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# router bgp 2`
	`RP/0/RSP0/CPU0:router(config-bgp)#`
		BGP ルーティング プロセスを設定し、ルータ設定モードを開始します。
		• 2 バイトの番号の範囲は 1 ～ 65535 です。4 バイトの番号の範囲は 1.0 ～ 65535.65535 です。

ステップ 3	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)#`
	`address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-af)#`
		VPNv4 アドレス ファミリを設定します。

ステップ 4	**neighbor** *A.B.C.D*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 10.10.10.0`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
		BGP ネイバーの IP アドレスを設定します。

ステップ 5	**remote-as** *as-number*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
	`remote-as 888`
		BGP ネイバーの AS 番号を設定します。

ステップ 6	**update-source** *type interface-path-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
	`update-source loopback0`
		BGP セッションが、特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。

ステップ 7	**address-family vpnv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)#`
	`address-family vpnv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		VPNv4 ユニ キャスト アドレス ファミリを設定します。

ステップ 8	**vrf** *vrf-name*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# vrf 9999`
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)#`
		VRF インスタンスを設定します。

	コマンドまたはアクション	目的
ステップ 9	**rd** {*as-number:nn* | *ip-address:nn* | **auto**} **例：** `RP/0/RSP0/CPU0:router(onfig-bgp-vrf)# rd auto`	ルート識別子を設定します。 **（注）** 一意のルート識別子を自動的に割り当てるには、**auto** キーワードを使用します。

ステップ 10	**address-family ipv4 unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-af)#`
		IPv4 ユニ キャスト アドレス ファミリを設定します。

ステップ 11	**allocate-label all** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# allocate-label all`	すべてのローカル プレフィクスおよびラベルとともに受信されたプレフィクスにラベルを割り当てます。

ステップ 12	**neighbor** *A.B.C.D*
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# neighbor 10.10.10.0`
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)#`
		BGP ネイバーの IP アドレスを設定します。

ステップ 13	**remote-as** *as-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# remote-as 888`	ネイバー BGP ルータとの情報交換をイネーブルにします。

ステップ 14	**address-family ipv4 labeled-unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# address-family ipv4 labeled-unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)#`
		IPv4 ラベル付きユニキャストアドレス ファミリを設定します。

ステップ 15	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy pass-all in`	すべてのインバウンド ルートに pass-all ポリシーを適用します。

	コマンドまたはアクション	目的
ステップ 16	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy pass-all out`	すべてのアウトバウンド ルートに pass-all ポリシーを適用します。

ステップ 17	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(cconfig-bgp-vrf-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

CSC-CE の設定

CSC-CE を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **address-family ipv4 unicast**
4. **redistribute ospf** *instance-number*
5. **allocate-label route-policy** *route-policy-name*
6. **exit**
7. **neighbor** *A.B.C.D*
8. **remote-as** *as-number*
9. **address-family ipv4 labeled-unicast**
10. **route-policy** *route-policy-name* **in**
11. **route-policy** *route-policy-name* **out**

12. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 1`	BGP ルーティング プロセスを設定し、ルータ設定モードを開始します。 • 2 バイトの番号の範囲は 1 ～ 65535 です。4 バイトの番号の範囲は 1.0 ～ 65535.65535 です。
ステップ 3	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast`	IPv4 ユニ キャストアドレス ファミリを設定します。
ステップ 4	**redistribute ospf** *instance-number* **例：** `RP/0/RSP0/CPU0:router(config-router-af)# redistribute ospf 1`	BGP に OSPF ルートを再配布します。
ステップ 5	**allocate-label route-policy** *route-policy-name* **例：** `RP/0/RSP0/CPU0:router(config-router-af)# allocate-label route-policy internal-routes`	ルート ポリシーと一致するルートにラベルを割り当てます。これらのラベル付きルートは address-family ipv4 labeled-unicast で設定されたネイバーにアドバタイズされます。
ステップ 6	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# exit`	現在の設定モードを終了します。
ステップ 7	**neighbor** *A.B.C.D* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.0.0.1`	BGP ネイバーの IP アドレスを設定します。
ステップ 8	**remote-as** *as-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 1`	ネイバー BGP ルータとの情報交換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 9	**address-family ipv4 labeled-unicast**
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast`
	`RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#`
		IPv4 ラベル付きユニキャストアドレス ファミリを設定します。

ステップ 10	**route-policy** *route-policy-name* **in** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in`	すべてのインバウンド ルートに route-policy ポリシーを適用します。
ステップ 11	**route-policy** *route-policy-name* **out** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out`	すべてのアウトバウンド ルートに route-policy ポリシーを適用します。

ステップ 12	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ピアへのスタティック ルートの設定

Inter-AS または CSC-CE ピアへのスタティック ルートを設定するには、次の作業を実行します。

Inter-AS または CSC ピアを設定すると、BGP は、そのピアに /32 ルートのラベルを割り当て、ヌル ラベルの書き換えを実行します。ラベル付きパケットをピアに転送すると、ルータはラベル スタックからトップ ラベルを削除します。ただし、このようなインスタンスでは、BGP はピアに /32 ルートを期待します。ここでは、ピアへの /32 のルートが実際に存在することを確認します。

この作業を実行する前に、次のことに注意してください。

- BGP ピアリングに確立に /32 ルートは必要ありません。短いプレフィクス長を使用するルートも動作します。
- 短いプレフィクス長ルートは割り当てられたラベルに関連付けられていません。BGP セッションが、スタティック ルートなしでピア間に存在していても、転送は動作しません。

（注） CSC-PE にスタティック ルートを設定するには、VRF でルータを設定する必要があります（詳細手順の説明のとおり）。

手順の概要

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*
5. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router(config)# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router static** **例：** `RP/0/RSP0/CPU0:router(config)# router static`	ルータ スタティック コンフィギュレーション モードを開始します。
ステップ 3	**address-family ipv4 unicast** **例：** `RP/0/RSP0/CPU0:router(config-static)# address-family ipv4 unicast`	IPv4 アドレス ファミリをイネーブルにします。 **（注）** CSC-PE でスタティック ルートを設定するには、**address-family** の前に **vrf** コマンドを使用してまず VRF を設定する必要があります。

	コマンドまたはアクション	目的
ステップ 4	***A.B.C.D/length*** *next-hop* **例：** `RP/0/RSP0/CPU0:router(config-static-afi)# 10.10.10.10/32 10.9.9.9`	宛先ルータのアドレスを入力します（IPv4 サブネット マスクを含む）。

ステップ 5	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-static-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-static-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

MPLS レイヤ 3 VPN 設定の確認

MPLS レイヤ 3 VPN の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. **show running-config router bgp** *as-number* **vrf** *vrf-name*
2. **show running-config routes**
3. **show ospf vrf** *vrf-name* **database**
4. **show running-config router bgp** *as-number* **vrf** *vrf-name* **neighbor** *ip-address*
5. **show bgp vrf** *vrf-name* **summary**
6. **show bgp vrf** *vrf-name* **neighbors** *ip-address*
7. **show bgp vrf** *vrf-name*
8. **show route vrf** *vrf-name ip-address*
9. **show bgp vpn unicast summary**
10. **show running-config router isis**
11. **show running-config mpls**

12. **show isis adjacency**
13. **show mpls ldp forwarding**
14. **show bgp vpnv4 unicast**
    show bgp vrf *vrf-name*
15. **show bgp vrf** *vrf-name* **imported-routes**
16. **show route vrf** *vrf-name ip-address*
17. **show cef vrf** *vrf-name ip-address*
18. **show cef vrf** *vrf-name ip-address* **location** *node-id*
19. **show bgp vrf** *vrf-name ip-address*
20. **show ospf vrf** *vrf-name* **database**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running-config router bgp** *as-number* **vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router# show running-config router bgp 3 vrf vrf_A`	現在の実行コンフィギュレーションの指定された VPN ルーティングおよび転送（VRF）の内容を表示します。
ステップ 2	**show running-config routes** **例：** `RP/0/RSP0/CPU0:router# show running-config routes`	現在の実行コンフィギュレーション内の Open Shortest Path First（OSPF）ルート テーブルを表示します。
ステップ 3	**show ospf vrf** *vrf-name* **database** **例：** `RP/0/RSP0/CPU0:router# show ospf vrf vrf_A database`	指定した VRF の OSPF データベースに関連する情報のリストを表示します。
ステップ 4	**show running-config router bgp** *as-number* **vrf** *vrf-name* **neighbor** *ip-address* **例：** `RP/0/RSP0/CPU0:router# show running-config router bgp 3 vrf vrf_A neighbor 172.168.40.24`	現在の実行コンフィギュレーションのボーダー ゲートウェイ プロトコル（BGP）VRF ネイバーの内容を表示します。
ステップ 5	**show bgp vrf** *vrf-name* **summary** **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A summary`	指定した BGP VRF 接続のステータスを表示します。

	コマンドまたはアクション	目的
ステップ 6	**show bgp vrf** *vrf-name* **neighbors** *ip-address* **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A neighbors 172.168.40.24`	指定されたネイバーへの BGP VRF 接続に関する情報を表示します。
ステップ 7	**show bgp vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A`	指定した BGP VRF に関する情報を表示します。
ステップ 8	**show route vrf** *vrf-name ip-address* **例：** `RP/0/RSP0/CPU0:router# show route vrf vrf_A 10.0.0.0`	指定した VRF のルーティング情報ベース（RIB）の現在のルートを表示します。
ステップ 9	**show bgp vpn unicast summary** **例：** `RP/0/RSP0/CPU0:router# show bgp vpn unicast summary`	すべての BGP VPN ユニキャスト接続のステータスを表示します。
ステップ 10	**show running-config router isis** **例：** `RP/0/RSP0/CPU0:router# show running-config router isis`	現在の実行コンフィギュレーションの Intermediate System-to-Intermediate System（IS-IS）の内容を表示します。
ステップ 11	**show running-config mpls** **例：** `RP/0/RSP0/CPU0:router# show running-config mpls`	現在の実行コンフィギュレーションの MPLS の内容を表示します。
ステップ 12	**show isis adjacency** **例：** `RP/0/RSP0/CPU0:router# show isis adjacency`	IS-IS 隣接情報を表示します。
ステップ 13	**show mpls ldp forwarding** **例：** `RP/0/RSP0/CPU0:router# show mpls ldp forwarding`	MPLS 転送にインストールされたラベル配布プロトコル（LDP）転送状態を表示します。
ステップ 14	**show bgp vpnv4 unicast** **例：** `RP/0/RSP0/CPU0:router# show bgp vpnv4 unicast`	VPNv4 ユニキャスト アドレスの BGP ルーティング テーブルのエントリを表示します。
ステップ 15	**show bgp vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A`	VRF vrf_A の BGP ルーティング テーブルのエントリを表示します。

	コマンドまたはアクション	目的
ステップ 16	**show bgp vrf** *vrf-name* **imported-routes** **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A imported-routes`	指定された VRF インスタンスにインポートされるルートの BGP 情報を表示します。
ステップ 17	**show route vrf** *vrf-name ip-address* **例：** `RP/0/RSP0/CPU0:router# show route vrf vrf_A 10.0.0.0`	現在指定されている RIB の VRF ルートを表示します。
ステップ 18	**show cef vrf** *vrf-name ip-address* **例：** `RP/0/RSP0/CPU0:router# show cef vrf vrf_A 10.0.0.1`	指定した VRF の IPv4 シスコ エクスプレス フォワーディング（CEF）テーブルを表示します。
ステップ 19	**show cef vrf** *vrf-name ip-address* **location** *node-id* **例：** `RP/0/RSP0/CPU0:router# show cef vrf vrf_A 10.0.0.1 location 0/1/cpu0`	指定された VRF とロケーションの IPv4 CEF テーブルを表示します。
ステップ 20	**show bgp vrf** *vrf-name ip-address* **例：** `RP/0/RSP0/CPU0:router# show bgp vrf vrf_A 10.0.0.0`	VRF vrf_A の BGP ルーティング テーブルのエントリを表示します。
ステップ 21	**show ospf vrf** *vrf-name* **database** **例：** `RP/0/RSP0/CPU0:router# show ospf vrf vrf_A database`	指定した VRF の OSPF データベースに関連する情報のリストを表示します。

MPLS レイヤ 3 VPN 実装の設定例

ここでは、MPLS L3VPN 機能の設定例を紹介します。

- 「BGP を使用する MPLS VPN の設定：例」（P.VPC-81）
- 「PE ルータでの Routing Information Protocol の設定：例」（P.VPC-82）
- 「EIGRP を使用した PE ルータの設定：例」（P.VPC-82）
- 「MPLS VPN CSC の設定例」（P.VPC-83）

BGP を使用する MPLS VPN の設定：例

次に、「vrf vpn1」の BGP を使用した MPLS VPN の設定例を示します。

```
  address-family ipv4 unicast
    import route-target
      100:1
    !
    export route-target
      100:1
    !
  !
!
route-policy pass-all
  pass
end-policy
!
interface Loopback0
  ipv4 address 10.0.0.1 255.255.255.255
!
interface gigabitEthernet 0/1/0/0
  vrf vpn1
  ipv4 address 10.0.0.2 255.0.0.0
!
interface gigabitEthernet 0/1/0/1
  ipv4 address 10.0.0.1 255.0.0.0
!
router ospf 100
  area 100
    interface loopback0
    interface gigabitEthernet 0/1/0/1
  !
!
router bgp 100
  address-family vpnv4 unicast
  retain route-target route-policy policy1
  neighbor 10.0.0.3
    remote-as 100
    update-source Loopback0
    address-family vpnv4 unicast
  !
  vrf vpn1
    rd 100:1
    address-family ipv4 unicast
      redistribute connected
    !
    neighbor 10.0.0.1
      remote-as 200
      address-family ipv4 unicast
        as-override
```

```
        route-policy pass-all in
        route-policy pass-all out
      !
      advertisement-interval 5
    !
  !
!
mpls ldp
  route-id looback0
  interface gigabitEthernet 0/1/0/1
!
```

PE ルータでの Routing Information Protocol の設定：例

次に、PE ルータでの RIP の設定例を示します。

```
vrf vpn1
  address-family ipv4 unicast
    import route-target
      100:1
    !
    export route-target
      100:1
    !
  !
!
route-policy pass-all
  pass
end-policy
!

interface gigabitEthernet 0/1/0/0
  vrf vpn1
  ipv4 address 10.0.0.2 255.0.0.0
!

router rip
 vrf vpn1
  interface GigabitEthernet0/1/0/0
  !
  timers basic 30 90 90 120
  redistribute bgp 100
  default-metric 3
  route-policy pass-all in
 !
```

EIGRP を使用した PE ルータの設定：例

次に、PE ルータでの Enhanced Interior Gateway Routing Protocol（EIGRP）の設定例を示します。

```
Router eigrp 10
 vrf VRF1
  address-family ipv4
   router-id 10.1.1.2
   default-metric 100000 2000 255 1 1500
   as 62
   redistribute bgp 2000
   interface Loopback0
   !
   interface GigabitEthernet0/6/0/0
```

MPLS VPN CSC の設定例

MPLS VPN CSC の設定例は次のとおりです。

- 「バックボーン キャリア コアの設定：例」（P.VPC-83）
- 「CSC-PE ルータと CSC-CE ルータ間のリンクの設定：例」（P.VPC-83）
- 「ピアへのスタティック ルートの設定：例」（P.VPC-84）

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 コアの設定例は、次のとおりです。

- 「CSC-PE ルータの VRF の設定：例」（P.VPC-83）
- 「CSC-PE ルータと CSC-CE ルータ間のリンクの設定：例」（P.VPC-83）

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。

```
config
  vrf vpn1
   address-family ipv4 unicast
    import route-target 100:1
    export route-target 100:1
   end
```

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 の設定：例」（P.VPC-83）
- 「CSC-CE の設定：例」（P.VPC-84）

CSC-PE の設定：例

この例では、CSC-PE ルータは同じ AS 内の PE ルータ（10.1.0.2）とのピアを確立します。また、CSC-CE ルータ（10.0.0.1）とのラベル付きユニキャスト ピアリングがあります。

```
config
    router bgp 2
        address-family vpnv4 unicast
        neighbor 10.1.0.2
            remote-as 2
            update-source loopback0
            address-family vpnv4 unicast
        vrf customer-carrier
            rd 1:100
            address-family ipv4 unicast
                allocate-label all
                redistribute static
        neighbor 10.0.0.1
            remote-as 1
            address-family ipv4 labeled-unicast
                route-policy pass-all in
                route-policy pass-all out
                as-override
end
```

CSC-CE の設定：例

次に、CSC-CE ルータを設定する例を示します。この例では、CSC-CE ルータは AS 2 内の CSC-PE ルータ 10.0.0.2 とのピアを確立します。

```
config
    router bgp 1
        address-family ipv4 unicast
            redistribute ospf 200
            allocate-label all
        neighbor 10.0.0.2
            remote-as 2
            address-family ipv4 labeled-unicast
            route-policy pass-all in
            route-policy pass-all out
end
```

ピアへのスタティック ルートの設定：例

次に、Inter-AS または CSC-CE ピアへのスタティック ルートを設定する例を示します。

```
config
 router static
  address-family ipv4 unicast
  10.0.0.2/32 40.1.1.1
end
```

その他の参考資料

詳細については、次のマニュアルを参照してください。

関連資料

関連項目	ドキュメント名
Cisco ASR 9000 シリーズ ルータの L2VPN コマンド	『*Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference*』の「*MPLS Virtual Private Network Commands on Cisco ASR 9000 Series Routers*」モジュール
ルーティング（BGP、EIGRP、OSPF、RIP）コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference*』
ルーティング（BGP、EIGRP、OSPF、RIP）設定	『*Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*』
MPLS LDP の設定：設定の概念、作業、および例	このマニュアルの「*Implementing MPLS Label Distribution Protocol on Cisco ASR 9000 Series Routers*」モジュール。
MPLS トラフィック エンジニアリング リソース予約プロトコルの設定：設定の概念、作業、および例	このマニュアルの「*Implementing RSVP for MPLS-TE on Cisco ASR 9000 Series Routers*」モジュール。
スタートアップ ガイド	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』

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
—	Cisco IOS XR ソフトウェアを使用している MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC 1700	『*Assigned Numbers*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 1966	『*BGP Route Reflectors: 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
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

IPv6 VPN プロバイダー エッジ転送 over MPLS

このモジュールでは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータで IPv6 VPN プロバイダー エッジ転送 MPLS を実装する方法について説明します。

IPv6 VPN プロバイダー エッジ（6PE/VPE）は、IPv6 転送に既存の MPLS IPv4 コア インフラストラクチャを使用します。6PE/VPE を使用すると、IPv6 サイト同士が MPLS ラベル スイッチド パス（LSP）を使用して MPLS IPv4 コア ネットワークを介して互いに通信できるようになります。

この機能は、プロバイダー エッジ（PE）ルータ上の IPv4 ネットワーク設定のマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）拡張に大きく依存して、各 IPv6 アドレス プレフィクスの IPv6 到達可能性情報（および MPLS ラベル）を交換します。エッジ ルータは、IPv4 と IPv6 の両方を実行するデュアルスタックとして設定され、IPv4 マッピング IPv6 アドレスを使用して IPv6 プレフィクスの到達可能性情報を交換します。

L2TP 機能を設定するために使用するコマンドの詳細については、
「*Cisco ASR 9000 Aggregation Services Router Routing Command Reference*」を参照してください。

6PE の実装の機能履歴：Cisco ASR 9000 シリーズ ルータ

リリース	変更箇所
リリース 3.9.1	この機能が導入されました。
リリース 4.0.0	A9K-SIP-700 の IPv6 L3VPN に対する 6PE および 6VPE 機能のサポートが追加されました。 6PE 機能での BGP の VRF/CE ごとのラベル割り当てのサポートが追加されました。
リリース 4.1.0	Open Shortest Path First バージョン 3（OSPFv3）IPv6 VPN プロバイダー エッジ（6VPE）機能のサポートが追加されました。

内容

- 「6PE/VPE 設定の前提条件」（P.VPC-88）
- 「6PE/VPE に関する情報」（P.VPC-88）
- 「6PE/VPE の実装方法」（P.VPC-91）
- 「6PE の設定例」（P.VPC-104）
- 「その他の参考資料」（P.VPC-106）

6PE/VPE 設定の前提条件

6PE を実装するには、次の前提条件を満たす必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。

  ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- MPLS および BGP4 設定およびトラブルシューティングについての知識。

6PE/VPE に関する情報

6PE 機能を設定するには、ここで説明する概念を理解する必要があります。

- 「6PE/VPE の概要」（P.VPC-88）
- 「6PE/VPE の利点」（P.VPC-89）
- 「IPv6 over MPLS バックボーンの導入」（P.VPC-89）
- 「プロバイダー エッジ ルータおよびカスタマー エッジ ルータ上の IPv6」（P.VPC-89）
- 「IPv6 プロバイダー エッジ マルチ パス」（P.VPC-90）
- 「OSPFv3 6VPE」（P.VPC-90）

6PE/VPE の概要

さまざまな手法を使用して、サービス プロバイダーのコア バックボーン上で IPv6 サービスを統合できます。

- さまざまなデータリンク層で動作する IPv6 専用ネットワーク
- デュアルスタック IPv4-IPv6 バックボーン
- 既存の MPLS バックボーンの活用

これらのソリューションは、IPv6 トラフィックトラフィックの量と生みだされる収益が、必要な投資と合意済みのリスクと一致する場合に、サービス プロバイダーのバックボーンに導入されます。条件は、エッジからスケーラブルな方法でネイティブ IPv6 サービスを導入する場合に都合が良く、IPv6 アドレッシングの制限はなく、適切に制御された IPv4 バックボーンを危険にさらすこともありません。バックボーンの安定性は、最近 IPv4 インフラストラクチャを安定化させたばかりのサービス プロバイダーに必須です。

MPLS ネットワークで IPv6 サービスを提供統合シナリオは複数考えられるため、MPLS/IPv4 インフラストラクチャを実行する複数のサービス プロバイダーは同様の傾向に従います。シスコ システムズは、これらすべての要件を満たすために特別に 6PE または IPv6 プロバイダー エッジ ルータ over MPLS を開発しました。

6PE の Inter-AS サポートでは、アドレス ファミリをイネーブルにし、PE および ASBR ラベルを割り当て、配布できるようにするため、ボーダー ゲートウェイ プロトコル（BGP）のサポートが必要です。

6PE/VPE の利点

現在 MPLS を導入しているサービス プロバイダーには、次の Cisco 6PE の利点を経験します。

- 最小限の運用コストとリスク：既存の IPv4 および MPLS サービスに影響はありません。
- プロバイダー エッジ ルータのアップグレードのみ：6PE/VPE ルータには、既存の PE ルータまたは新規の IPv6 トラフィック専用のものが使用できます。
- IPv6 カスタマー エッジ ルータに影響なし：ISP は、スタティック、IGP または EGP を実行しているすべてのカスタマー CE に接続できます。
- 生産サービス レディ：ISP は IPv6 プレフィクスを委任できます。
- 既存の MPLS サービスへの IPv6 導入：6PE/VPE ルータはいつでも追加できます。

IPv6 over MPLS バックボーンの導入

6PE（IPv6 over MPLS）によってイネーブルにされたバックボーンを使用すると、IPv6 ドメイン同士が MPLS IPv4 コア ネットワークを介して互いに通信できるようになります。この実装では、転送は IP ヘッダー自体ではなくラベルに基づいているため、コア ルータのバックボーン インフラストラクチャのアップグレードおよび再設定も必要ありません。これは、IPv6 導入に非常に費用効果の高い方法を提供します。

また、MPLS 環境で本来提供されているバーチャル プライベート ネットワーク（VPN）サービスおよびトラフィック エンジニアリング（TE）サービスを使用して、IPv4 VPN および MPLS-TE をサポートするインフラストラクチャを介して IPv6 ネットワークを VPN やエクストラネットに組み込むことができます。

プロバイダー エッジ ルータおよびカスタマー エッジ ルータ上の IPv6

サービス プロバイダー エッジ ルータ

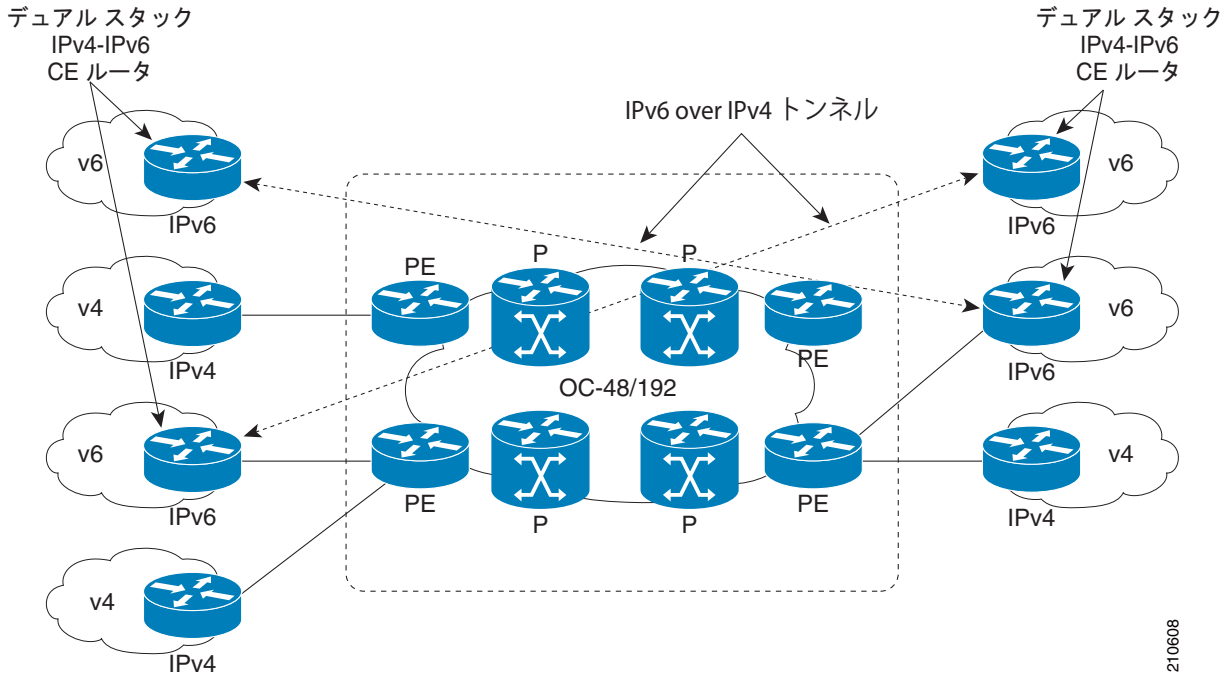
6PE は特に現在 MPLS ネットワークを実行するサービス プロバイダーに適用されます。利点の 1 つとして、コア ネットワークのハードウェア、ソフトウェア、または設定をアップグレードする必要がなく、動作および既存の IPv4 トラフィックによって生みだされる収益に影響がありません。多くのサービス プロバイダーが MPLS を使用して顧客にサービスを提供しています。マルチサービス インフラストラクチャのテクノロジーとしての MPLS は、レイヤ 3 VPN、QoS、トラフィック エンジニアリング、高速リルート、ATM の統合、および IP スイッチングを提供できます。

カスタマー エッジ ルータ

MPLS ネットワークに IPv6 を導入する最も簡単な方法は、CE ルータ上でトンネルを使用することです。これは、MPLS の動作またはインフラストラクチャに影響がなく、コア内の P ルータまたは PE ルータを変更する必要はありません。ただし接続する CE の数の増加に伴い、ISP のグローバル IPv6 プレフィクスの委任が困難になると、トンネル メッシュが必要です。

図 7 に、CE ルータ上のトンネルを使用したネットワーク アーキテクチャを示します。

図 7　CE ルータ上でトンネルを使用した IPv6



IPv6 プロバイダー エッジ マルチ パス

IPv6 の内部および外部 BGP マルチパスによって、IPv6 ルータは、宛先に到達するために複数のパス（同じ隣接自律システム（AS）や Sub-AS、または同じメトリックなど）間のロード バランシングを行うことができます。6PE マルチパス機能では、マルチプロトコル内部 BGP（MP-iBGP）を使用して、MPLS IPv4 コア ネットワークを介して IPv6 ルートを配布し、MPLS ラベルを各ルートに付加します。

MP-IBGP マルチパスが 6PE ルータでイネーブルになっていると、MPLS 情報（ラベル スタック）を使用して、ラベルの付いたすべてのパスが、転送テーブルにインストールされます。この機能によって、6PE はロード バランシングを実行できます。

OSPFv3 6VPE

Open Shortest Path First バージョン 3（OSPFv3）IPv6 VPN プロバイダー エッジ（6VPE）機能は、Cisco IOS XR OSPFv3 実装に VPN ルーティングおよび転送（VRF）およびプロバイダー エッジからカスタマー エッジ（PE-CE）へのルーティングのサポートを追加します。この機能により次の内容が可能になります。

- OSPFv3 ルーティング プロセスごとに複数の VRF サポート
- OSPFV3 PE-CE 拡張

複数の VRF のサポート

OSPFv3 は複数の VRF を単一のルーティング プロセスでサポートしており、ルート プロセッサ（RP）リソースをあまり消費せずに VRF を数十～数百のに拡張できます。

複数の OSPFv3 プロセスが、単一のルータで設定できます。大規模な VRF の導入では、これにより複数の RP をまたいでパーティション VRF 処理が可能になります。また、これはデフォルト ルーティング テーブルまたは影響の大きい VRF を通常の VRF から隔離するためにも使用されます。すべての VRF に単一プロセスを使用することを推奨します。必要に応じて、2 番目の OSPFv3 プロセスを、IPv6 ルーティング用に設定する必要があります。

（注） 最大 4 個の OSPFv3 プロセスがサポートされます。

OSPFv3 PE-CE 拡張

IPv6 プロトコルは、今日のカスタマー ネットワークで大きく導入されつつあります。サービス プロバイダー（SP）は、IPv4 プロトコルですでに提供されている VPN サービスに加えて、IPv6 プロトコルをサポートするために顧客にバーチャル プライベート ネットワーク サービスを提供することが可能である必要があります。

IPv6 をサポートするには、ルーティング プロトコルが VPN 環境での動作するために、追加拡張が必要です。OSPFv3 が PE-CE リンクで動作するためには、OSPFv3 への拡張が必要です。

VRF Lite

VRF-Lite 機能は、BGP または MPLS ベースのバックボーンなしの VRF の実装を可能にします。VRF-Lite では、PE ルータは VRF インターフェイスを使用して直接接続されます。OSPFv3 に場合、BGP または MPLS バックボーンを使用した導入とは反対に、VRF-Lite のシナリオで次の内容が異なる動作をする必要があります。

- DN ビット処理：VRF-Lite 環境では、DN ビット処理はディセーブルです。
- ABR のステータス：VRF コンテキスト（デフォルト VRF を除く）では、エリア 0 への接続性に関係なく、OSPFv3 ルータは自動的に ABR として設定されます。VRF-Lite 環境では、この自動 ABR のステータス設定がディセーブルです。

（注） VRF-Lite をイネーブルにするには、OSPFv3 VRF コンフィギュレーション サブモードで **capability vrf-lite** コマンドを発行します。

6PE/VPE の実装方法

ここでは、次の実装手順について説明します。

- 「6PE/VPE の設定」（P.VPC-91）
- 「PE から PE コアの設定」（P.VPC-93）
- 「CE から PE コアの設定」（P.VPC-97）
- 「OSPFv3 を PE ルータと CE ルータ間のルーティング プロトコルに設定」（P.VPC-100）

6PE/VPE の設定

ここでは、IPv4 クラウドを介して IPv6 プレフィクスを転送するように PE ルータの 6PE/VPE を設定する方法について説明します。

6PE/VPE を設定する PE ルータが IPv4 クラウドおよび IPv6 クラウドの両方に参加していることを確認します。

（注） 6PE の場合、両方のクラウドからのルートの学習には、BGP、OSPF、IS-IS、EIGRP、RIP、スタティックなどの Cisco IOS XR ソフトウェアでサポートされているすべてのルーティング プロトコルを使用できます。ただし、6VPE の場合、ルートの学習には BGP、EIGRP、およびスタティック ルーティング プロトコルだけを使用できます。

手順の概要

1. **configure**
2. **router bgp** *as-number*
3. **neighbor** *ip-address*
4. **address-family ipv6 labeled-unicast**
5. **exit**
6. **exit**
7. **address-family ipv6 unicast**
8. **allocate-label** [**all** | **route-policy** *policy_name*]
9. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 1`	ルータが存在する自律システム（AS）を識別する番号を入力します。 2 バイトの番号の範囲は 1 ～ 65535 です。4 バイトの番号の範囲は 1.0 ～ 65535.65535 です。
ステップ 3	**neighbor** *ip-address* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# neighbor 1.1.1.1`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング セッションを設定するネイバー設定モードを開始します。
ステップ 4	**address-family ipv6 labeled-unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv6 labeled-unicast`	IPv6 ラベル付きユニキャスト アドレス プレフィクスを指定します。 **（注）** このオプションは、IPv6 ネイバー設定モード、および VRF ネイバー設定モードでも使用できます。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# exit`	BGP アドレス ファミリ サブモードを終了します。
ステップ 6	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# exit`	BGP ネイバー サブモードを終了します。
ステップ 7	**address-family ipv6 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv6 unicast`	IPv6 ユニキャスト アドレス プレフィクスを指定します。
ステップ 8	**allocate-label** [**all** | **route-policy** *policy_name*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# allocate-label all`	指定された IPv4 ユニキャスト ルートの MPLS ラベルを割り当てます。 **（注）** **route-policy** キーワードを使用すると、ネイバーにアドバタイズされる特定のルートのフィルタリングをより細かく制御できます。

ステップ 9	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

PE から PE コアの設定

ここでは、プロバイダー エッジ（PE）から PE コアを設定する方法について説明します。

VPN ルーティングおよび転送（VRF）の設定についての詳細は、『*Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*』の「*Implementing BGP on Cisco ASR 9000 Series Router*」モジュールを参照してください。

手順の概要

1. **configure**
2. **router bgp**
3. **address-family vpnv6 unicast**
4. **bgp dampening** [*half-life* [*reuse suppress max-suppress-time*] | **route-policy** *route-policy-name*]
5. **bgp client-to-client reflection** { **cluster-id** | **disable** }
6. **neighbor** *ip-address*
7. **remote-as** *as-number*
8. **description** *text*
9. **password** { **clear** | **encrypted** } *password*
10. **shutdown**
11. **timers** *keepalive hold-time*
12. **update-source type** *interface-id*
13. **address-family vpnv6 unicast**
14. **route-policy** *route-policy-name* { **in** | **out** }
15. **exit**
16. **vrf** *vrf-name*
17. **rd** { *as-number : nn* | *ip-address : nn* | **auto** }
18. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 10`	BGP AS 番号を指定し、BGP 設定モードを開始して、BGP ルーティング プロセスを設定できるようにします。
ステップ 3	**address-family vpnv6 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv6 unicast`	vpnv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**bgp dampening** [*half-life* [*reuse suppress max-suppress-time*] | **route-policy** *route-policy-name*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# bgp dampening 30 1500 10000 120`	指定されたアドレス ファミリの BGP ダンプニングを設定します。
ステップ 5	**bgp client-to-client reflection** {**cluster-id | disable** } **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# bgp client-to-client reflection disable`	クライアント間のルート リフレクションを設定します。
ステップ 6	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-af)# exit`	アドレス ファミリ コンフィギュレーション サブモードを終了します。
ステップ 7	**neighbor** *ip-address* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.1.1.1`	BGP ルーティングのためにルータをネイバー コンフィギュレーション モードにして、ネイバーの IP アドレスを BGP ピアとして設定します。
ステップ 8	**remote-as** *as-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100`	ネイバーを作成し、リモート自律システム番号をそのネイバーに割り当てます。
ステップ 9	**description** *text* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# description neighbor 172.16.1.1`	ネイバーの説明を提供します。description は、コメントを保存するために使用されます。ソフトウェアの機能には影響しません。
ステップ 10	**password** { **clear** | **encrypted** } *password* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# password encrypted 123abc`	2 つの BGP ネイバーの間の TCP 接続上で Message Digest 5（MD5）認証をイネーブルにします。
ステップ 11	**shutdown** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# router bgp 1`	指定されたネイバーのあらゆるアクティブ セッションを終了し、すべての関連するルーティング情報を削除します。
ステップ 12	**timers** *keepalive hold-time* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# timers 12000 200`	BGP ネイバーのタイマーを設定します。

	コマンドまたはアクション	目的
ステップ 13	**update-source type** *interface-id* **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source gigabitEthernet 0/1/5/0`	ネイバーとの iBGP セッションを形成するときに、iBGP セッションが特定のインターフェイスのプライマリ IP アドレスをローカル アドレスとして使用できるようにします。
ステップ 14	**address-family vpnv6 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpvn6 unicast`	VPN ネイバー アドレス ファミリ設定モードを開始します。
ステップ 15	**route-policy** *route-policy-name* { **in** | **out** } **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pe-pe-vpn-in in`	インバウンド ルートのルーティング ポリシーを指定します。ポリシーを使用すると、ルートのフィルタリングやルート属性の変更ができます。
ステップ 16	**route-policy** *route-policy-name* { **in** | **out** } **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pe-pe-vpn-out out`	アウトバウンド ルートのルーティング ポリシーを指定します。ポリシーを使用すると、ルートのフィルタリングやルート属性の変更ができます。
ステップ 17	**exit** **例：** `RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# exit`	アドレス ファミリ設定およびネイバー サブモードを終了します。
ステップ 18	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf-pe`	VRF インスタンスを設定します。

	コマンドまたはアクション	目的
ステップ 19	**rd** { *as-number : nn* | *ip-address : nn* | **auto** } **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd 345:567`	ルート識別子を設定します。 ルータが自動的に VRF に一意の RD を割り当てるようにする場合は、auto キーワードを使用します。

ステップ 20	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-vrf)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

CE から PE コアの設定

ここでは、PE からカスタマー エッジ（CE）コアを設定する方法について説明します。

手順の概要

1. **configure**
2. **router bgp**
3. **vrf** ***vrf-name***
4. **bgp router-id** *ip-address*
5. **label-allocation-mode** { **per-ce** | **per-vrf** }
6. **address-family ipv6 unicast**
7. **redistribute** {**connected** | **static** | **eigrp** }
8. **neighbor** ***ip-address***
9. **remote-as** ***as-number***
10. **ebgp-multihop** { *maximum hops* | **mpls** }
11. **address-family ipv6 unicast**

12. **site-of-origin** [*as-number : nn* | *ip-address : nn*]
13. **as-override**
14. **allowas-in** [*as-occurrence-number*]
15. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* **例：** `RP/0/RSP0/CPU0:router(config)# router bgp 10`	BGP AS 番号を指定し、BGP 設定モードを開始して、BGP ルーティング プロセスを設定できるようにします。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf-pe`	VRF インスタンスを設定します。
ステップ 4	**bgp router-id** *ip-address* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)#bgp router-id 172.16.9.9`	BGP スピーキング ルータの固定ルータ ID を設定します。
ステップ 5	**label-allocation-mode { per-ce | per-vrf }** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# label-allocation-mode per-ce`	CE ごとのラベル割り当てモードを設定して PE ルータでの追加ルックアップを回避し、ラベル スペースを節約します(デフォルトのラベル割り当てモードはプレフィクス単位)。このモードでは、PE ルータは、すべての即時ネクスト ホップ（ほとんどの場合、これは CE ルータ）に 1 個のラベルを割り当てます。このラベルは直接、ネクスト ホップにマップされるため、データ転送中に VRF ルート ルックアップが実行されることはありません。ただし、割り当てられるラベルの数は、各 VRF に 1 つではなく、各 CE に 1 個です。BGP はすべてのネクスト ホップを認識するため、各ネクスト ホップにラベルを割り当てます（各 PE-CE インターフェイスではありません)。発信インターフェイスがマルチアクセス インターフェイスで、ネイバーのメディア アクセス コントロール（MAC）アドレスが不明な場合は、アドレス解決プロトコル（ARP）がパケット転送の間にトリガーされます。 per-vrf キーワードは同じラベルを一意の VRF からアドバタイズされたすべてのルートに使用するように設定します。

	コマンドまたはアクション	目的
ステップ 6	**address-family ipv6 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv6 unicast`	IPv6 アドレス ファミリ ユニキャストを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。 このコマンドで可能なすべてのキーワードおよび引数のリストを表示するには、CLI ヘルプ（?）を使用します。
ステップ 7	**redistribute {connected | static | eigrp }** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-af)#`	指定したインスタンスからのルートが BGP に再配布されるようにします。
ステップ 8	**neighbor** *ip-address* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf)# neighbor 10.0.0.0`	CE ネイバーを設定します。ip-address 引数は、プライベート アドレスである必要があります。
ステップ 9	**remote-as** *as-number* **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# remote-as 2`	CE ネイバーのリモート AS を設定します。
ステップ 10	**ebgp-multihop {** *maximum hops* **| mpls }** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# ebgp-multihop 55`	CE ネイバーが直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れ、試行するように設定します。
ステップ 11	**address-family ipv6 unicast** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# address-family ipv6 unicast`	IPv6 アドレス ファミリ ユニキャストを指定し、アドレス ファミリ コンフィギュレーション サブモードを開始します。 このコマンドで可能なすべてのキーワードおよび引数のリストを表示するには、CLI ヘルプ（?）を使用します。
ステップ 12	**site-of-origin** [*as-number:nn* | *ip-address:nn*] **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# site-of-origin 234:111`	Site of Origin（SoO）拡張コミュニティを設定します。この CE のネイバーから学習したルートは PE の他の部分へアドバタイズされる前に SoO 拡張コミュニティでタグ付けされます。as-override が PE ルータ上で設定されている場合、ループの検出には SoO が頻繁に使用されます。プレフィクスが同じサイトにループ バックする場合、PE はこれを検出し、CE に更新を送信しません。
ステップ 13	**as-override** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# as-override`	PE ルータの AS のオーバーライドを設定します。これにより、PE ルータは CE の ASN と自分（PE）の ASN を置き換えます。 **（注）** 情報が損失は、ルーティング ループが発生する可能性があります。as-override によるループを回避するには、site-of-origin とともに使用します。

	コマンドまたはアクション	目的
ステップ 14	**allowas-in [** *as-occurrence-number* **]** **例：** `RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# allowas-in 5`	AS パスに対し、PE の自律システム番号（ASN）を指定された回数だけ許可します。 ハブ & スポーク VPN ネットワークは、HUB CE を通じて、HUB PE へのルーティング情報のループ バックを必要とします。この場合、PE ASN が存在しているため、ループバックされた情報は HUB PE によってドロップされます。これを回避するには、PE ASN があっても、指定回数までプレフィクスを許可する allowas-in コマンドを使用します。

ステップ 15	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# end`
	または
	`RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

OSPFv3 を PE ルータと CE ルータ間のルーティング プロトコルに設定

プロバイダー エッジ（PE）からカスタマー エッジ（CE）へ Open Shortest Path First バージョン 3（OSPFv3）を使用するルーティング 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. **configure**
2. **router ospfv3** *process-name*
3. **vrf** *vrf-name*
4. **capability vrf-lite**
5. **router-id** {*router-id* | *type interface-path-id*}
6. **domain-id type** {**0005** | **0105** | **0205** | **8005**} **value** *domain-id*

7. **redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または
   redistribute connected [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または
   redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または
   redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または
   redistribute eigrp *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   または
   redistribute rip [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
8. **area** *area-id*
9. **interface** *type interface-path-id*
10. **end**
    または
    commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-name* **例：** `RP/0/RSP0/CPU0:router(config)# router ospf 109`	OSPF 設定モードを開始します。このモードでは、OSPF ルーティング プロセスの設定を行えます。
ステップ 3	**vrf** *vrf-name* **例：** `RP/0/RSP0/CPU0:router(config-ospf)# vrf vrf_1`	VPN ルーティングおよび転送（VRF）インスタンスを設定し、OSPF ルーティングの VRF 設定モードを開始します。
ステップ 4	**capability vrf-lite** **例：** `RP/0/RSP0/CPU0:router(config-ospf-vrf)# capability vrf-lite`	VRF 機能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	**router-id** {*router-id* | type interface-path-id} **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf)# router-id 172.20.10.10	VRF のルータ ID を設定します。 **（注）** VRF 単位でルータ ID の設定が必要です。
ステップ 6	**domain-id type** {0005 | 0105 | 0205 | 8005} value domain-id **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf)# domain-id type 0005 value CAFE00112233	ドメイン ID を指定します。
ステップ 7	**redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute connected** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute static** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute eigrp** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}][**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] または **redistribute rip** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*] **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf)# redistribute connected	ルートが OSPF に再配布されるようにします。OSPF に再配布できるルートは次のとおりです。 • ボーダー ゲートウェイ プロトコル（BGP） • 接続 • Enhanced Interior Gateway Routing Protocol（EIGRP） • OSPF • スタティック • Routing Information Protocol（RIP; ルーティング情報プロトコル）
ステップ 8	**area** *area-id* **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 0	OSPF エリアをエリア 0 として設定します。

	コマンドまたはアクション	目的
ステップ 9	**interface** type interface-path-id **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf-ar)# interface GigabitEthernet 0/3/0/0	インターフェイス GigabitEthernet 0/3/0/0 をエリア 0 に関連付けます。
ステップ 10	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-ospf-vrf-ar-if)# end または RP/0/RSP0/CPU0:router(config-ospf-vrf-ar-if)# commit	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

6PE の設定例

ここでは、次の設定例について説明します。

- 「PE ルータでの 6PE の設定：例」（P.VPC-104）
- 「PE ルータでの 6VPE の設定：例」（P.VPC-104）

PE ルータでの 6PE の設定：例

この設定例では、PE ルータでの 6PE の設定を示します。

```
interface GigabitEthernet0/3/0/0
 ipv6 address 2001::1/64
!
router isis ipv6-cloud
 net 49.0000.0000.0001.00
 address-family ipv6 unicast
  single-topology
 interface GigabitEthernet0/3/0/0
  address-family ipv6 unicast
  !
!
router bgp 55400
 bgp router-id 54.6.1.1
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
  network 55:5::/64
  redistribute connected
  redistribute isis ipv6-cloud
   allocate-label all

 !
 neighbor 34.4.3.3
  remote-as 55400
  address-family ipv4 unicast
  !
  address-family ipv6 labeled-unicast
```

PE ルータでの 6VPE の設定：例

この設定例では、PE ルータでの 6VPE の設定を示します。

```
vrf vpn1
 address-family ipv6 unicast
  import route-target
   200:2
  !
  export route-target
   200:2

interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255

interface GigabitEthernet0/0/0/1
 vrf  vpn1
 ipv6 address 2001:c003:a::2/64
```

```
router bgp 1
 bgp router-id 10.0.0.1
 bgp redistribute-internal
 bgp graceful-restart
 address-family ipv4 unicast
!

address-family vpnv6 unicast
 !
 neighbor 10.0.0.2                >>>> Remote peer loopback address.
  remote-as 1
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv6 unicast
   route-policy pass-all in
   route-policy pass-all out
 !

  vrf vpn1
   rd 100:2
   bgp router-id 140.140.140.140
   address-family ipv6 unicast
   redistribute connected
 !

 neighbor 2001:c003:a::1
   remote-as 6502
   address-family ipv6 unicast
   route-policy pass-all in
   route-policy pass-all out
 !
```

PE から CE 間の OSPFv3 の設定 : 例

次に、プロバイダー エッジ（PE）からカスタマー エッジ（CE）へ Open Shortest Path First バージョン 3（OSPFv3）を使用するルーティング セッションを設定するに例を示します。

```
router ospfv3 0
 vrf V1
  router-id 100.0.0.2
  domain-id type 0005 value CAFE00112233
  domain-id secondary type 0105 value beef00000001
  domain-id secondary type 0205 value beef00000002
  capability vrf-lite
  redistribute bgp 1
  area 0
   interface POS0/3/0/1
 vrf V2
  router-id 200.0.0.2
  capability vrf-lite
  area 1
   interface POS0/3/0/2
```

その他の参考資料

この機能に関する詳細については、次の資料を参照してください。

関連資料

関連項目	ドキュメント名
スタートアップ ガイド	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』

標準

標準[1]	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。	—

1. サポートされている規格がすべて記載されているわけではありません。

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用している MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
—	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

INDEX

HC	Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide
IC	Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide
MCC	Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide
MNC	Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide
MPC	Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide
QC	Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration Guide
RC	Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide
SC	Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide
SMC	Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide
LSC	Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide

数字

6PE/VPE
- BGP マルチパス **VPC-90**
- 概要 **VPC-88**
- サービス プロバイダーの考慮事項 **VPC-88**
- サポートされるプロトコル **VPC-92**
- 使用の条件 **VPC-88**
- 設定方法 **VPC-91**
- 前提条件 **VPC-88**
- 導入方法 **VPC-89**

B

BGP
- 連合 **VPC-17**

BGP4 設定 **VPC-88**

BGP（ボーダー ゲートウェイ プロトコル）
- メッセージおよび MPLS ラベル **VPC-20**
- ルーティング情報 **VPC-20**
- ルートの配布 **VPC-21**

BGP マルチパス
- 6PE/VPE **VPC-90**

C

CSC（Carrier Supporting Carrier）
- CSC-PE リンクの設定 **VPC-69**
- カスタマー キャリア ネットワークのオプション **VPC-23**
- 設定例 **VPC-76**
- トポロジの識別 **VPC-68**
- バックボーン キャリアとカスタマー キャリアの設定オプション **VPC-22**
- ピアへのスタティック ルートの設定 **VPC-76**

CSC-CE リンク、設定方法 **VPC-73**

CSC-PE リンク、設定方法 **VPC-69**

E

eBGP **VPC-10**

I

Inter-AS 設定
- BGP **VPC-17**
- サポート対象 **VPC-17**
- プロバイダー間 VPN **VPC-17**

IP 接続の確認、CSC
- MPLS レイヤ 3 VPN **VPC-69**

M

MPLS VPN
- Inter-AS ASBR VPC-16
- 主要コンポーネント VPC-15

MPLS レイヤ 3 VPN
- FIB VPC-10
- MPLS 転送 VPC-14
- PE ルータ VPC-12
- VPN ルーティング情報 VPC-14
- 概念 VPC-11
- カスタマー エッジ ルータ VPC-12
- カスタマー ルータ VPC-12
- コンポーネント VPC-12
- 作業 VPC-13
- 自動ルート識別子 VPC-15
- 主要コンポーネント VPC-15
- 自律システム VPC-16
- スケーラビリティ VPC-12
- 制約事項 VPC-10
- セキュリティ VPC-12
- 設定 VPC-11
- 前提条件 VPC-10
- 定義 VPC-11
- 定義済み VPC-11
- トポロジ VPC-12
- 配布するルーティング情報 VPC-13
- プロバイダー ルータ VPC-12

P

PE ルータ
- MPLS レイヤ 3 VPN VPC-12

V

VRF（仮想ルーティングおよび転送）
- バックボーン キャリア コアの設定 VPC-69

か

カスタマー エッジ ルータ
- 6PE/VPE VPC-89
- MPLS レイヤ 3 VPN VPC-12

カスタマー エッジ ルータ（CE）
- MPLS レイヤ 3 VPN VPC-12

さ

サービス プロバイダー、6PE VPC-88
サービス プロバイダーのエッジ ルータ、6PE VPC-89

し

自動ルート識別子、MPLS レイヤ 3 VPN VPC-15
自律システム VPC-16

す

スタティック
- ルータからピアへ、設定方法 VPC-76

と

トンネル タイプ
- 6PE VPC-89

ふ

プロバイダー間 VPN、MPLS VPN VPC-17