



CHAPTER 5

MPLS VPN サービスの管理

この章では、Cisco Prime Provisioning 6.3、マルチプロトコル ラベル スイッチング (MPLS)、パーティシャル プライベート ネットワーク (VPN) の使用を開始するために必要なタスクについて説明します。



(注)

この項では、MPLS VPN の使用を開始するために必要な、重要なタスクの一部を概説します。基本的な Prime Provisioning サービスの設定の詳細については、「[Prime Provisioning サービスの設定](#)」(P.5-4) を参照してください。



(注)

Prime Network Vision で、マップのエンドポイントを選択してサービスを作成できます。MPLS VPN の場合、「no CE」オプション (CE デバイスが存在しない) のみが Prime Provisioning でサポートされています。

- 1) いずれかのマップで、<Ctrl> クリックを使用して 1 つ以上のエンドポイント デバイスを選択します。
- 2) 右クリック メニューで、[Fulfill/Create Service] サービスを選択します。Prime Provisioning でサービスを作成するときに最初に表示されるものと同じ画面が表示されます。
- 3) ポリシーを選択します。選択したエンドポイントの数によっては、一部のポリシーが機能しない場合があります。たとえば、5 個のエンドポイントを選択した場合、ポイントツーポイント サービスを作成することはできませんが、VPLS または L3 VPN は作成できます。
- 4) ポリシーを選択すると、[Service Request] ページがリンクとともに、また、選択されたデバイスが事前に読み込まれた状態で表示されます。

この章は、次の内容で構成されています。

- 「[MPLS VPN の概要](#)」 (P.5-2)
- 「[Prime Provisioning サービスの設定](#)」 (P.5-4)
- 「[独立 VRF 管理](#)」 (P.5-15)
- 「[MPLS VPN での IPv6 および 6VPE サポート](#)」 (P.5-32)
- 「[MPLS VPN サービス ポリシー](#)」 (P.5-42)
- 「[MPLS VPN サービス要求](#)」 (P.5-83)
- 「[標準 PE-CE リンクのプロビジョニング](#)」 (P.5-104)
- 「[マルチ VRFCE PE-CE リンクのプロビジョニング](#)」 (P.5-115)
- 「[プロビジョニング管理 VPN](#)」 (P.5-126)
- 「[ケーブル サービスのプロビジョニング](#)」 (P.5-136)

- 「Carrier Supporting Carrier のプロビジョニング」 (P.5-146)
- 「複数のデバイスのプロビジョニング」 (P.5-150)
- 「複数の自律システムのスパニング」 (P.5-161)
- 「サンプル コンフィグレット」 (P.5-172)
- 「MPLS VPN のトラブルシューティング」 (P.5-253)
- 「VRF」 (P.5-262)

MPLS VPN の概要

具体的な内容は、次のとおりです。

- 「はじめる前に」 (P.5-2)
- 「Prime Provisioning サービスのアクティブ化」 (P.5-2)
- 「MPLS ポリシーとサービス要求の操作」 (P.5-3)

はじめる前に

MPLS VPN を使用してプロビジョニングを行うには、次の手順を実行する必要があります。

-
- ステップ 1** Prime Provisioning をインストールします。『[Cisco Prime Provisioning 6.3 Installation Guide](#)』を参照してください。
 - ステップ 2** ライセンスを購入します。
 - ステップ 3** ネットワークを評価します。
たとえば、ネットワークは MPLS、MP-BGP 対応、サポートされるプラットフォーム上の PE ルータであることなどの特定の基準を満たす必要があります。Prime Provisioning は、特定のネットワーク内のデバイスではなく、PE-CE のみをプロビジョニングします。
 - ステップ 4** Prime Provisioning にデータを取り込みます。
-

Prime Provisioning サービスのアクティブ化

MPLS サービスをアクティブにするには、Prime Provisioning が管理するデバイス、プロバイダー、カスタマーなどの事前設定情報とそれらの役割を「認識」できるように Prime Provisioning を設定する必要があります。Prime Provisioning サービスをアクティブ化するための主な手順として、次の設定があります。

- デバイス
- プロバイダーの情報 (プロバイダー、リージョン、および PE)
- 顧客情報 (カスタマー、サイト、および CPE)
- リソース プール
 - IP アドレス
 - ルート ターゲット (RT)

- ルート識別子 (RD)
- Site of Origin (SOO)
- バーチャルプライベート ネットワーク (VPN)
- カスタマー エッジ (CE) ルーティング コミュニティ (CERC)
- 名前付き物理回線 (NPC)



(注) これらのステップの詳細は、「[Prime Provisioning サービスの設定](#)」(P.5-4) で説明します。

MPLS ポリシーとサービス要求の操作

Prime Provisioning でプロバイダー、カスタマー、デバイス、およびリソースを設定したら、MPLS ポリシーの作成、サービス要求のプロビジョニング、およびサービスの展開をする準備は完了です。サービス要求が展開されたら、サービス要求のモニタ、監査、およびレポートを実行できます。このマニュアルでは、これらすべてのタスクについて説明します。これらのタスクを実行するには、次の手順を実行します。

- ステップ 1** 必要に応じて、MPLS の概念の概要情報を確認します。
- ステップ 2** MPLS ポリシーを設定します。
- 基本的な情報と重要な概念については、このマニュアルの以降の章に加え、「[MPLS VPN サービス ポリシー](#)」(P.5-42) を参照してください。
- ステップ 3** MPLS サービス要求をプロビジョニングします。
- プロビジョニングするサービス要求のタイプに応じて、該当する項を参照してください。
- 「[プロビジョニング管理 VPN](#)」(P.5-126)
 - 「[MPLS VPN サービス要求](#)」(P.5-83)
 - 「[標準 PE-CE リンクのプロビジョニング](#)」(P.5-104)
 - 「[マルチ VRFCE PE-CE リンクのプロビジョニング](#)」(P.5-115)
 - 「[プロビジョニング管理 VPN](#)」(P.5-126)
 - 「[ケーブル サービスのプロビジョニング](#)」(P.5-136)
 - 「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146)
 - 「[複数のデバイスのプロビジョニング](#)」(P.5-150)
 - 「[複数の自律システムのスパニング](#)」(P.5-161)
- ステップ 4** MPLS サービス要求を展開します。
- 「[MPLS VPN サービス要求](#)」(P.5-83) を参照してください。
- ステップ 5** 展開したサービスのステータスを確認します。
- 次の中から 1 つ以上の方法を使用できます。
- サービス要求をモニタします。「[サービス要求のモニタリング](#)」(P.8-11) の項を参照してください。
 - サービス要求を監査します。「[サービス要求の展開、モニタリング、および監査](#)」(P.3-176) の項を参照してください。
 - MPLS レポートを実行します。「[MPLS レポートの生成](#)」(P.10-42) を参照してください。

- ステップ 6** MPLS サービスのトラブルシューティングを行います。
[「MPLS VPN のトラブルシューティング」\(P.5-253\)](#) を参照してください。

特定のトピックの詳細については、このマニュアルの次の項を参照してください。

- IPv6 および 6VPE サポートの詳細については、「[MPLS VPN での IPv6 および 6VPE サポート \(P.5-32\)](#)」を参照してください。
- MPLS サービス用に Prime Provisioning によって生成されるサンプル コンフィグレットについては、「[サンプル コンフィグレット \(P.5-172\)](#)」を参照してください
- Prime Provisioning ポリシーおよびサービス要求でのテンプレートおよびデータ ファイルの使用の詳細については、次を参照してください。[第 9 章「テンプレートおよびデータ ファイルの管理」](#)

Prime Provisioning サービスの設定

この項では、MPLS VPN サービス ポリシーとサービス要求をサポートするように Prime Provisioning サービスを設定するための基本的な手順などについて説明します。



(注)

この項では、MPLS VPN に関連する Prime Provisioning サービスに関する概要を説明します。これらと、他の基本的な Prime Provisioning サービスの設定の詳細については、[第 2 章「Prime Provisioning を設定する前に」](#) および [第 8 章「サービス要求の管理」](#) を参照してください。

具体的な内容は、次のとおりです。

- 「[概要 \(P.5-4\)](#)」
- 「[IOS XR サポートのためのデバイスの設定 \(P.5-6\)](#)」
- 「[IOS から IOS XR への PE デバイスの移行 \(P.5-7\)](#)」
- 「[VPN の定義 \(P.5-7\)](#)」
- 「[固有ルート識別子を使用した MPLS サービス要求のプロビジョニング \(P.5-12\)](#)」

概要

MPLS VPN サービス要求を作成するには、次のインフラストラクチャ データを作成する必要があります。

- デバイス

Prime Provisioning のデバイスは、ネットワーク内の物理デバイスを論理的に表したものです。インベントリ マネージャまたは Prime Provisioning GUI を使用して、デバイス（コンフィギュレーション）を Prime Provisioning にインポートできます。また、インベントリ マネージャの自動検出機能を使用して、リポジトリにデバイスをインポートすることもできます。

デバイス属性を設定するには、[第 2 章「Prime Provisioning を設定する前に」](#)の [デバイスおよびデバイス グループを設定する方法](#) を参照してください。

- 未処理デバイスのインポートまたは追加

Prime Provisioning が管理するネットワーク要素はすべて、Prime Provisioning リポジトリ内のデバイスとして定義する必要があります。要素とは、Prime Provisioning が情報を収集できる任意のデバイスです。ほとんどの場合、デバイスは Cisco IOS ルータおよびスイッチです。Prime

Provisioning 内のデバイスは、手動で、または自動検出を介して、またはデバイス コンフィギュレーション ファイルをインポートすることで設定できます。デバイス設定のインポート、追加、および収集を実行する手順の詳細については、付録 E 「インベントリ - ディスカバリ」を参照してください。

- カスタマー

通常、カスタマーは、サービス プロバイダーからネットワーク サービスを受ける企業または大企業です。カスタマーは、Prime Provisioning の主要論理コンポーネントでもあります。

- サイト

サイトは、カスタマーと CE を接続する Prime Provisioning の論理コンポーネントです。また、物理的なカスタマー サイトを表すこともできます。

- CPE/CE デバイス

CPE とは「顧客宅内装置」であり、通常はカスタマー エッジルータ (CE) です。また、Prime Provisioning の論理コンポーネントでもあります。カスタマー サイトとデバイスを関連付けることで Prime Provisioning で CPE を作成できます。

カスタマーおよびサイトを作成する手順の詳細については、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」(P.2-42) を参照してください。

- プロバイダー

一般的にプロバイダーとは、ネットワーク サービスをカスタマーに提供する「サービス プロバイダー」または大企業です。プロバイダーは、Prime Provisioning の主要論理コンポーネントでもあります。

- リージョン

リージョンは、プロバイダーと PE を接続する Prime Provisioning の論理コンポーネントです。また、物理的なプロバイダー リージョンを表すこともできます。

- PE デバイス

PE は、プロバイダー エッジルータまたはスイッチです。また、Prime Provisioning の論理コンポーネントでもあります。プロバイダー リージョンとデバイスを関連付けることで Prime Provisioning で PE を作成できます。Prime Provisioning では、PE は「アクセス ポイント」ルータ (POP) またはレイヤ 2 スイッチ (CLE) です。

プロバイダーおよびリージョンを作成するには、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」(P.2-42) を参照してください。

- アクセス ドメイン (レイヤ 2 アクセス用)

PE を CE に接続するレイヤ 2 イーサネット スイッチング ドメインは、アクセス ドメインと呼ばれます。PE-POP に接続されるすべてのスイッチは、このアクセス ドメインに属します。これらのスイッチはプロバイダーに属し、PE-CLE として Prime Provisioning に定義されます。

プロバイダーおよびリージョンを作成するには、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」(P.2-42) を参照してください。

- リソース プール

- IP アドレス

- マルチキャスト

- ルート識別子

- ルート ターゲット

- VLAN (レイヤ 2 アクセス用)

プロバイダーおよびリージョンを作成するには、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」(P.2-42) を参照してください。

- VPN

サービス ポリシーを作成する前に、Prime Provisioning 内に VPN 名を定義する必要があります。

- ルート ターゲット

ルート ターゲットを作成するには、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」(P.2-42) を参照してください。

IOS XR サポートのためのデバイスの設定

Prime Provisioning は、シスコの IOS XR ソフトウェアを実行しているデバイス上の基本 MPLS VPN のプロビジョニングをサポートします。Cisco IOS ファミリの新しいメンバーである IOS XR は、常時稼働の操作のために設計された固有のセルフヒーリングの自己防衛型オペレーティング システムで、システムの容量を 92Tbps まで拡張できます。



(注)

MPLS VPN 用の IOS XR デバイスに対してサポートされる特定のプラットフォームおよび機能と、サポートされる IOS XR バージョンの詳細については、『Cisco Prime Provisioning 6.3 Release Notes』を参照してください。

MPLS VPN で IOS XR サポートをイネーブルにするには、次の手順を実行します。

-
- ステップ 1** DCPL プロパティ **Provisioning/Service/mpls/platform/CISCO_ROUTER/IosXRConfigType** を [XML] に設定します。
- 設定できる値は、**CLI**、**CLI_XML**、および **XML** (デフォルト) です。
- ステップ 2** DCPL プロパティ **DCS/getCommitCLIConfigAfterDownload** を true (デフォルト) に設定します。
- これにより、XML コンフィギュレーションがダウンロードされた後に、コミットされた CLI コンフィギュレーションを Prime Provisioning が取得できるようになります。詳細については、「[IOS XR デバイスでのコンフィグレットの表示](#)」(P.8-6) を参照してください。
- ステップ 3** 次に示すように、Prime Provisioning に IOS XR デバイスとしてデバイスを作成します。
- [Inventory] > [Physical Inventory] > [Devices] > [Create] > [Cisco Device] を選択することにより、シスコ デバイスを作成します。
- [Create Cisco Router] ウィンドウが表示されます。
- [Device and Configuration Access Information] の下にある [OS] 属性を [IOS_XR] に設定します。



(注)

DCPL プロパティの設定とシスコ デバイスの作成に関する追加情報については、[Appendix B](#)、[“Property Settings”](#) を参照してください。

- ステップ 4** このマニュアルの手順に従って、MPLS VPN サービス要求を作成して展開します。
-

IOS XR デバイスのサンプル コンフィグレットは、「[サンプル コンフィグレット](#)」(P.5-172) で提供されています。

IOS から IOS XR への PE デバイスの移行

IOS から IOS XR への PE デバイスの移行については、「[IOS から IOS XR への PE デバイスの移行 \(P.5-103\)](#)」を参照してください。

VPN の定義

サービス展開時に、Prime Provisioning は、論理 VPN 関係を設定するための Cisco IOS コマンドを生成します。プロビジョニングプロセスの最初、サービス ポリシーを作成する前に、Prime Provisioning 内に VPN を定義できます。



(注)

VPN および VRF の情報を独立 VRF オブジェクト内で指定することもできます。これは、後で PE デバイスに配置され、その後 MPLS VPN サービス要求を介して MPLS VPN リンクに関連付けられます。この機能の使用方法的詳細については、「[独立 VRF 管理 \(P.5-15\)](#)」を参照してください。

この項では、MPLS VPN および IP マルチキャスト VPN の定義方法を説明します。次の事項について説明します。

- 「[MPLS VPN の作成 \(P.5-7\)](#)」
- 「[IP マルチキャスト VPN の作成 \(P.5-9\)](#)」
- 「[VPN の固有ルート識別子のイネーブル化 \(P.5-12\)](#)」

MPLS VPN の作成

バーチャル プライベート ネットワーク (VPN) は、簡単に言うと、同じルーティング テーブルを共有するサイトの集まりです。VPN は、インターネットなどの公共のインフラストラクチャを介してプライベート IP ネットワーキングを実現するフレームワークでもあります。Prime Provisioning では、VPN は VPN サービスを介して通信するように設定された一連のカスタマー サイトです。VPN は、一連の管理ポリシーによって定義します。

VPN は、2つのサイトがプロバイダーのネットワークを介して非公開で通信できるネットワークです。つまり、VPN の外側のサイトは、このネットワークのパケットを傍受できず、また新しいパケットを挿入できません。プロバイダー ネットワークは、1つの VPN だけのパケットをこの VPN を介して転送できるように設定されています。つまり、データが VPN に入ること、または VPN から出ることはいけません (これらを許可するように特別に設定されていない場合)。プロバイダー エッジ ネットワークからカスタマー エッジ ネットワークへの物理接続があるため、従来の意味での認証は必要ではありません。

MPLS VPN を作成するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VPNs] を選択します。
[VPNs] ウィンドウが表示されます。
- ステップ 2** [VPN] ウィンドウで、[Create] をクリックします。
[Create New VPN] ウィンドウが表示されます。
- ステップ 3** [Name] フィールドに VPN の名前を入力します。
- ステップ 4** [Select] をクリックし、[Customer] フィールドからこの VPN に関連付けられるカスタマーを選択します。

- ステップ 5** デフォルトのルーティング コミュニティを作成するには、[Create Default Route Target(s)] チェックボックスをオンにしてプロバイダーを選択します。
- ステップ 6** 固有ルータ識別子をイネーブルにするには、チェックボックスをオンにします。この属性の対象範囲については、「VPN の固有ルータ識別子のイネーブル化」(P.5-12) を参照してください。
- ステップ 7** OSPF ドメイン ID 値を 10 進形式で入力します。[Hex value] フィールドは、対応する 16 進数値を表示する編集不可のテキスト フィールドです。この 16 進数値は、実際にデバイスに表示される値です。
- OSPF ドメイン ID はいつでも変更できます。すでに展開されている VPN の OSPF ドメイン ID を変更しようとする、この VPN を使用して、属性 [Use VRF/VPN Domain ID] がイネーブルであるすべてのサービス要求は、[Requested] 状態に移行します。Prime Provisioning は、[Requested] 状態に移行したサービス要求のリストを提供し、それらを展開できるようにします。この操作は、展開されている VPN のマルチキャストをイネーブルまたはディセーブルにする操作と似ています。
 - OSPF ドメイン ID は、IOS XR デバイスでのみサポートされます。IOS デバイスの場合、OSPF ドメイン ID が指定されている VPN を選択すると、Prime Provisioning はこの属性を無視します。
 - 詳細については、「OSPF プロトコルの選択」(P.5-64) の [OSPF Domain ID] 属性の説明を参照してください。
- ステップ 8** VPN のマルチキャストをイネーブルにするには、[Enable IPv4 Multicast] チェックボックスまたは [Enable IPv6 Multicast] チェックボックスをオンにします。「IP マルチキャスト VPN の作成」(P.5-9) を参照してください。



(注) これらの属性は、MVRFCPE ポリシーおよびサービス要求とともに使用する場合はサポートされません。



(注) [Enable IPv6 Multicast] は、IOS デバイスおよび IOS 6VPE デバイスではサポートされません。



(注) 属性の次のセット (ルート ターゲットまで) は、イネーブルなマルチキャスト属性の 1 つがオンである場合にのみ GUI でアクティブになります。これらの属性の対象範囲については、「IP マルチキャスト VPN の作成」(P.5-9) を参照してください。

- ステップ 9** ルート ターゲット : デフォルトのルート ターゲットをイネーブルにしない場合は、Prime Provisioning で前もって作成していた、カスタマイズされたルート ターゲットを選択できます。



(注) マルチキャストがイネーブルである場合は、CERC を指定する必要があります。

- [CE Routing Communities] ペインから、[Select] をクリックします。
[Select CE Routing Communities] ダイアログボックスが表示されます。
- この VPN に使用する CERC のチェックボックスをオンにして、[Select] をクリックします。
[Create VPN] ダイアログボックスに戻り、新しい CERC 選択が Hub Route Target (HRT; ハブ ルート ターゲット) および Spoke Route Target (SRT; スポーク ルート ターゲット) の値とともに表示されます。

- ステップ 10** [Enable VPLS] チェックボックスをオンにして、VPLS をイネーブルにします。

- ステップ 11** [Service Type] ドロップダウン メニューから VPLS サービス タイプを選択します ([ERS] (Ethernet Relay Service) または [EWS] (Ethernet Wire Service))。

ステップ 12 ドロップダウンメニューから、[Full Mesh] (各 CE は他のすべての CE に直接接続できます) または [Hub and Spoke] (ハブ CE のみが各スポーク CE に接続でき、スポーク CE はお互いに直接接続できません) の VPLS トポロジを選択します。

ステップ 13 この VPN の設定が終了したら、[Save] をクリックします。

[VPNs] ダイアログボックスの左下隅の [Status] 表示で示されるように、VPN が正常に作成されました。

IP マルチキャスト VPN の作成

バイナリプレフィックス 1110 で始まる IP アドレスは、マルチキャストグループアドレスとして識別されます。特定のマルチキャストグループアドレスに対して、任意の時点で複数の送信者および受信者が存在する可能性があります。送信者は、宛先 IP アドレスとしてグループアドレスを設定して、データを送信します。ネットワーク内で、このグループアドレスをリッスンしているすべての受信者にこのデータを配信するのは、ネットワークの役割です。



(注)

マルチキャストをイネーブルにして VPN を作成する前に、1 つ以上のマルチキャストリソースプールを定義する必要があります。詳細については、「[マルチキャストプールの作成](#)」(P.2-48) を参照してください。

IOS XR を実行しているデバイスのサービス要求でマルチキャスト VPN を使用する場合は、[Create VPN] ウィンドウのマルチキャスト属性がすべてサポートされるわけではありません。これは、IOS マルチキャストコマンドから IOS XR コマンドへの 1 対 1 のマッピングが存在しないためです。これらの例外は次の手順に示されています: IOS と IOS XR のマルチキャストルーティングコマンドの比較については、「[IOS および IOS XR デバイスでのマルチキャストルーティング](#)」(P.5-39) を参照してください。

マルチキャスト VRF 展開もサポートされています。Prime Provisioning での VRF オブジェクトサポートの詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。

IP マルチキャスト VPN を作成するには、「[MPLS VPN の作成](#)」(P.5-7) で説明されている手順で VPN のマルチキャストをイネーブルにできる箇所まで完了してから、次の手順を実行します。

ステップ 1 [Enable IPv4 Multicast] チェックボックスまたは [Enable IPv6 Multicast] チェックボックスのいずれか、または両方をオンにして、VPN のマルチキャストをイネーブルにします。



(注)

[Enable IPv6 Multicast] は、IOS デバイスおよび IOS 6VPE デバイスではサポートされません。

現在のウィンドウが更新され、追加のフィールドがアクティブになります。

使用方法に関する注釈:

- リリース 3.7.0 以降を実行している IOS XR PE デバイスの場合、Prime Provisioning を使用して、マルチキャスト VPN を IPv6 PE-CE リンクに展開し、VRF オブジェクトの作成中にマルチキャストをイネーブルにすることができます。
- VPN を作成するときに、IPv4、IPv6、またはその両方についてマルチキャストをイネーブルにできます。VPN または VRF オブジェクトの作成時に IPv6 マルチキャストがイネーブルになった場合、IPv6 アドレスをスタティックランデブーポイント (RP) アドレスとして入力できます。

- 既存の VPN オブジェクトを変更して IPv4 または IPv6、あるいはその両方に対してマルチキャストをイネーブルにすることもできます。IPv4 マルチキャストがイネーブルである場合、同じ VPN の IPv4 リンクを含むすべての展開済みサービス要求は、[Requested] 状態に移行します。
- さらに、特定の MPLS リンクに対して IPv4、IPv6 またはその両方のマルチキャストをイネーブルにするかどうかを、MPLS サービス要求内で指定できます。
- IPv6 マルチキャストがイネーブルである場合、同じ VPN の IPv6 リンクを含むすべての展開済みサービス要求は、[Requested] 状態に移行します。IPv4 が以前に設定されていて、IPv6 マルチキャストのみが VPN でイネーブルになっている場合、IPv6 リンクを使用するサービス要求のみが [Requested] 状態に移行します。
- IPv6 マルチキャストがイネーブルの場合、既存の VPN オブジェクトを変更し、IPv6 スタティック RP アドレスを追加できます。すでに [Deployed] 状態にあるサービス要求は、[Requested] 状態に移行します。
- IP アドレッシング スキームとして IPv6 番号指定または IPv4+IPv6 番号指定を使用するサービス要求内のサービス ポリシーまたは MPLS VPN リンク、およびマルチキャストがイネーブルであるマルチキャスト VPN を作成できます。

ステップ 2 Multicast Distribution Tree (MDT; マルチキャスト分散ツリー) アドレスの場合、デフォルト (チェックボックスはすでにオン) を受け入れて自動選択機能をイネーブルにするか、または自動選択のチェックボックスをオフにしてから、次の 2 つのフィールドに値を入力します。

- Default MDT Address
- Data MDT Subnet

ステップ 3 [Data MDT Size] ドロップダウン リストから、[Data MDT Size] の値を選択します。

ステップ 4 [Data MDT Threshold] フィールドに、[Data MDT Threshold] に対する有効な値 (1 ~ 4294967 キロビット/秒) を入力します。

ステップ 5 デフォルトの PIM (Protocol Independent Multicast) モードの場合、[Default PIM Mode] ドロップダウン リストからモードを選択します。

- SPARSE_MODE
- SPARSE_DENSE_MODE



ヒント マルチキャスト ルーティング アーキテクチャでは、IP マルチキャスト ルーティングを既存の IP ネットワークに追加できます。PIM は、独立したユニキャスト ルーティング プロトコルです。Dense および Sparse の 2 つのモードで動作できます。



(注) IOS XR デバイスの場合、SPARSE_DENSE_MODE が選択されると、コンフィグレットは生成されません。IOS XR では Sparse-Dense モードはサポートされず、Sparse モード (デフォルト) と双方向モードのみがサポートされます。IOS XR デバイスの場合、インターフェイスでマルチキャスト ルーティングがイネーブルになると、Sparse モードがデフォルトで実行されます。したがって、Sparse モードの場合もコンフィグレットは生成されません。

ステップ 6 [MDT MTU] フィールドに、MDT MTU (最大伝送単位) に有効な値を入力します。



(注) この属性に対する IOS デバイスと IOS XR デバイスの範囲は異なります。IOS デバイスの場合の範囲は 576 ~ 18010、IOS XR デバイスの場合の範囲は 1401 ~ 65535 です。マルチキャスト VPN が展開されるデバイスのタイプがわかっている場合、サービス要求作成時にデバイスタイプの検証が実行されます。

ステップ 7 PIM SSM (Source Specific Multicast) をイネーブルにするには、関連付けられたチェックボックスをオンにします。

このチェックボックスをオンにすると、次のようになります。

- a. 関連ドロップダウン リストがアクティブになり、DEFAULT 列挙が SSM デフォルトとして入力されています。これにより、次の CLI、**ip pim vrf vrfName ssm default** が作成されます。



(注) IOS XR デバイスの場合、DEFAULT を選択すると、コンフィグレットは生成されません。これは、このコマンドが、標準 SSM 範囲 232.0.0.0/8 を使用して、デフォルトで IOS XR デバイス上で実行されているためです。

- b. アクセス リスト番号または名前付きアクセス リストを SSM 設定に関連付ける場合、[SSM] ドロップダウン リストから DEFAULT ではなく RANGE 列挙を選択します。これにより、次の CLI、**ip pim vrf vrfName ssm range {ACL# | named-ACL-name}** が作成されます。

ステップ 8 前のステップで RANGE を選択した場合、[SSM List Name] フィールドがアクティブになり、アクセス リスト番号またはアクセス リスト名を入力できます。

ステップ 9 [Multicast Route Limit] フィールドに、Multicast Route Limit に有効な値 (1 ~ 2147483647) を入力します。

使用方法に関する注釈：

- VRF あたりのルート制限を設定するコマンドは、IOS と IOS XR の両方でサポートされます。
- GUI にリストされている範囲 (1 ~ 2147483647) は、IOS の場合です。IOS XR の場合、範囲は 1 ~ 200000 です。GUI の範囲値に関する情報を表示するには、属性のツールチップアイコンをクリックします。
- Prime Provisioning は、この属性を使用して VPN または VRF オブジェクトを使用するサービス要求が作成されると、デバイス固有の値検証を実行します。
- Multicast Route Limit の値は、IPv4 アドレス ファミリと IPv6 アドレス ファミリの両方で共有されます。

ステップ 10 自動 Rendezvous Point (RP; ランデブー ポイント) リスナー機能をイネーブルにするには、[Enable Auto RP Listener] チェックボックスをオンにします。



(注) IOS XR デバイスの場合、この属性に対してコンフィグレットは生成されません。デフォルトでは、この機能は IOS XR デバイス上で実行されます。

ステップ 11 スタティック RP を設定するには、[Configure Static-RP] チェックボックスをオンにします。

このチェックボックスをオンにすると、PIM スタティック RP の [Edit] オプションがアクティブになります。

ステップ 12 PIM スタティック RP を編集または追加するには、[PIM Static RPs] 領域で [Edit] をクリックします。[Edit PIM Static RPs] ウィンドウが表示されます。

ステップ 13 [Edit PIM Static RP] ウィンドウで該当するすべてのフィールドに入力してから、[OK] をクリックします。

データがメイン [Create VPN] ウィンドウに表示されます。

ステップ 14 変更内容を保存してこのマルチキャスト VPN をシステムに追加するには、ウィンドウの下部で [Save] をクリックします。

VPN の固有ルート識別子のイネーブル化



(注)

Cisco Prime Provisioning 6.3 では、固有ルート識別子のイネーブル化は、IOS デバイスと IOS XR PE デバイスの両方でサポートされます。IPv6 およびデュアルスタック サービスの場合にもサポートされます。

マルチパス ロード シェアリングのサポートには、VPN (VRF) の各 PE ルータに固有 Route Distinguisher (RD; ルート識別子) が必要です。この目的は、同じ RD が異なるカスタマーに割り当てられないようにすることです。これにより、同じ RD を同じ VRF に使用できます。つまり、PE 内のすべてのサイトが同じ固有 RD を持つことができます。固有 RD 機能はオプションです。これは、グローバル VPN レベルとサービス要求レベルの両方でイネーブルです。VPN の PE ごとに固有 RD を使用できるようにするために、[Create VPN] ウィンドウには属性 [Enable Unique Route Distinguisher] のフィールドが含まれています。

[Enable Unique Route Distinguisher] が選択されている Prime Provisioning を使用して展開された各 VPN は、マルチパス VPN としてマークされます。これにより、各 PE の各 VRF に固有 RD が割り当てられるようになります。すでに展開されている VPN に対してマルチパスをイネーブルにすると、VPN のすべての PE に新規 VRF が作成され、固有 RD が割り当てられます。VPN に対して [Enable Unique Route Distinguisher] が選択されると、この VPN を使用するポリシーまたはサービス要求を設定するときに、[Allocate New Route Distinguisher] 属性および [VRF and RD Overwrite] 属性はイネーブルになります。

固有 RD 機能を使用するには、次の手順を実行します。

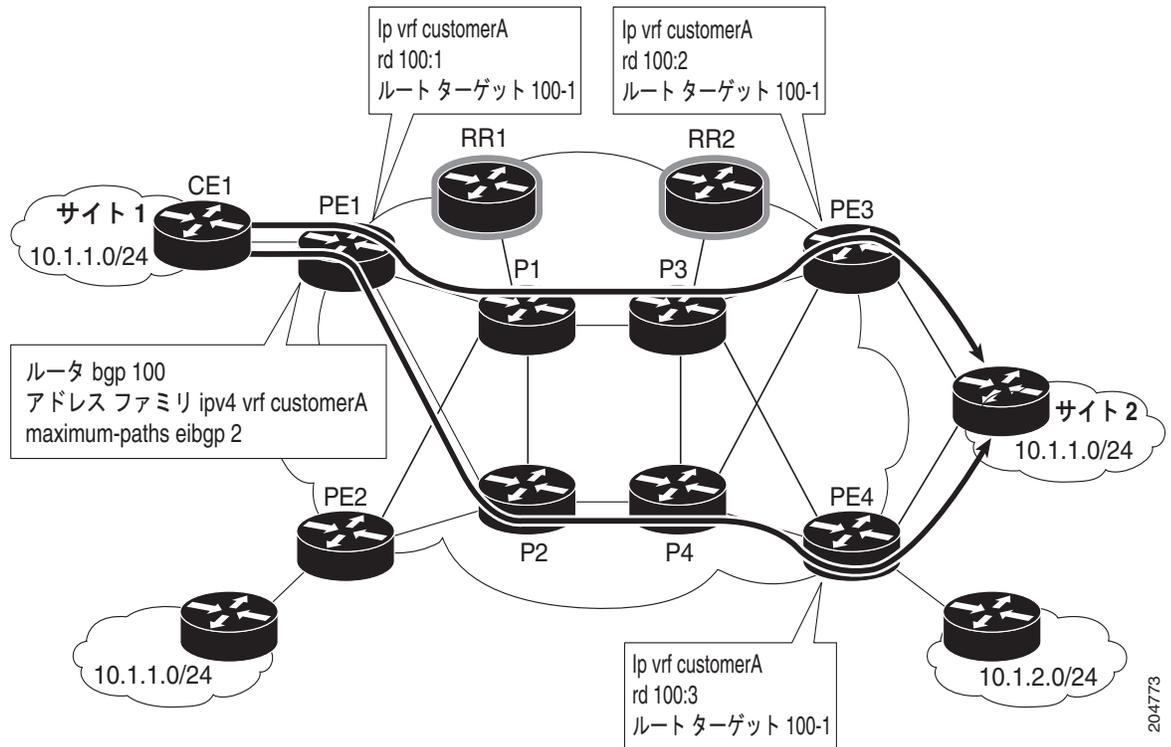
-
- ステップ 1** VPN を作成するときに、[Enable Unique Route Distinguisher] チェックボックスをオンにします。
 - ステップ 2** 後でサービス ポリシーまたはサービス要求を作成するときに、[VRF and VPN Membership] ウィンドウでその VPN を選択します。
[Unique Route Distinguisher] フィールドが表示されます。
 - ステップ 3** 固有 RD 割り当て機能が必要な場合は、[Unique Route Distinguisher] チェックボックスをオンにします。
-

この機能が MPLS VPN ポリシーおよびサービス要求でどのように使用されるかについての詳細は、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。

固有ルート識別子を使用した MPLS サービス要求のプロビジョニング

固有ルート識別子 (RD) 機能は、マルチパス ロード バランシングを実装するために使用します。マルチホーム CE は、使用可能な複数のパス間でロード バランシングを必要とすることがよくあります。フル メッシュ BGP 環境では、PE は特定のプレフィックスへの使用可能なパスをすべて受信するため、ロード バランシングを簡単に実現できます。ただし、サービス プロバイダー コア内にルート リフレクタが存在する場合、PE ルータは複数のパスが存在する場合でも 1 つのルートのみを受信し、ロード バランシングは発生しません。ロード バランシングを実現するには、サービス プロバイダーは各 PE ルータのカスタマー VPN に対して固有 RD 値を実装する必要があります。さらに、必要な数のパスを持つ eiBGP コンフィギュレーション (その間でのロード バランシングが必要) を、サービス プロバイダー環境でイネーブルにする必要があります。図 5-1 に、ロード バランシングの例を示します。

図 5-1 さまざまな RD を使用するロード バランシング



マルチパス ロードシェアリングのサポートには、VPN (VRF) の各 PE ルータに固有 RD が必要です。この目的は、同じ RD が異なるカスタマーに割り当てられないようにすることです。これにより、同じ RD を同じ VRF に使用できます。つまり、PE 内のすべてのサイトが同じ固有 RD を持つことができます。固有 RD 機能はオプションです。これを使用するかどうかをポリシー レベルとサービス要求レベルの両方で指定できます。

これは、グローバル VPN レベルとサービス要求レベルの両方でイネーブルです。

Prime Provisioning は、Prime Provisioning GUI のフィールドとオプションを使用して BGP マルチパス ロードシェアリングをサポートします。次のステップで、これを行う方法の概要を説明します。

- ステップ 1** VPN を作成するときに、[Create VPN] ウィンドウで [Enable Unique Route Distinguisher] チェックボックスをオンにします。
- 詳細については、「[VPN の固有ルート識別子のイネーブル化](#)」(P.5-12) を参照してください。
- ステップ 2** ポリシー ([MPLS Policy Editor - VRF and VPN Membership] ウィンドウ) またはサービス要求 ([MPLS Link Attribute Editor - VRF and VPN] ウィンドウ) の属性を設定するときに、[BGP Multipath Load Sharing] チェックボックスを使用して、BGP マルチパス ロードシェアリングをイネーブルまたはディセーブルにします。

チェックボックスをオンにして BGP マルチパス ロード シェアリングをイネーブルにすると、追加の属性が GUI に表示されます。これらの属性および設定方法の詳細については、「[BGP マルチパス ロード シェアリングおよび最大パス設定](#)」(P.5-80) を参照してください。

- ステップ 3** このポリシーに基づくサービス要求を作成するときに、[MPLS Link Attribute Editor - VRF and VPN] ウィンドウで [Unique Route Distinguisher] チェックボックスをオンにします。



(注) [Unique Route Distinguisher] 属性は動的であり、固有 RD がイネーブルな VPN が選択されている場合にのみ GUI に表示されます。

- ステップ 4** サービス要求作成を完了し、サービス要求を保存します。

固有 RD の使用例

次の使用例で、固有 RD 機能の動作を示します。

使用例の詳細：

- VPN/VRF のデフォルト値は次のとおりです。

```
ip vrf V24:unique2
rd 1:33
route-target import 1:14
route-target import 1:15
route-target export 1:14
```

- 表 5-1 に示されているように、サービス要求は、PE の使用、およびサービス要求作成時の [Unique RD] 属性のイネーブル化またはディセーブル化により作成されます。

さまざまなケースの結果については、表の「結果」列で説明されています。

表 5-1 固有 RD の使用例

SR #	PE	固有 RD	VRF:RD	結果
1	pe1	False	V24:33	この PE をこの <i>vrfName:RD</i> 名で設定したのが初めてであるため、Prime Provisioning はデフォルトの <i>vrfName:RD</i> を使用します。
2	pe2	False	V24:33	Prime Provisioning は、デフォルトの <i>vrfName:RD</i> を使用します。
3	pe3	True	V25:34	[Unique RD] が true であり、異なる PE 上にあるため、Prime Provisioning は新規 <i>vrfName:RD</i> を作成します。この PE (pe3) では、この <i>vrfName:RD</i> は設定されていません。
4	pe3	True	V25:34	Prime Provisioning は SR #3 の <i>vrfName:RD</i> を使用します。これは、PE ルータに新規 RD がすでに存在するためです。
5	pe2	True	V26:35	Prime Provisioning は新規 <i>vrfName:RD</i> を作成します。これは、SR #2 で V24:33 という VRF がすでに設定されていますが、[Unique RD] が true として選択されたのが初めてであるためです。

表 5-1 固有 RD の使用例 (続き)

SR #	PE	固有 RD	VRF:RD	結果
6	pe1	True	V27:36	Prime Provisioning は新規 <i>vrfName:RD</i> を作成します。これは、SR #1 で V24:33 という VRF がすでに設定されていますが、この PE で [Unique RD] が true として選択されたのが初めてであるためです。
7	pe1	False	V24:33	Prime Provisioning は、SR #1 の場合と同様に、デフォルトの <i>vrfName:RD</i> を使用します。
8	pe3	False	V24:33	Prime Provisioning は、SR #1 の場合と同様に、デフォルトの <i>vrfName:RD</i> を使用します。
9	pe3	True	V25:34	Prime Provisioning は、SR #4 で新規に作成された <i>vrfName:RD</i> を使用します。これは、この PE に対する新規 <i>vrfName:RD</i> がすでに作成されているためです。
10	pe2	True	V26:35	Prime Provisioning は、SR #5 で新規に作成された <i>vrfName:RD</i> を使用します。これは、この PE に対する新規 <i>vrfName:RD</i> がすでに作成されているためです。
11	pe1	True	V27:36	Prime Provisioning は、SR #6 で新規に作成された <i>vrfName:RD</i> を使用します。これは、この PE に対する新規 <i>vrfName:RD</i> がすでに作成されているためです。

独立 VRF 管理

この項では、MPLS VPN リンクおよびサービス要求から独立して VRF オブジェクトを作成、展開、および管理する方法を提供する独立 VRF 管理について説明します。展開した VRF オブジェクトは、MPLS VPN リンクにも使用できます。

以前のリリースの Prime Provisioning で使用できた従来の VPN モデルでは、オペレータはまず VPN オブジェクトを作成してから、VPN オブジェクトを MPLS VPN リンクに関連付けていました。必要な VRF 情報は、MPLS VPN リンクをプロビジョニングするときに生成され、展開されます。VRF 情報が削除されるのは、VRF に関連付けられた最後のリンクがデコミッションされた場合だけです。ただし、場合によっては物理リンクから独立してプロビジョニングされた VRF 情報があることが必要な場合があります。Prime Provisioning では、現在、この項で説明する独立 VRF の管理機能を使用してこのシナリオがサポートされています。これにより、MPLS VPN リンクとは関係なく VRF オブジェクトの作成、変更、および削除を実行できるようになります。これには、次のようないくつかの利点があります。

- VRF 情報およびテンプレートは、インターフェイスと関連付けることなく、PE デバイスで直接展開できます。
- VRF 情報は、VRF 向けのリンクなしで存在できます。
- VRF オブジェクトは、リンクに関連付けられている場合でも変更できます。
- Route Target (RT; ルート ターゲット) は、停止せずに追加および削除できます。

物理リンクとは独立して VRF を管理するには、この項の残りの部分で詳細に説明されている次の作業を行う必要があります

- VRF オブジェクトの作成、変更、削除。
- VRF サービス要求と呼ばれる、新しいタイプのサービス要求の作成、変更、展開、デコミッション、および削除。

- サービス ポリシーとサービス要求を介した MPLS VPN リンクを持つ、展開済み VRF オブジェクトの使用。
- 従来の MPLS VPN サービス要求の独立 VRF モデルへの移行。



(注) 従来の Prime Provisioning VRF モデルは、下位互換性を得るために、現在でもサポートされています。MPLS VPN リンクの作成中に、どの VRF モデルを使用するかを選択できます。これについては、この項の後のほうで説明します。



(注) 独立 VRF の関連付けは、MVRFCE ベースのサービス ポリシーとサービス要求ではサポートされていません。

具体的な内容は、次のとおりです。

- 「IOS XR デバイスでの IPv6 のマルチキャスト サポート」(P.5-16)
- 「VRF オブジェクトの操作」(P.5-17)
- 「VRF サービス要求の操作」(P.5-23)
- 「MPLS VPN サービス要求とポリシーでの VRF の使用」(P.5-28)
- 「既存の MPLS VPN サービス要求から VRF オブジェクト モデルへの移行」(P.5-32)

IOS XR デバイスでの IPv6 のマルチキャスト サポート

リリース 3.7.0 以降を実行している IOS XR PE デバイスの場合、Prime Provisioning を使用して、VRF オブジェクトの作成中にマルチキャストをイネーブルにできます。VRF オブジェクトを作成するとき、IPv4 または IPv6、あるいはその両方に対してマルチキャストをイネーブルにできます。VRF オブジェクトの作成中に IPv6 マルチキャストをイネーブルにした場合は、IPv6 アドレスをスタティック ランデブー ポイント (RP) アドレスとして入力できます。

既存の VRF オブジェクトを変更して IPv4 または IPv6、あるいはその両方に対してマルチキャストをイネーブルにすることもできます。IPv4 マルチキャストがイネーブルの場合、同じ VPN または VRF の IPv4 リンクを含む、展開されたすべてのサービス要求は、[Requested] 状態になります。

さらに、特定の MPLS リンクに対して IPv4、IPv6 またはその両方のマルチキャストをイネーブルにするかどうかを、MPLS サービス要求内で指定できます。

IPv6 マルチキャストがイネーブルの場合、同じ VPN または VRF の IPv6 リンクを含む、展開されたすべてのサービス要求は、[Requested] 状態になります。IPv4 が以前に設定されていて、IPv6 マルチキャストのみが VPN でイネーブルになっている場合、IPv6 リンクを使用するサービス要求のみが [Requested] 状態に移行します。

IPv6 マルチキャストがイネーブルの場合、既存の VRF オブジェクトを変更し、IPv6 スタティック RP アドレスを追加できます。すでに [Deployed] 状態にあるサービス要求は、[Requested] 状態に移行しません。

IP アドレッシング スキームとして IPv6 Numbered または IPv4+IPv6 Numbered を使用し、またマルチキャストがイネーブルのマルチキャスト VRF を使用するサービス要求にサービス ポリシーまたは MPLS VPN リンクを作成できます。

VRF オブジェクトの操作

この項では、VRF オブジェクトを作成、変更、および削除する方法について説明します。この項の後の項では、VRF オブジェクトがサービス要求でどのように使用されるかについて説明します。

新しい VRF オブジェクトの作成

VRF オブジェクトの作成は、VPN の作成と類似しています。ただし、[Import RT List] や [Export RT List] など、いくつかの追加属性が含まれます。VRF オブジェクトを作成した後、これ以降の項で説明されているように、VRF サービス要求を使用してそれを後でプロビジョニングします。

VRF オブジェクトを作成するには、次の手順を実行します。

-
- ステップ 1** [Inventory] > [Logical Inventory] > [VRFs] を選択します。
- ステップ 2** [VRFs] ウィンドウで、[Create] をクリックします。
[Create New VRF] ウィンドウが表示されます。
- ステップ 3** [Name] : VRF オブジェクトの名前を入力します。
これは単純なテキスト フィールドです。選択した名前を入力します。次の特殊文字は使用しないことをお勧めします (' ` " < > () [] { } \ / & ^ ! ? ~ * % = , . + |)。これにより、特定のデバイスの VRF 名に誤設定が生じる可能性があるためです。
この名前は PE デバイスに直接展開されます。Prime Provisioning で VPN オブジェクトを作成するときに VPN 名に適用可能なすべての検証を VRF 名に適用できます。この属性は必須です。
- ステップ 4** [Provider] : この VRF に関連付けられたプロバイダーを選択するには、次の手順を実行します。
a. [Select] をクリックします。
[Select Provider] ダイアログボックスが表示されます。
b. プロバイダーのリストから、適切なプロバイダーを選択し、[Select] をクリックします。
- ステップ 5** [Description] : 必要に応じて、VRF の説明を入力します。
入力した説明に対する検証は行われません。
- ステップ 6** [Route Target(s)] : この VRF のルート ターゲットを選択するには、次の手順を実行します。
a. [Select] をクリックします。
[Select CE Routing Communities] ダイアログボックスが表示されます。
b. リストから適切なルート ターゲットを選択し、[Select] をクリックします。VRF ごとに 1 つのルート ターゲットのみを使用できます。
- ステップ 7** [Import RT List] : VRF にインポートする 1 つ以上のルート ターゲット (RT) を入力します。
複数の RT の場合は、カンマ (,) 区切りのリストを使用します。RT リストは、たとえば 100:120,100:130,100:140 のようになります。
- ステップ 8** [Export RT List] : VRF からエクスポートされる 1 つ以上のルート ターゲット (RT) を入力します。
複数の RT の場合は、カンマ (,) 区切りのリストを使用します。
- ステップ 9** [Import Route Map] : デバイスに定義したルート マップの名前を入力します。
Prime Provisioning は、VRF のプロビジョニング中にこの名前を検証します。ルート マップが定義されていない場合、Prime Provisioning はエラーを生成します。
- ステップ 10** [Export Route Map] : デバイスに定義したルート マップの名前を入力します。

Prime Provisioning は、VRF のプロビジョニング中にこの名前を検証します。ルート マップが定義されていない場合、Prime Provisioning はエラーを生成します。

ステップ 11 [Maximum Routes] : VRF にインポートできるルートの最大数を指定します。

これは、IOS デバイスの場合は 1 ~ 4294967295 の整数値にし、IOS XR デバイスの場合は 32 ~ 2000000 の整数値にします。

ステップ 12 [Threshold] : しきい値を指定します。しきい値は、割合を定義し、これを超えた場合は警告メッセージが生成されます。

これは、1 ~ 100 の整数値です。この属性は、IOS デバイスでは必須ですが、IOS XR デバイスではオプションです。特定のデバイス タイプの検証は、サービス要求の作成中に実行されます。

ステップ 13 [RD Format] : RD (ルート識別子) フォーマットのフォーマットを指定するには、ドロップダウン リストからフォーマット タイプを選択します。

- [RD_AS] : AS (自律システム) フォーマットで RD を指定します。これはデフォルトの選択肢です。
- [RD_IPADDR] : IP アドレス フォーマットで RD を指定します。これは、IOS デバイスと IOS XR PE デバイスでサポートされています。

選択された RD フォーマットによって、次の手順で RD をどのように設定する必要があるかが決まります。

ステップ 14 [RD] : RD (ルート識別子) を (前の手順で選択したフォーマットに従って) 手動で指定するか、[Autopick RD] チェックボックスをオンにして Prime Provisioning が自動的にルート識別子プールから RD を選択するようにします (そのように設定されている場合)。

使用方法に関する注釈 :

- この属性は必須です。
- [Autopick RD] チェックボックスをオンにすると、RD のテキスト入力フィールドがディセーブルになります。
- [RD_IPADDR] フォーマットと組み合わせて [Autopick RD] チェックボックスがオンの場合、それぞれのプロバイダーの RD プールから RD の VPN ID が自動で選択されて、RD を形成するためにラベル IP の後尾に付加されます 例 : IP:1245。(この値は、VRF オブジェクトが保存されて編集されたときに表示されます)。サービス要求を作成するときは、実際の IP アドレスを選択します。これは、IP アドレス (つまり、ループバック IPv4 アドレス) は異なる PE では異なる可能性があるためです。
- RD_AS フォーマットとともに [Autopick RD] チェックボックスをオンにすると、Prime Provisioning はルート識別子プールから値を選択し、それをこの特定の VRF オブジェクトに割り当てます。
- [Autopick RD] がオフの場合、表示されたテキスト フィールドに ([RD Format] 属性に指定されたとおりに) 次のフォーマットのいずれかを使用して手動で RD を指定する必要があります。
 - RD_AS フォーマットの RD 値は *as_number:number* の形式にする必要があります。
as_number は AS 番号 (2 バイト値) で *number* は 4 バイトの整数値です。AS 番号は、1 ~ 65,535 の範囲にすることができます。例 : 100:1254。
 - RD_IPADDR の RD 値は *ip_address:number* の形式にする必要があります。*ip_address* は IPv4 アドレスで *number* は 4 バイトの整数値です。この数値は、1 ~ 65,535 の範囲のみにすることができます。例 : 10.23.6.5:1245。
- RD 値を IP アドレス形式で手動で指定した場合、オペレータはさまざまな PE にわたって VRF を展開する必要があります。
- RD フォーマットの検証は、[RD Format] 属性に設定されている RD フォーマットに基づいて実行されます。

- 新しい RD フォーマットの検証以外、PE との関連付けを検証するための確認はされません。
- VRF オブジェクトが展開されていない場合のみ、Prime Provisioning で既存の VRF オブジェクトを新しい RD フォーマットで変更できます。
- 次の Prime Provisioning テンプレート変数は RD フォーマットをサポートしています。
 - RD_FORMAT
 - RD_IPADDRESS

ステップ 15 [OSPF Domain ID] : OSPF ドメイン ID を 10 進形式で入力します。

使用方法に関する注釈 :

- 値を 10 進形式で入力します。[Hex value:] フィールドは、対応する 16 進数値を表示する編集不可のテキスト フィールドです。この 16 進数値は、実際にデバイスに表示される値です。
- OSPF ドメイン ID はいつでも変更できます。展開済みの MPLS サービス要求に関連付けられ、[Use VRF/VPN Domain ID] 属性がイネーブルになっている VRF の OSPF ドメイン ID を変更しようとする、これらのサービス要求は [Requested] 状態に移行します。Prime Provisioning では、この VRF オブジェクトを使用するサービス要求のリストを使用して、それらを展開できます。
- OSPF ドメイン ID プロパティは VRF サービス要求に影響を及ぼしません。また、OSPF ドメイン ID に関連する設定が VRF サービス要求で展開されることはありません。
- OSPF ドメイン ID は、IOS XR デバイスでのみサポートされます。IOS デバイスの場合、OSPF ドメイン ID を指定して VRF オブジェクトを使用すると、Prime Provisioning はこの属性を無視します。
- [OSPF Domain ID] 属性は、ルートの再配布元の OSPF ドメインを一意に識別します。このドメイン ID は、カスタマーごとに固有である必要があります。IOS デバイスの場合、IOS がプロセスごとに 1 つの VRF だけを許可するために、デフォルト動作では OSPF プロセス ID を OSPF ドメイン ID と見なします。IOS XR は、プロセスごとに複数の VRF をサポートしています。このため、IOS XR デバイスの場合、各 VRF に対して固有の OSPF ドメイン ID を明示的に設定する必要があります。OSPF プロセスごとに 1 つの VRF を設定することはできますが、これはスケーラブルなソリューションではありません。
- 詳細については、「OSPF プロトコルの選択」(P.5-64) の [OSPF Domain ID] 属性の説明を参照してください。

ステップ 16 [Enable IPv4 Multicast] または [Enable IPv6 Multicast] : これらのチェックボックスの 1 つまたは両方をオンにして、マルチキャスト VRF をイネーブルにします。

このチェックボックスの下にあるマルチキャスト属性を使用できます。マルチキャスト属性の設定方法詳細については、「IP マルチキャスト VPN の作成」(P.5-9) を参照してください。



(注) この属性は、MVRFCPE ポリシーとサービス要求で使用する場合はサポートされません。



(注) [Enable IPv6 Multicast] は、IOS デバイスおよび IOS 6VPE デバイスではサポートされません。



(注) マルチキャストがイネーブルの場合は、ルート ターゲットは必須です。



(注) MDT MTU 属性の場合 : IOS デバイスの場合の範囲は 576 ~ 18010 です。IOS XR デバイスの範囲は 1401 ~ 65535 です。特定のデバイス タイプの検証は、サービス要求の作成中に実行されます。

- ステップ 17** この VRF オブジェクトの設定が終了したら、[Save] をクリックします。
Prime Provisioning は選択した属性に基づいて、新しい VRF オブジェクトを作成します。新しい VRF は、ウィンドウの [VRF Name] 列に一覧表示されます。

VRF オブジェクトのコピー

既存の VRF オブジェクトを新しいオブジェクトの基盤として使用できます。これを行うには、VRF オブジェクトをコピーし、コピーの名前を変更して、(任意で) 属性を変更します。

既存の VRF オブジェクトをコピーするには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRFs] を選択します。
[VRFs] ウィンドウが表示されます。



(注) この例では、VRF オブジェクトがすでに作成されていることを想定しています。VRF オブジェクトの作成方法については、「[新しい VRF オブジェクトの作成](#)」(P.5-17) を参照してください。

- ステップ 2** VRF オブジェクトのチェックボックスをオンにして、既存の VRF オブジェクト (たとえば、VRF_1) を選択します。
VRF オブジェクトを選択すると、[Edit]、[Copy]、および [Delete] ボタンがアクティブになります。
- ステップ 3** VRF オブジェクトをコピーするには、[Copy] ボタンをクリックします。
コピー対象の VRF オブジェクトから、属性フィールドに値が取り込まれます。
- ステップ 4** [Name] フィールドの名前を変更して、新しい VRF オブジェクトの名前を指定します。
- ステップ 5** 必要に応じて他の属性を [Create VRF] ウィンドウで編集します。



(注) VRF のコピー機能によって、ルート識別子 (RD)、デフォルトの MDT アドレス、およびデータ MDT サブネットを除く、親のすべての属性がコピーされます。RD は常に自動選択に設定されます ([Autopick RD] チェックボックスはデフォルトでオンになります)。親 VRF に自動選択が設定されている場合、コピー機能によって作成された VRF オブジェクトに伝送されません。

- ステップ 6** 編集が完了したら、[Save] ボタンをクリックします。
[VRF Management] ウィンドウが新しい VRF オブジェクトとともに表示されます。
- ステップ 7** VRF オブジェクトのコピー操作は完了です。

Prime Provisioning リポジトリでの VRF オブジェクトの検索

すべての VRF オブジェクトは Prime Provisioning のリポジトリに格納されます。Prime Provisioning GUI で [Inventory] > [Logical Inventory] > [VRF] を選択して [VRF Management] ウィンドウにアクセスすると、VRF オブジェクトを表示できます。[matching] フィールドとともに [Show VRF with] ドロップダウンリストを使用すると、VRF オブジェクトを検索できます。[Show VRF with] ドロップダウンリストを使用して、次の属性を検索し、VRF オブジェクトを表示できます。

- VRF Name
- Provider
- Route Distinguisher
- Route Target



(注) 検索では大文字と小文字は区別されません。また、ワイルドカード (*) 検索がサポートされていません。

展開していない VRF オブジェクトの変更

VRF オブジェクトは個別に (Single-VRF 編集) またはバッチ モード (マルチ VRF 編集) で変更できます。この項では、VRF サービス要求によってまだ展開していないか、MPLS VPN リンクに関連付けられていない VRF オブジェクトを変更するための基本的な手順について説明します。「[展開した VRF オブジェクトの変更](#)」(P.5-22) に説明されているように、展開された VRF を変更する場合に考慮すべき特別な項目がいくつかあります。

Single-VRF 編集モード

VRF オブジェクトを編集するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRF] を選択して、Prime Provisioning リポジトリに VRF オブジェクトをリストします。
[VRFs] ウィンドウが表示されます。
- ステップ 2** 編集する VRF を選択し、[Edit] ボタンをクリックします。
- ステップ 3** 編集する属性を更新します。
- ステップ 4** [Save] をクリックして編集内容を保存します。

Multi-VRF 編集モード

Multi-VRF 編集機能を使用して、複数の VRF で共通の属性を変更できます。たとえば、Multi - VRF 編集は複数の VRF でルート ターゲットを追加または削除する場合に役立ちます。

複数の VRF オブジェクトを同時に編集するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRFs] を選択して、Prime Provisioning リポジトリに VRF オブジェクトをリストします。
[VRFs] ウィンドウが表示されます。
- ステップ 2** 編集する VRF を選択し、[Edit] ボタンをクリックします。
[Edit Multiple VRFs] ウィンドウが表示されます。

[Edit VRFs] ウィンドウは [Create VRF] ウィンドウや [Edit VRF] ウィンドウに似ています。ただし、[VRF Details] フィールドが追加されており、RT のインポートとエクスポート フィールドのレイアウトが異なります。また、Multi-VRF 編集モードでは、一部の属性を編集できません。

ステップ 3 編集した VRF の詳細を表示するには、[VRF Details] 行で [Attributes] リンクをクリックします。

[VRF Details] ウィンドウが表示されます。これには、編集された VRF がリストされ、VRF ごとに次の属性が表示されます。

- Name
- Provider
- Route Target
- Import Route Map
- Export Route Map
- Import Route Target
- Export Route Target
- MultiCast IPv4
- MultiCast IPv6

ステップ 4 インポートまたはエクスポート ルート マップを追加または削除するには、表示されたフィールドに目的の値を入力します。

各フィールドには複数の RT を入力できます。複数の RT の場合は、カンマ (,) 区切りのリストを使用します。

ステップ 5 必要に応じて、[Route Target(s)]、[Import Route Map]、[Export Route Map]、および [Multicast Attributes] の値を更新します。



(注) [Provider] 属性を Multi-VRF 編集モードで編集することはできません。

ステップ 6 編集内容を保存するには、[Save] をクリックします。

展開した VRF オブジェクトの変更

VRF サービス要求を介して PE デバイスで VRF オブジェクトを展開した後は（「[VRF サービス要求の展開](#)」(P.5-26) を参照）、VRF オブジェクトの変更時に注意すべき特別な考慮事項がいくつかあります。

- VRF オブジェクトは、複数のリンクまたは VRF サービス要求、あるいはその両方に関連付けられている可能性があります。
- 従来の VPN オブジェクトとは異なり、複数の VRF サービス要求によって参照されていても VRF オブジェクトを変更できます。
- VRF オブジェクトを展開した後、[VRF Name]、[Provider]、および [RD] 属性を変更することはできません。



(注) [RD] 属性は、IOS 12.0 (32) SY 以上を実行する PE デバイスに VRF サービス要求を展開した場合は変更できます。

展開した VRF オブジェクトを変更するには、次の手順を実行します。

- ステップ 1** 展開した VRF オブジェクトの変更を試みると、[Affected Jobs] ウィンドウが表示されます。変更された VRF オブジェクトに関連付けられた、影響を受ける VRF サービス要求がウィンドウに表示されます。各 VRF サービス要求の [Job ID]、[SR ID]、[Link ID]、[VRF Name]、および [Description] 情報が一覧表示されます。
- ステップ 2** VRF サービス要求の詳細を表示するには、[Job ID] リンクをクリックします。[Service Request Details] ウィンドウが表示されます。
- ステップ 3** 必要に応じて、サービス要求の詳細を確認します。
- ステップ 4** 次のいずれかの操作を実行します。
- [Save] をクリックして VRF オブジェクトを保存し、影響を受けるすべての VRF サービス要求を [Requested] 状態に移行します。
 - [Save and Deploy] をクリックして VRF オブジェクトを保存し、影響を受けるすべての VRF サービス要求を [Requested] 状態に移行し、すべての VRF サービス要求の即時展開をスケジュール設定します。
 - 操作をキャンセルするには [Cancel] をクリックし、[Edit VRFs] ウィンドウに戻ります。

VRF オブジェクトの削除

Prime Provisioning リポジトリから VRF オブジェクトを削除するには、次の手順を実行します。



(注)

1 つ以上の VRF オブジェクトが VRF サービス要求によってまだ使用されている場合には、前もって実行する必要のあるステップがあります。これについては、次の手順の後にある注釈で説明します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRF] を選択して、Prime Provisioning リポジトリに VRF オブジェクトをリストします。[VRFs] ウィンドウが表示されます。
- ステップ 2** 削除する VRF を選択し、[Delete] ボタンをクリックします。
- ステップ 3** [Delete] をクリックして確認します。VRF オブジェクトが使用中でない場合は、選択した VRF オブジェクトは削除されます。

VRF サービス要求に関連付けられた VRF オブジェクトの削除

VRF オブジェクトは、VRF サービス要求に関連付けられている場合、削除できません。削除しようとすると、「Delete VRF Failed」メッセージが [Status] ウィンドウに表示されます。この場合、VRF オブジェクトを削除するには、最初に関連する VRF サービス要求をすべてデコミッション、展開、および削除する必要があります。エラーメッセージ提供される情報を使用して、削除する VRF オブジェクトに関連する VRF サービス要求およびリンクを識別します。

VRF サービス要求の操作

保存された VRF オブジェクトは、VRF サービス要求という名前の特異なタイプのサービス要求を介してプロバイダー エッジ (PE) デバイスに展開されます。

VRF サービス要求の概要

VRF サービス要求では、物理インターフェイスを選択せずに、VRF オブジェクトをルータに設定できます。各 VRF サービス要求は、1 つ以上のリンクで構成されています。各リンクは次の要素で構成されています。

- 1 つの VRF オブジェクト
- 1 つの PE オブジェクト
- 1 つのテンプレート（任意）

また、VRF サービス要求はカスタマーに関連付けられています。



(注)

通常の MPLS サービス要求と VRF サービス要求の重要な違いは、VRF サービス要求には必要なサービス ポリシーがないことです。そのため、VRF サービス要求はサービス ポリシーに関連付けられません。

VRF サービス要求の状態は、「サービス拡張」(P.5-84) で説明されているように、通常の Prime Provisioning サービス要求の状態遷移に従います。

VRF サービス要求の定義

VRF サービス要求を定義するには、次の手順を実行します。

ステップ 1 [Operate] > [Service Requests] > [VRF] を選択して、[VRF Service Requests] ウィンドウにアクセスします。

[VRFs] ウィンドウが表示されます。



(注) 必要に応じて、[Add Link] ボタンをクリックして、リンク情報を設定するための行を作成します。

このウィンドウを使用して、VRF オブジェクト、PE デバイス、およびオプションテンプレートでそれぞれ構成されている 1 つ以上のリンクを設定することで、VRF サービス要求を定義することができます。また、リンクごとにアドレススキームも指定します。ルート識別子 (RD) 値を表示できます。場合によってはそれを設定できます。これは、VRF オブジェクトを作成する場合に RD 形式と RD がどのように指定されているかによって異なります。PE デバイスと VRF オブジェクトの任意の組み合わせを指定して、任意の数のリンクを展開できます。注目すべき重要なポイントは、ルータの物理インターフェイスを選択する必要がないことです。

リンクを設定するには、次の手順を実行します。

ステップ 2 [Customer] 属性の横にあるリンクをクリックして、VRF サービス要求のカスタマーを設定します。

[Select Customer] ウィンドウが表示されます。目的のカスタマーを選択し、[Select] ボタンをクリックします。この属性はオプションです。

ステップ 3 [Select VRF] リンクをクリックして、Prime Provisioning リポジトリから VRF オブジェクトを選択します。

[Select Independent VRF] ウィンドウが表示されます。

ステップ 4 オプション ボタンをクリックし、[Select] ボタンをクリックして、VRF オブジェクトを選択します。

必要に応じて、[Show VRFs with] および [matching] フィールドを使用して、[VRF Name]、[Provider]、[Route Distinguisher]、または [Route Target] で検索することによって表示する VRF オブジェクトを制限できます。



(注) Prime Provisioning リポジトリに VRF オブジェクトを追加する方法については、「新しい VRF オブジェクトの作成」(P.5-17) を参照してください。

ステップ 5 リンク用の PE デバイスを選択するには、[Select PE] リンクをクリックします。

[Select PE Device] ウィンドウが表示されます。

ステップ 6 オプション ボタンをクリックし、[Select] ボタンをクリックして、PE を選択します。

必要に応じて、[Show PEs with] および [matching] フィールドを使用して、表示する PE デバイスを制限できます。

このステップでは、ステップ 4 および 5 で選択した VRF オブジェクトをいずれの PE デバイスに展開するかを指定します。



(注) VRF オブジェクトおよび PE デバイスは同じプロバイダーに属している必要があります。このため、Prime Provisioning では、表示する PE のリストをリンクに対して選択した VRF オブジェクト内で指定したのと同じプロバイダーの PE に制限します。

PE を選択した後、[RD IP Address Value] 列にメッセージが表示されます。場合によっては、IP アドレスを入力するためのテキスト フィールドが表示されます。これは、次の手順で説明します。

ステップ 7 リンクに関連付けられるテンプレート データ ファイルを選択するには、[Add Template] リンクをクリックします。

[Add/Remove Templates] ウィンドウが表示されます。これは、データ ファイルを選択し、末尾や先頭への追加などの操作の指定を行うための標準的な Prime Provisioning ウィンドウです。

Prime Provisioning でのテンプレートの操作の詳細については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。[Add/Remove Templates] ウィンドウ使用の詳細については、「サービス要求でのテンプレートの使用」(P.9-26) を参照してください。

ステップ 8 リンクの [Address Family] ドロップダウン リストから適切な項目を選択して、アドレス スキームを指定します。

選択できる基準は、次のとおりです。

- IPv4
- IPv6
- IPv4 および IPv6

IPv4 および IPv6 オプションを使用すると、VRF オブジェクトが IPv4 と IPv6 の両方の設定を使用して展開されます。

ステップ 9 設定上適切であれば、RD IP アドレスを [RD IP Address Value] 列のテキスト フィールドに入力します。また、[Select Loopback] リンクをクリックして、サービス要求で使用される PE デバイスのループバック IP アドレスを選択できます。

使用方法に関する注釈：

- [RD IP Address Value] フィールドの内容と振る舞いは、次のように、サービス要求で使用されている VRF オブジェクトに RD フォーマットと RD 属性がどのように指定されていたかによって異なります。

- VRF オブジェクトで RD フォーマットが RD_IPADDR のように設定されており、RD 属性に対して自動選択がオンになっている場合、[RD IP Address Value] 列には手動で RD IP アドレス値を入力するテキストフィールドが表示されます。あるいは、サービス要求で使用される PE デバイスのループバック IP アドレスを選択することもできます。RD は、各プロバイダーの RD プールから選択した VPN ID にこの IP アドレスを追加することで形成されます。入力した IP アドレスは、Prime Provisioning によって検証されます。基本的な IPv4 アドレスが使用できます。ネットワーク プレフィックスは許可されません。
 - VRF オブジェクトで RD フォーマットが RD_IPADDR のように設定されており、ユーザが手動で RD 属性の RD IP アドレスを入力した場合、[RD IP Address Value] 列に「RD IP Address Manual」と表示されます。この場合、IP アドレスを入力しないでください。
 - VRF オブジェクトで RD フォーマットが RD_AS のように設定されており、RD 属性に対して自動選択がオンになっていたか、値が手動で入力された場合、[RD IP Address Value] 列に「RD AS Format」と表示されます。これらのいずれの場合でも値は入力しません。
- テキストフィールドに入力した IP アドレスを使用する RD を使用して VRF サービス要求を展開すると、[RD IP Address Value] フィールドはディセーブルになり変更できません。[RD IP Address Value] を変更する必要がある場合は、VRF サービス要求をデコミッション、削除、および再展開する必要があります。

- ステップ 10** VRF サービス要求に追加リンクを設定する場合、[Add Link] ボタンをクリックし、リンクごとにステップ 4 からステップ 9 までを繰り返します。
- ステップ 11** VRF サービス要求のリンクの設定が完了したら、[Save] をクリックして VRF サービス要求を保存します。
- [Service Requests] ウィンドウが表示され、[Job ID]、[State]、[Type]、および他の属性が表示された VRF サービス要求が表示されます。VRF サービス要求の初期状態は、[Requested] です。
- ステップ 12** VRF サービス要求を展開するには、「[VRF サービス要求の展開](#)」(P.5-26) を参照してください。

VRF サービス要求の展開

VRF サービス要求を展開するには、次の手順を実行します。

- ステップ 1** [Service Requests] ウィンドウで、展開する VRF サービス要求を選択します。
- ステップ 2** [Deploy] ボタンをクリックして、ドロップダウン リストから [Deploy] を選択します。
- [Deploy Service Request task] ウィンドウが表示されます。
- ステップ 3** タスク パラメータを目的の値に設定し、[Save] ボタンをクリックします。
- 展開タスクをすぐに開始するには、デフォルトをそのまま使用し、[Save] をクリックします。[Service Request] ウィンドウが再表示され、VRF サービス要求が [Deployed] 状態に移行します。

展開した VRF サービス要求の状態を確認する方法のステップについては、「[IOS から IOS XR への PE デバイスの移行](#)」(P.5-103) および「[サービス要求のモニタリング](#)」(P.8-11) を参照してください。

VRF サービス要求の変更

VRF サービス要求のリンクを追加するか、既存のリンク属性を変更するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択して、[Service Request Manager] ウィンドウにアクセスします。
- ステップ 2** [Service Requests] ウィンドウで VRF サービス要求を選択し、[Edit] をクリックします。
[VRF Service Request Editor] ウィンドウが表示されます。
- ステップ 3** 必要に応じて VRF サービス要求の属性を変更します。
-  **(注)** どの MPLS VPN リンクにも関連付けられていない VRF サービス要求のリンクのみを変更できます。MPLS VPN リンクに関連付けられている VRF のサービス要求のリンクを変更しようとすると、Prime Provisioning は VRF サービス要求の保存中にエラーを出します。
-
- ステップ 4** [Save] をクリックして編集内容を保存します。
-

VRF サービス要求のデコミッションと削除

VRF サービス要求は、Prime Provisioning の他のサービス要求と同じようにデコミッションおよび削除されます。



- (注)** MPLS サービス要求で参照されている VRF オブジェクトを持つ VRF サービス要求に何らかのリンクが存在する場合、VRF サービス要求のデコミッションは行えません。
-

VRF サービス要求をデコミッションするには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択して、[Service Requests Manager] ウィンドウにアクセスします。
- ステップ 2** [Service Requests] ウィンドウで VRF サービス要求を選択し、[Decommission] ボタンをクリックします。
[Confirm Request] ウィンドウが表示されます。
- ステップ 3** [OK] をクリックして確定します。
[Service Request] ウィンドウが表示され、[DELETE] 操作タイプの VRF サービス要求が表示されます。
- ステップ 4** [DELETE] 操作タイプのサービス要求を展開して、サービス要求が正常にデコミッションされるようにします。
-

VRF サービス要求の VRF オブジェクト名での検索

VRF オブジェクト名で Prime Provisioning リポジトリ内の VRF サービス要求を検索および表示するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択して、[Service Requests Manager] ウィンドウにアクセスします。
- ステップ 2** [Show Services with] ドロップダウン リストで [VRF Object Name] を選択します。

- ステップ 3** 必要に応じて、[matching] および [of Type] フィールドを設定します。
VRF サービス要求のみを検索するには、[of Type] フィールドで [VRF] を選択します。
- ステップ 4** [Find] をクリックして、指定した VRF オブジェクト名を持つサービス要求を検索します。

展開された VRF サービス要求によって生成されたコンフィグレットの表示

展開された VRF サービス要求によって生成されたコンフィグレットを表示するには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択して、使用可能なサービス要求を表示します。
- ステップ 2** 該当するチェックボックスをオンにして、関連付けられたコンフィグレットを表示する VRF サービス要求を選択します。
- ステップ 3** [Details] ボタンをクリックします。
[Service Request Details] ウィンドウが表示されます。
- ステップ 4** [Configlets] ボタンをクリックします。
[Service Request Configlets] ウィンドウが表示されます。このウィンドウには、コンフィグレットが生成されたデバイスのリストが表示されます。
- ステップ 5** デバイスに対して生成されたコンフィグレットを表示するには、デバイスを選択し、[View Configlet] ボタンをクリックします。
デフォルトでは、直近で生成されたコンフィグレットが表示されます。
-  **(注)** コンフィグレットが IOS XR デバイスで展開される場合は、コンフィグレットを XML または CLI フォーマット、あるいはその両方のフォーマットで表示するオプションがあります。この振る舞いについての詳細は、「[IOS XR デバイスでのコンフィグレットの表示](#)」(P.8-6) を参照してください。
- ステップ 6** 必要に応じて、作成時間に基づいてデバイスのコンフィグレットを表示できます。サービス要求に対してコンフィグレットが生成された時間に基づいて特定のコンフィグレットを表示するには、[Create Time] リストで目的の作成時間を選択します。
- ステップ 7** VRF コンフィグレット データの表示が完了したら、[OK] をクリックします。

MPLS VPN サービス要求とポリシーでの VRF の使用

すでに展開された VRF オブジェクトは、MPLS VPN サービス要求およびサービス ポリシー内で使用できます。

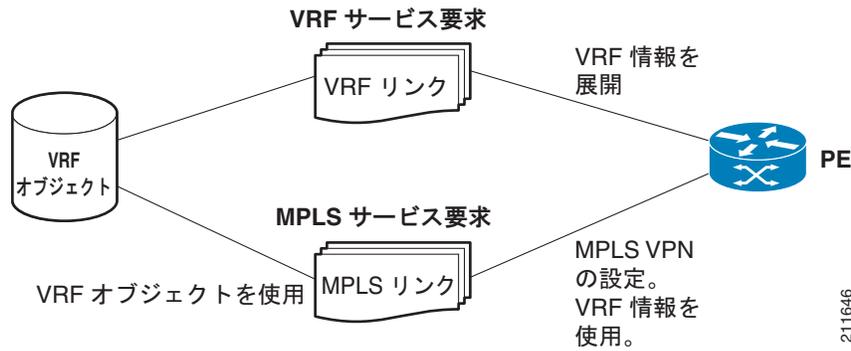


- (注)** 独立 VRF の関連付けは、MVRFCPE ベースのサービス ポリシーとサービス要求ではサポートされていません。

VRF オブジェクト、サービス要求、および PE デバイスの関係

図 5-2 に、VRF オブジェクト、MPLS サービス要求、VRF サービス要求、および PE デバイス間の関係を示します。次の手順で説明する概念を理解するために、この図を参照してください。

図 5-2 VRF オブジェクト、VRF サービス要求、MPLS VPN サービス要求、および PE



MPLS VPN サービス要求内への VRF オブジェクトの指定

VRF オブジェクトは、MPLS VPN サービス要求の作成中に VRF および VPN 属性を設定するときに選択できます。この段階で、VPN 属性を個々に設定するか（IP Solution Center の以前のリリースと同様）、既存の VRF オブジェクトを使用することができます。後者の場合、VPN および VRF のデータが VRF オブジェクトから MPLS VPN リンクに「継承」されます。VRF オブジェクトは、展開されない場合と、展開される場合があります。VRF オブジェクトが展開されない場合、Prime Provisioning はそれを自動的に展開します。MPLS VPN サービス要求での VRF オブジェクトの機能の詳細については、「MPLS サービス要求で VRF オブジェクトを使用する際の注意事項」(P.5-31) を参照してください。

VRF オブジェクトを使用して MPLS VPN サービス要求を作成するには、次の手順を実行します。

- ステップ 1** 既存の MPLS VPN サービス要求を作成または使用して、VRF および VPN 属性を定義する時点までワークフローに従う必要があります。これは、[MPLS Link Editor – VRF and VPN] ウィンドウで実行します。



(注) MPLS VPN サービス要求ワークフロー内でこのウィンドウに到達する方法については、このマニュアルの関連する項を必要に応じて参照してください。

- ステップ 2** この MPLS VPN リンクで VRF オブジェクトを使用しない場合は、[Use VRF Object] をオフのままにします。
この場合、MPLS サービス要求で通常行うように VPN に対して属性を設定します。このステップについては、このマニュアルの他の項で説明します。
- ステップ 3** MPLS VPN リンクで VRF オブジェクトを使用するには、[Use VRF Object] チェックボックスをオンにします。
非表示の [BGP Multipath Load Sharing] を除く、VPN および VRF の標準属性すべておよび [VRF Object] 属性が表示されます。
- ステップ 4** VRF オブジェクトを選択するには、[VRF Object] 属性の右側にある [Select] ボタンをクリックします。

[Select Independent VRF] ウィンドウが表示されます。

[Select Independent VRF] ウィンドウには、PE で展開された VRF オブジェクトすべてがその RD 値、プロバイダーおよび CERC 情報とともに一覧表示されます。

ステップ 5 一意のルート識別子機能をイネーブルにするには、[Unique RD] チェックボックスをオンにします。



(注) [Unique RD] 機能では、MPLS サービス要求ごとに 1 つの MPLS VPN リンクに制限されています。[Unique RD] オプションを選択する場合は、サービス要求に 1 つの MPLS VPN リンクだけが存在するようにします。

固有 RD 機能をイネーブルにする場合は、次の使用例のシナリオに留意してください。

- 選択した VRF がいずれのデバイスでも展開されていない場合は、VRF サービス要求が選択した VRF および PE デバイスに対して作成されます。
- 選択した VRF がその PE デバイスでは展開されていないが、異なる PE デバイスで展開されている場合は、新しい VRF オブジェクト（選択した VRF のコピー）が作成され、VRF サービス要求が新しく作成された VRF および PE デバイスに対して作成されます。
- 選択した VRF が PE デバイスだけで展開されている場合は、何も実行されません。この場合、自動で一意になります。
- 選択した VRF が PE デバイスおよび他のいくつかのデバイスでも展開されている場合は、VRF オブジェクトの新しいコピーが更新された名前で作成され、VRF サービス要求が新しく作成された VRF および PE デバイスに対して作成されます。
- 名前は同じでも RD が異なる 2 つの VRF を作成することができます。

ステップ 6 目的の VRF オブジェクトを選択し、[Select] ボタンをクリックします。



(注) その後の Prime Provisioning による VRF オブジェクト選択の管理方法については、この手順の後の「MPLS サービス要求で VRF オブジェクトを使用する際の注意事項」(P.5-31) を参照してください。

ステップ 7 [Select] ボタンをクリックして、VRF オブジェクトの選択を確認し、[MPLS Link Editor – VRF and VPN] ウィンドウに戻ります。

ステップ 8 BGP マルチパス ロード シェアリングを設定するには、[BGP Multipath Load Sharing] チェックボックスをオンにします。

追加属性の設定については、「BGP マルチパス ロード シェアリングおよび最大パス設定」(P.5-80) を参照してください。



(注) [Force Modify Shared Multipath Attributes] 属性を使用して、他のリンクによって使用される共有 VRF 属性の強制変更をイネーブルにします。このフィールドは持続されません。

ステップ 9 テンプレートまたはデータ ファイルをサービス要求に関連付ける場合は、[Next] ボタンをクリックします。

[Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。テンプレートをサービス要求に関連付ける手順、およびこの機能のこのウィンドウでの使用方法について

では、第 9 章「[テンプレートおよびデータ ファイルの管理](#)」を参照してください。サービス要求のテンプレートおよびデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じて [Service Request Editor] ウィンドウに戻ります。

ステップ 10 テンプレートを追加しなかった場合は、[MPLS Link Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 11 [Save] ボタンをクリックして、VRF オブジェクトを使用した MPLS VPN サービス要求の作成を完了します。

[Service Requests] ウィンドウが表示され、サービス要求が [Requested] 状態になり展開可能になっていることを示します。

MPLS サービス要求で VRF オブジェクトを使用する際の注意事項

VRF オブジェクトを MPLS VPN サービス要求で使用する場合は、次の点に注意してください。

- 選択した VRF オブジェクトが PE デバイスで展開されていない場合は、Prime Provisioning は新しい VRF サービス要求を選択した VRF オブジェクトおよび PE デバイスで作成し、現在の MPLS VPN サービス要求展開プロセスの一部として展開します。
- MPLS VPN サービス要求で選択した VRF オブジェクトが PE デバイスに展開されていないが、VRF サービス要求が [Requested] 状態または何らかの障害状態にある場合、Prime Provisioning は MPLS VPN サービス要求の一部として VRF サービス要求を展開しようとします。
- VRF サービス要求が作成された MPLS VPN サービス要求をデコミッションする場合、Prime Provisioning は VRF サービス要求を自動的に削除しません。コンフィギュレーションをデバイスから削除するために、ユーザはこのような VRF サービス要求をデコミッションして展開する必要があります。
- VRF コンフィギュレーションが選択されたとき、VRF 関連の情報はデバイスにプロビジョニングされません。VRF 名は、インターフェイスでの ip vrf forwarding や BGP、OSPF、EIGRP でのアドレス ファミリ コンフィギュレーションなどすべての MPLS VPN コンフィギュレーション コマンドで使用されます。

VRF オブジェクト名による MPLS VPN サービス要求の検索

VRF オブジェクト名で Prime Provisioning リポジトリ内の VRF サービス要求を検索および表示するには、次の手順を実行します。

ステップ 1 [Operate] > [Service Requests] > [Service Request Manager] を選択して、[Service Requests Manager] ウィンドウにアクセスします。

ステップ 2 [of Type] ドロップダウン リストで [VRF] を選択します。

ステップ 3 必要に応じて、[matching] および [of Type] フィールドを設定します。

MPLS VPN サービス要求だけを検索するには、[of Type] フィールドで [MPLS VPN] を選択します。

ステップ 4 [Find] ボタンをクリックして、指定した VRF オブジェクト名に関連付けられている MPLS VPN サービス要求を検索します。

MPLS VPN サービス ポリシー内への VRF オブジェクトの指定

MPLS VPN ポリシーの定義中に、VRF オブジェクトを選択できます。これは、[MPLS Policy Editor – VRF and VPN Membership] ウィンドウでの MPLS VPN ポリシー ワークフロー中に実行されます。

[VRF Object] 属性を使用する手順は、「[MPLS VPN サービス要求内への VRF オブジェクトの指定 \(P.5-29\)](#)」で説明した手順と似ています。これらの属性の使用の詳細については、該当する項を参照してください。

MPLS ポリシーに VRF オブジェクトを選択する場合は、このポリシーを使用する MPLS VPN サービス要求によって VRF オブジェクトはその後使用されます。標準の Prime Provisioning ポリシー使用に従って、[VRF Object] 属性の隣にある [Editable] チェックボックスをオンにして、ポリシーに基づいたサービス要求がポリシーに指定された同じ VRF オブジェクトを確実に使用するようになります。



(注) ポリシーに独立 VRF オブジェクト機能を使用していない場合は、[MPLS Policy Editor – VRF and VPN Membership] ウィンドウにある VRF および VPN 属性を設定する必要があります。詳細については、「[VRF および VPN の情報の定義 \(P.5-76\)](#)」を参照してください。

既存の MPLS VPN サービス要求から VRF オブジェクト モデルへの移行

Prime Provisioning には、従来の MPLS VPN サービス要求を独立 VRF モデルに移行するための移行スクリプトがあります。移行スクリプトでは、1 つ以上の MPLS VPN サービス要求 ID 番号を入力として受け入れて、各サービス要求に対して適切な VRF オブジェクトおよび VRF サービス要求を作成します。このスクリプトは \$PRIMEP_HOME/bin ディレクトリにあります。スクリプトおよびその構文は、次のとおりです。

```
runMplsSRMigration srid1 [srid2] [srid3] ...
```

[srid1] は最初の MPLS VPN サービス要求 ID であり、[srid2] は 2 番目のサービス要求です。以降同様に続きます。

Prime Provisioning は、スクリプトに渡された各 MPLS VPN サービス要求に対して次のタスクを実行します。

- サービス要求に対して定義した VPN および VRF 属性に基づいて VRF オブジェクトを作成します。
- すべての VPN プロパティを VRF オブジェクトにコピーします。
- MPLS VPN リンクで選択した VRF オブジェクトおよび PE で VRF サービス要求を作成します。
- VRF オブジェクトを指すように MPLS VPN リンクを変更します。
- VRF サービス要求および MPLS サービス要求でコンフィギュレーション監査を実行して、移行の妥当性を確認します。

MPLS VPN での IPv6 および 6VPE サポート

この項では、IPv6 の概要と、MPLS VPN での 6VPE のサポートを説明します。



(注) Prime Provisioning GUI で MPLS VPN 機能がどのように実装およびサポートされているかについては、提供されている参照に示されているように、このマニュアルの該当する項を参照してください。

IPv6 および 6VPE の概要

Prime Provisioning MPLS VPN 管理アプリケーションは、Prime Provisioning Layer 3 VPN サービスの IPv6 VPN および 6VPE をプロビジョニングするために、IOS および IOS XR を実行しているシスコ デバイスの設定および管理をサポートしています。



(注) IOS および IOS XR バージョン、および IPv6 をサポートしているハードウェア プラットフォームの最新情報については、『Cisco Prime Provisioning 6.3 Release Notes』を参照してください。

ここでは、IPv6 および 6VPE テクノロジーの概要について説明します。Prime Provisioning がどのように IPv6 をサポートしているかについての概要は、「IPv6 および 6VPE の MPLS VPN サポート」(P.5-35) を参照してください。

Internet Protocol Version 6 (IPv6)

IPv6 は、世界中で広く展開され、使用されているインターネット プロトコルである IPv4 に代わるものとして設計された IP プロトコルの一種です。IPv6 はネットワーク アドレスのビット数を 32 ビット (IPv4 の場合) から 128 ビットに 4 倍に増やすか、およそ 3.4×10^{38} のアドレス可能なノードにします。これにより、世界中のすべてのネットワーク デバイスにグローバルに一意的な IP アドレスを十分に確保することができます。シスコは、IPv6 を Cisco IOS および IOS XR ソフトウェアに導入しています。つまり、現在のシスコ ベースのネットワークでは IPv6 を使用でき、IPv4 と IPv6 の間の共存と並列処理を行えることから、ネットワーク管理者は必要に応じて IPv6 を設定できるようになります。多くの人は IPv6 をより大規模なグローバル インターネットを構築するための 1 つの方法と見なしていますが、IPv6 を使用しても、イントラネットおよび他の同様のアプリケーション用に VPN を作成しなくて済むわけではありません。

IPv6 over MPLS バックボーンを展開するために、さまざまな展開方法を使用できます。現在、サービス プロバイダーは現在の IPv4 MPLS バックボーンに変更を加えずに IPv6 をサポートする 2 種類の方法を提供しています。

- **6PE。** MPLS を介した Cisco IOS IPv6 プロバイダー エッジ ルータ (6PE)。6PE を使用することで、IPv6 ドメインは IPv4 クラウドを介してお互いに通信できるようになります。IPv6 ドメインごとに 1 つの IPv4 アドレスのみが必要であり、明示的にトンネルを設定する必要はありません。6PE 技術により、サービス プロバイダーは IPv4 MPLS を介したグローバルな IPv6 到達可能性を提供できるようになります。これにより、他のすべてのデバイスに対して 1 つの共有ルーティング テーブルを使用できるようになります。
- **6VPE。** MPLS を介した Cisco IPv6 VPN プロバイダー エッジ ルータ (6VPE)。これにより、IPv6 ネットワークに関する RFC 2547bis と同様の VPN モデルが容易になります。6VPE は、通常の IPv4 MPLS VPN プロバイダー エッジ とほぼ同じですが、Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) 内に IPv6 サポートが追加されています。これは、VPN メンバー デバイス用に、論理的に分割されたルーティング テーブル エントリを提供します。

Prime Provisioning の MPLS VPN は 6VPE を使用して、IPv6 over a MPLS バックボーンを展開するためのレイヤ 3 VPN サービスを管理します。

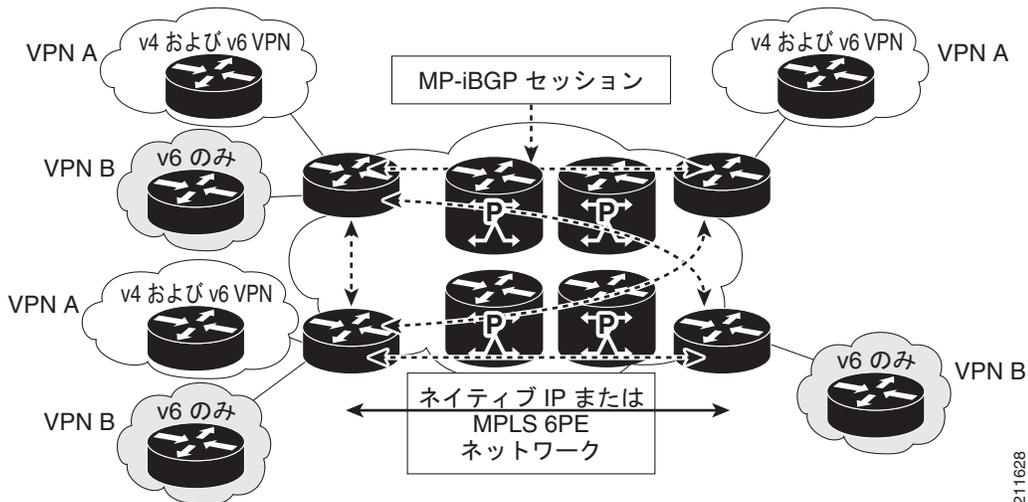
IPv6 VPN プロバイダー エッジ ルータ (6VPE)

シスコの 6VPE ソリューションは、IPv6 アドレッシングを制限することなく、拡張可能な方法で、IPv6 VPN サービスを簡単に展開します。これは、適切に制御されたサービス プロバイダーの IPv4 バックボーンまたはカスタマー ネットワークを損ないません。VPN サービス 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サービス プロバイダーにとって重要な問題の 1 つです。IPv4 VPN カスタマーの場合、IPv6 VPN サービスは IPv4 の MPLS VPN とまったく同じです。

IPv6 MPLS VPN サービス モデルは、IPv4 MPLS VPN のモデルと似ています。IPv4 バックボーンを介して MPLS IPv4 VPN サービスをすでに展開したサービス プロバイダーは、コア ルータに何も変更を行う必要なく、PE ルータの IOS バージョンとデュアルスタック設定を更新することで、同じ IPv4 バックボーンを介した IPv6 MPLS VPN サービスを展開できます。IPv4 サービスは IPv6 サービスと同時に提供できます。図 5-3 に示されているように、PE-CE リンクは IPv4 リンク、IPv6 リンク、または IPv4 リンクと IPv6 リンクの組み合わせにすることができます。

図 5-3 6VPE の展開



IPv6 VPN サービスは、IPv4 の MPLS VPN とまったく同じです。6VPE は、IPv4 の MPLS VPN と同じアーキテクチャ機能を提供します。これは、IPv6 VPN を提供し、同じコンポーネントを使用します (以下を参照)。

- Multiprotocol BGP (MP-BGP; マルチプロトコル BGP) VPN アドレス ファミリ
- ルート識別子
- VPN ルーティングおよび転送 (VRF) インスタンス
- Site of Origin (SOO)
- 拡張コミュニティ
- MP-BGP

6VPE ルータは、サポートされているルーティング プロトコルのいずれかを使用して、IPv4 または IPv6 ルーティング情報を交換し、ネイティブの IPv4 および IPv6 VRF インターフェイスを介した各高速スイッチング CEF または分散 CEF パスを使用して IPv4 および IPv6 トラフィックを切り替えます。6VPE ルータはマルチプロトコル BGP を使用して MPLS ドメイン内の他の 6VPE ルータで到着可能性情報を交換し、ドメイン内の他の P および PE デバイスと共通の IPv4 ルーティング プロトコル (OSPF または IS-IS のなど) を共有します。分割されたルーティング テーブルは、IPv4 および IPv6 スタックに保持されます。エッジ LSR での着信カスタマー IPv6 パケットには、次の MPLS ラベルの階層がインポートされます。

- LDP により分散される iBGP ネクスト ホップの外部ラベル (IGP ラベル)
- MP-BGP によって分散される IPv6 プレフィックスの内部ラベル (VPN ラベル)。

6VPE VRF インターフェイスの着信カスタマー IPv6 パケットは、MPLS ラベルに基づいてサービス プロバイダーの IPv4 コア内に透過的に転送されます。これにより、IPv6 パケット トンネルの必要がなくなります。MPLS コア内の P ルータは IPv6 ラベル付きパケットを切り替えていることを認識しません。

IPv6 および 6VPE の MPLS VPN サポート

この項では、MPLS VPN の管理アプリケーションが IPv6 および 6VPE をどのようにサポートするかを概説します。

ここで説明されている Prime Provisioning サービスの設定については、「[Prime Provisioning サービスの設定](#)」(P.5-4) を参照してください。

IPv6 用の IOS および IOS XR サポート

IPv6 サービスは、IOS と IOS XR のサポートされているバージョンと、PE および CE ロールの両方のハードウェア プラットフォームについて、Prime Provisioning で使用できます。



(注)

IOS および IOS XR バージョン、および IPv6 をサポートしているハードウェア プラットフォームの最新情報については、『[Cisco Prime Provisioning 6.3 Release Notes](#)』を参照してください。

特に明記されていない限り、次の項で説明する IPv6 機能は、IOS デバイスと IOS XR デバイスの両方でサポートされます。

インベントリおよびデバイス管理

MPLS VPN サービスをアクティブにするには、Prime Provisioning が管理するデバイス、プロバイダー、カスタマーなどの事前設定情報を「認識」できるように Prime Provisioning を設定する必要があります。IPv6 および 6VPE のインベントリおよびデバイス管理をサポートする Prime Provisioning 機能は次のとおりです。

Discovery

- Prime Provisioning インベントリ マネージャは、Prime Provisioning リポジトリへの 6VPE デバイスの一括インポートをサポートしています。

Collect Config Task

- [Collect Config task] は、OS タイプとバージョン情報を取得します。デバイスが Cisco 12000 シリーズ ルータ、Cisco CRS-1 Carrier Routing System または ASR 9000 シリーズ ルータで、IOS XR を実行している場合、このデバイスに 6VPE サポートのマークが付けられます (デフォルトでは、[Create PE Device] ウィンドウの [6VPE] チェックボックスは XR デバイスに対してチェックされます)。[Create PE Device] ウィンドウの [6VPE] チェックボックスを手動でオンにして、N-PE デバイスを IOS デバイス用の 6VPE として指定する必要があります。
- IPv6 サービスを使用する IOS デバイスの Collect Config task は、IPv4 IOS デバイスの場合と同じです。

Device Configuration

- IPv6 アドレス指定を使用する 6VPE デバイスは、Prime Provisioning GUI で作成および管理できます。

- [Create PE Device] ウィンドウの [6VPE] チェックボックスをオンにして、6VPE として N-PE デバイスを指定する必要があります。IOS および IOS XR デバイスの IPv6 サービスは、このチェックボックスをオンである場合に、MPLS および VRF サービス要求でのみ使用できます。



(注) Prime Provisioning GUI でデバイスの [6VPE] チェックボックスがオンされているが、そのデバイスが実際には IPv6 サービスをサポートしていない場合、そのデバイスに展開される MPLS VPN サービス要求は、[Failed Deploy] 状態になります。

- [Interface Attributes] ウィンドウの列は、IPv6 アドレスを示します。複数のインターフェイスを選択して、IPv6 アドレスを一括変更することはできません。[IPv6 Address] 列は編集できません。
- [Edit Device Interface] ウィンドウには、インターフェイス上に IPv6 アドレスが表示されます。IPv4 と IPv6 の両方のアドレスを含むデュアル スタック インターフェイスの場合は、両方のアドレスが表示されます。
- Prime Provisioning は、IOS XR PE デバイスおよび IOS 6VPE デバイスの PE インターフェイスで複数の IPv6 アドレスをサポートします。
- [Create CPE Device] ウィンドウには、インターフェイス上に IPv6 アドレスが表示されます。IPv4 と IPv6 の両方のアドレスを含むデュアル スタック インターフェイスの場合は、両方のアドレスが表示されます。
- 既存の Create Interface 機能を使用して、IPv6 インターフェイスを作成することはできません。現在、この画面ではデバイス設定を変更しないまま、リポジトリ内のみインターフェイスを作成できます。この機能は、IPv6 アドレスをサポートしません。デバイスでの IPv6 インターフェイスの作成は、MPLS VPN サービス展開でサポートされます。

VPN の作成および設定

IPv6 および 6VPE の VPNPrime Provisioning ワークフローの変更はありません。

IPv6 のマルチキャスト VPN サポートは、このリリースの IOS デバイスでは使用できません。現在、これは、サポートされている IOS XR デバイスだけで使用できます。詳細については、次の項を参照してください。

- 「[IOS および IOS XR デバイスでのマルチキャスト ルーティング](#)」(P.5-39)
- 「[IPv6 でのマルチキャスト サポート \(IOS XR 限定\)](#)」(P.5-40)

独立 VRF オブジェクトのサポート

Prime Provisioning では、独立 VRF オブジェクトに VPN および VRF の情報を指定できます。このオブジェクトは、PE デバイスに配置され、さらに MPLS VPN サービス要求によって MPLS VPN リンクに関連付けられます。Prime Provisioning は、VRF オブジェクトの IPv4、IPv6 デュアルスタック アドレッシングをサポートします。

独立 VRF オブジェクトの使用および管理の詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。

リソース プール

Prime Provisioning はリソース プールを使用して、VLAN、VCID、および IP アドレスなどの重要なパラメータをサービスのプロビジョニング中に割り当てます。IPv6 アドレス プールは、本リリースではサポートされていません。

MPLS VPN サービス プロビジョニング

Prime Provisioning MPLS VPN の管理アプリケーションは、IPv6 プロバイダー エッジルータ (6VPE) への IPv6 レイヤ 3 VPN のプロビジョニングをサポートします。Prime Provisioning では 6VPE に次を設定する機能を使用できます。

- 6VPE で IPv6 アドレス指定を使用する (オプションで、IPv4、IPv6、または両方の IPv6+IPv4 アドレス)。
- CE デバイス上の 6VPE 接続インターフェイスにスタティック ルートを割り当てる。
- MP-BGP ピアリングをターゲット 6VPE でイネーブルにする。
- 接続対象を再配布する (必要な場合)。

次の項では、MPLS VPN ポリシー定義、サービス要求作成、Prime Provisioning で IPv6 および 6VPE をサポートするサービス要求監査の機能について説明します。

MPLS VPN ポリシー

IPv6 および 6VPE の MPLS VPN ポリシー定義のサポートを次に示します。

- MPLS VPN サービス ポリシー設計では、次のポリシー タイプの 6VPE ルータで IPv6 を設定できます。
 - Regular : PE-CE (管理対象外 CE あり)
 - 管理対象外 CE と非 CE のシナリオの両方が IPv6 でサポートされています。
- サービス ポリシーは、次のアドレス設定スキームをサポートします。
 - IPv4
 - IPv6
 - デュアルスタック (IPv4 と IPv6 の両方)
- MPLS Policy Editor の [IP Numbering Scheme] フィールド : [IP Address Scheme] ウィンドウを使用して、サポートされる各アドレス スキームを指定できます。
- IPv4 ルーティングと IPv6 ルーティングはそれぞれ独立しています。Prime Provisioning GUI では、IPv4 および IPv6 に同じまたは異なるルーティング プロトコルを入力できます。
- ポリシーを設定する場合、IPv6 アドレス設定スキームに対して次の PE と CE 間のルーティング プロトコルがサポートされます。
 - スタティック
 - BGP
 - EIGRP (IOS XR デバイスでサポートされるのみ)
 - なし
- IPv6 マルチキャスト VPN は IOS 6VPE 設定ではサポートされません。IOS XR デバイスのマルチキャスト VPN のサポートについては、「[IOS および IOS XR デバイスでのマルチキャスト ルーティング](#)」(P.5-39) を参照してください。
- IPv6 の有効性をチェックします。IPv6 アドレス フィールドに入力されるアドレスに対して、次のチェックが実行されます。
 - アドレスはそれぞれが「:」(コロン) で区切られた、16 ビットの指定された 8 つの連続するブロックにすることができます。各 16 ビットブロックは、4 桁の 16 進数 16 として指定できます。たとえば、21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A です。

- 先行ゼロは各 16 進数のブロックで省略できます。前の例の変更された有効なアドレスを示します。前の例は、21DA: D3: 0:2F3B: 2AA: FF: FE28: 9C5A です。
- 連続する「0:」のブロックがある場合、「::」に置き換えられます。たとえば、21DA:D3:0:0:0:FF:FE28:9C5A は 21DA:D3::FF:FE28:9C5A のように表示することができます。
- 文字列の「::」はアドレスに複数回表示できません。たとえば、21DA:0000:0000:2F3B:0000:0000:0000:9C5A は次のように表示することができます。21DA::2F3B:0000:0000:0000:9C5A または 21DA:0000:0000:2F3B::9C5A。ただし、21DA::2F3B::9C5A とは表示されません。

MPLS VPN サービス ポリシーの定義については、「[MPLS VPN サービス ポリシー](#)」(P.5-42) を参照してください。

MPLS VPN サービス要求

IPv6 および 6VPE をサポートするための MPLS VPN ポリシー作成時の属性設定は、サービス要求作成のワークフローの対応するウィンドウに継承されます。オプションが、ポリシー作成中に編集可能として設定された場合、サービス要求作成時にこれらを変更できます。

- MPLS Link Attribute Editor の [IP Numbering Scheme] フィールド : [IP Address Scheme] ウィンドウを使用して、サポートされる各アドレス スキームを指定できます。
- IPv4 および IPv6 のアンナバード方式は、IOS XR デバイスではサポートされません。IOS XR (または IOS 6VPE) デバイスを選択し、[IP Addressing Scheme] ウィンドウに移動すると、次のオプションが表示されます。
 - IPv4 Numbered
 - IPV6 Numbered
 - IPV4+IPV6 Numbered
- 標準 PE-CE MPLS サービスの一部として、必須 VRF は PE デバイス上で設定されます。CE 側インターフェイスは、IPv6 アドレスで設定され、インターフェイスが、VRF に割り当てられます。PE-CE ルーティング情報とともに、BGP での IPv6 アドレス ファミリ設定が設定されます。
- PE インターフェイスが (IPv4 と IPv6 の両方のアドレス含む) デュアル スタック構成の場合、IPv4 と IPv6 両方のルーティング情報を個別に入力できます。GUI によって、既存の IPv4 ルーティング情報に加えて IPv6 ルーティング情報を入力するための手順が示されます。
- Prime Provisioning はサービス要求に含まれない CE デバイスのシナリオをサポートします。本リリースでは、サービス要求にアンナバード CE デバイスが存在する状況もサポートします。後者の場合、サービス プロビジョニングのコンフィグレットは生成されますが、CE デバイスにロールされません。
- 6VPE サービス要求は変更できます。
- PE デバイスが IOS XR デバイスの場合、すべての設定操作は IOS XR インターフェイスを使用して実行されます。
- IOS XR 6VPE デバイスでは、生成されるすべてのコンフィグレットは XML 形式です。IOS XR のバージョンが異なれば、異なる XML コンフィグレットが生成されます。ただし、設定は、XML スキーマでの変更を除いて、ほとんど同じです。
- IOS 6VPE デバイスでは、すべてのコンフィギュレーションは XML 形式で生成されます。

MPLS VPN サービス要求の作成については、本書の「[MPLS VPN サービス要求](#)」(P.5-83) およびこれ以降の章を参照してください。

MPLS サービス要求監査

L3 VPN 機能監査は、IPv6 VPN (IPv6 アドレスおよび 6VPE デバイス) をサポートします。これには、PE デバイスの VRF ルートテーブルでのリモート CE へのルートチェックが含まれます。サービス要求の監査の詳細については、「[監査レポートのサービス要求の表示](#)」(P.8-4) を参照してください。

IOS および IOS XR デバイスでのマルチキャスト ルーティング

IOS XR デバイスのマルチキャスト VRF 展開は、IPv4、IPv6、IPv4+IPv6 サービスでサポートされています。現在、IOS XR マルチキャストは IOS XR バージョンの指定されたバージョンでのみサポートされています。このリリースでサポートされている IOS XR バージョンのリストについては、『[Cisco Prime Provisioning 6.3 Release Notes](#)』を参照してください。

この項では、Prime Provisioning が IOS XR デバイスでどのようにマルチキャストルーティングをサポートするかについて説明します。この機能をサポートする GUI ([Create VPN] ウィンドウ) の変更はありません。IOS XR XML は、マルチキャストルーティングコマンドをサポートしないため、対応する IOS XR CLI を使用してコンフィギュレーションがデバイスにプッシュされます。

次の項では、関連する IOS コマンドと対応する IOS XR コマンドの例を示して、マルチキャストルーティングを有効にします。

IOS コマンド

次に、IOS の設定例を示します。

```
ip vrf V27:MulticastCERC3
rd 100:124
address-family ipv4
route-target import 100:406
route-target import 100:407
route-target export 100:406
mdt default 226.2.3.4
mdt data 226.5.6.7 0.0.0.15 2000
mdt mtu 2000
ip multicast-routing vrf V27:MulticastCERC3
ip pim vrf V28:VPN13 ssm default
ip pim vrf V27:MulticastCERC3 rp-address 10.20.1.1
ip pim vrf V27:MulticastCERC3 rp-address 10.20.3.1 test2
ip pim vrf V27:MulticastCERC3 rp-address 10.20.2.1 test1 override
```

IOS XR コマンド

次の IOS コマンドは、IOS XR に対応するコマンドが存在しないため、IOS XR デバイスでサポートされていません。

- **ip multicast vrf <vrfName> route-limit.** これがサポートされていないのは、VRF ごとにルート制限を設定するためのコマンドが IOS XR デバイスで使用できないためです。
- **ip pim vrf <vrfName> sparse-dense-mode.** Sparse-Dense モードは、IOS XR ではサポートされていません。スパースモードと双方向モードのみがサポートされます。

次の IOS コマンドは、マルチキャストルーティングがイネーブルにされている場合、デフォルトで、IOS XR デバイスでイネーブルにされています。これらはディセーブルにできません。

- **ip pim vrf <vrfName> sparse-mode**
- **ip pim vrf <vrfName> ssm default**
- **ip pim vrf <vrfName> autorp listener**

IPv6 でのマルチキャスト サポート (IOS XR 限定)

IPv6 でのマルチキャストは、IOS XR デバイスのみでサポートされます。具体的には、このリリースでは、Cisco 12000 シリーズ ルータでのみこの機能がサポートされています。Prime Provisioning では、サポートされている PE デバイスおよびサポートされているバージョンの IOS XR で次のことが可能です。

- IPv6 PE-CE リンクに展開されるマルチキャスト VPN。
- VRF オブジェクトの作成中にマルチキャストをイネーブルにする。

VPN または VRF オブジェクトを作成する場合、IPv4 または IPv6、あるいはこれらの両方でマルチキャストをイネーブルにできます。VPN または VRF オブジェクトの作成時に IPv6 マルチキャストがイネーブルになった場合、IPv6 アドレスをスタティック ランデブー ポイント (RP) アドレスとして入力できます。

既存の VPN または VRF オブジェクトを変更して IPv4 または IPv6、あるいはその両方に対してマルチキャストをイネーブルにすることもできます。IPv4 マルチキャストがイネーブルの場合、同じ VPN または VRF の IPv4 リンクを含む、展開されたすべてのサービス要求は、[Requested] 状態になります。

さらに、特定の MPLS リンクに対して IPv4、IPv6 またはその両方のマルチキャストをイネーブルにするかどうかを、MPLS サービス要求内で指定できます。

IPv6 マルチキャストがイネーブルの場合、同じ VPN または VRF の IPv6 リンクを含む、展開されたすべてのサービス要求は、[Requested] 状態になります。IPv4 が以前に設定されていて、IPv6 マルチキャストのみが VPN でイネーブルになっている場合、IPv6 リンクを使用するサービス要求のみが [Requested] 状態に移行します。

IPv6 マルチキャストがイネーブルの場合、既存の VPN または VRF オブジェクトを変更して、IPv6 スタティック RP アドレスを追加できます。すでに [Deployed] 状態にあるサービス要求は、[Requested] 状態に移行します。

IP アドレッシング スキームとして IPv6 番号指定または IPv4+IPv6 番号指定を使用するサービス要求内のサービス ポリシーまたは MPLS VPN リンク、およびマルチキャストがイネーブルであるマルチキャスト VPN または VRF を作成できます。

IOS 6VPE サポートのために更新された DCPL プロパティ

2 つの DCPL プロパティが更新され、デバイスへのダウンロードが終了した後で遅延を必要とする特定の IOS コマンドをサポートするようになりました。これにより、IPv6 コンフィギュレーション コマンドを含む IOS デバイスに MPLS VPN サービス要求を展開するときに遅延が生じることがあります。

- DCPL プロパティ `GTL/CSL/ios/delayAfterDownloadingCmd` は、Telnet などのターミナルセッション プロトコルを使用してダウンロードした後に遅延を必要とする IOS コマンドをサポートするために Prime Provisioning に追加されました。リスト エレメントのフォーマット

```
cmd_regex:delay_in_seconds; no vrf definition *:105
```

「no vrf definition」コマンドがデバイスにプッシュされた後、デバイスでそれが有効になるまでに 105 秒間の遅延があります。

- DCPL プロパティ `GTL/CSL/ios/delayBeforeDownloadingCmd` は、Telnet などのターミナルセッション プロトコルを使用してダウンロードした後に遅延を必要とする特定の IOS コマンドをサポートするために Prime Provisioning に追加されました。リスト エレメントのフォーマット

```
cmd_regex:delay_in_seconds;
vrf definition *:70;
```

「vrf definition」コマンドがデバイスにプッシュされた後、デバイスでそれが有効になるまでに 70 秒間の遅延があります。

MPLS レポート

MPLS VPN レポートは、IPv6 アドレスおよび 6VPE デバイスをサポートします。IPv6 および 6VPE の MPLS VPN レポートの生成については、「[MPLS レポートの生成](#)」(P.10-42) を参照してください。

既存の IPV4 VRF のデュアルスタック (IPV4+IPV6) VRF へのアップグレード

ここでは、MPLS サービス要求を使用した、IOS 6VPE デバイスでの VRF アップグレードについて説明します。次の点に注意してください。

- この機能は、IOS 12.2(33) SRE2 バージョン以上でのみサポートされます。
- VRF での IPv4 の導入では、常に、コマンド「`ip vrf vrf-name`」がデバイスで生成されます。デュアルスタック (IPv4+IPv6) または IPv6 にアップグレードされる場合、次のことが行われます。
 - 同じデバイスで同じ VRF を共有する任意のリンクが、デバイスの「`vrf definition vrf-name`」にアップグレードされます。
 - 同じデバイスで同じ VRF を共有するすべての関連サービス要求が [Requested] 状態になります。
 - すべてのサービス要求を監査パスのために再展開する必要があります。
- Prime Provisioning からの VRF アップグレードシナリオは、「`vrf upgrade-cli multi-af-mode non-common-policies vrf vrf-name force`」コマンドがデバイスでサポートされている場合にのみ、IOS 6VPE デバイスに対して機能します。サポートされていない場合、サービス要求は [FAILED-DEPLOYED] 状態になります。このコマンドは、IOS バージョン 12.2 (33) SRE2 で使用できます。
- アップグレードでは、通常、IOS ベース IPv6 を最初から開始するのではなく、既存の IPv4 サービス要求から開始します。次の例は、通常のさまざまなアップグレードを示します。

次は、一般的な VRF 変更シナリオです。

- IPv4 からデュアルスタック (IPv4 と IPv6)。コンフィグレットが IPv6 リンク用に生成されます。コマンド「`vrf upgrade-cli multi-af-mode non-common-policies vrf vrf-name force`」を使用して、コマンド「`ip vrf vrf-name`」が「`vrf definition vrf-name`」にアップグレードされます。
- IPv4 から IPv4。コンフィグレットでの変更はありません。
- IPv4 から IPv6。「No」コマンド（「`no ip vrf vrf-name`」）が IPv4 リンクで生成されます。新しいコンフィグレット（「`vrf definition vrf-name`」）が IPv6 リンクで展開されます。
- IPv6 から IPv4。「No」コマンド（「`no vrf definition vrf-name`」）が IPv6 リンクで生成されます。新しいコンフィグレット（「`vrf vrf vrf-name`」）が IPv4 リンクに発行されます。
- リホーミング（つまり、PE 間での移動）では、古いデバイスで「no」コマンドが発行され、リホームされる PE で新しいコマンドが発行されます。

参考のために、VRF の変更シナリオの例を次に示します。

IPv4 リンクでは VRF は次のように設定されています。

```
ip vrf V8:stellavpn8
  rd 64512:1572
  route-target export 64512:15870
  route-target import 64512:15870
  route-target import 64512:15871
!
```

IPv6 リンクでは VRF は次のように設定されています。

```
vrf definition V4:stellavpn4
  rd 64512:1568
```

```

!
address-family ipv6
route-target export 64512:15862
route-target import 64512:15862
exit-address-family
!

```

IPv4+IPv6 リンク (IPv4 からデュアルスタックにアップグレードされる) で VRF が次のように設定されます。

```

vrf upgrade-cli multi-af-mode non-common-policies vrf V9:stellavpn9 force !
vrf definition V9:stellavpn9
rd 64512:1573
!
address-family ipv4
route-target export 64512:15872
route-target import 64512:15872
route-target import 64512:15873
exit-address-family
!
address-family ipv6
route-target export 64512:15872
route-target import 64512:15872
route-target import 64512:15873
exit-address-family

```

サポートされていない IPv6 および 6VPE 機能

IPv6 および 6VPE では、次の機能はサポートされていません。

- デバイスでの既存の IPv6 VPN サービスの検出。
- CPE デバイス定義および設定での IPv6 アドレッシング。
- IPv6 アドレス プール。
- IPv6 マルチキャスト アドレス プール。
- IPv4 および IPv6 アンナンバード アドレス方式は、6VPE および IOS XR ではサポートされていません。
- 6VPE および IOS XR での Grey Management VPN サポート。
- IOS XR デバイスでの eBGP ルート マップをサポートするステージングのサービス要求の展開。
- 管理対象 CE サービス (デバイスが IPv6 サービスをサポートしていない場合)。
- Multi-VRF CE (MVRFCPE; マルチ VRF CE) サポート。
- IPv6 ルーティング、BGP VPNv6 コンフィギュレーションのイネーブル化などの、6VPE デバイスでのワンタイム設定処理。
- トンネル インターフェイス。IPv6 アドレスは、[Tunnel Source Address] の値として指定できません。

MPLS VPN サービス ポリシー

この項では、Cisco Prime Provisioning GUI を使用して MPLS VPN サービス ポリシーを定義する方法を説明します。また、Prime Provisioning のテンプレートとデータ ファイルをポリシーに関連付けることもできます。ポリシーでのテンプレートおよびデータ ファイルの使用の詳細については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。

ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザ定義の属性を作成することもできます。追加情報機能の使用方法の背景説明については、付録 F「サービスに情報を追加する方法」を参照してください。

サービス ポリシーの概要

MPLS VPN のプロビジョニングは、サービス ポリシーの定義で始まります。サービス ポリシーは、単一のサービス要求で複数の PE-CE リンクに適用できます。ネットワーク オペレータはサービス ポリシーを定義します。サービス オペレータは、サービス ポリシーを使用してサービス要求を作成します。各サービス要求には、PE-CE リンクのリストが含まれています。サービス オペレータがサービス要求を作成するときに、オペレータは入力する必要があるポリシー情報のみを参照します。その他の必要な情報はすべて、サービス ポリシー自体（および自動検出プロセス）によって入力されます。

サービス ポリシー エディタ

Prime Provisioning のサービス ポリシーを定義するときに一連のダイアログボックスが表示され、MPLS サービス要求を実行するために必要な各主要カテゴリのパラメータを指定できます。サービス ポリシー エディタには、[Attribute]、[Value]、および [Editable] の 3 つの列があります。

- **Attribute**

[Attribute] 列には各主要カテゴリに定義する必要がある各パラメータの名前が表示されます（たとえば、IP アドレスまたはルーティング プロトコル）。

- **Value**

[Value] 列には、各パラメータとオプションに対応する他の選択可能な項目およびフィールドが表示されます。

属性を編集するときに呼び出されるダイアログボックスのタイプは、属性のタイプによって異なります。一部の場、値は単純な文字列値または整数値であり、単一のテキスト入力フィールドが表示されます。それ以外の場合、値が複雑になるか、IP アドレスなど複数の値で構成されます。これらの場合、必要な値を指定できるようにダイアログボックスが表示されます。入力する値は検証され、無効な値が入力されると、無効な値に関する通知が表示されます。その他の場合、チェックボックスが表示され、特定のオプションをイネーブルまたはディセーブルにできます。



(注) 場合によっては、属性の値を変更すると、関連する属性の値が無効になります。たとえば、PE インターフェイス名を変更すると、PE カプセル化値が無効になる可能性があります。これが発生すると、サービス ポリシー エディタから無効な値が除去され、それらを適切にリセットする必要があります。

一部の属性間には親子関係があります。これらの場合、親属性の値を変更すると、子属性がイネーブルまたはディセーブルになる場合があります。たとえば、PE カプセル化の値を変更すると、Data Link Connection Identifier (DLCI)、VLAN ID、ATM 回線 ID、トンネル ソース属性、および宛先アドレス属性がイネーブルまたはディセーブルになる可能性があります。

- **Editable**

[Editable] 列を使用して、ネットワーク オペレータは複数のサービス要求全体にわたって変更される可能性のある属性を示すことができます。属性のチェックボックスが編集可能としてオンになっていると、そのサービス要求ポリシーを使用してサービス要求を作成または変更するときに、サービス オペレータはそれらの属性のみを使用できます。

属性カテゴリが編集可能と設定されている場合、関連属性および子属性もすべて編集可能属性です。

Cisco Prime Provisioning の IP アドレスについて

VPN（またはエクストラネット）内では、すべての IP アドレスは固有である必要があります。カスタマー IP アドレスは、プロバイダー IP アドレスとオーバーラップできません。オーバーラップは、2 つのデバイスが相互に参照できない場合、つまり、2 つのデバイスが分離された非エクストラネット VPN 内にある場合にのみ可能です。

Prime Provisioning MPLS VPN ソフトウェアでは、アドレスを取得する IP アドレス プールがあることを想定しています。製品がこれらのアドレスを自由に使用できることが保証されるのは、それらがプロバイダー IP アドレスである場合のみです。

PE-CE リンクに対する IP アドレス空間の固有セクションを事前定義することが、安定したセキュリティを確保する唯一の方法です。このため、セキュリティおよびメンテナンスの観点から、PE-CE リンクでカスタマーの IP アドレスを使用することは推奨しません。

MPLS VPN サービス ポリシーの定義

この項の残りの部分では、PE-CE リンクの MPLS サービス ポリシー定義の拡張例を説明します。これは、MPLS サービス ポリシーの定義に含まれるさまざまなステップを例示するためのものです。これらの手順は、異なるタイプの MPLS VPN サービス ポリシーを定義するための基盤として使用することができます。その他のタイプの MPLS VPN ポリシーについては、このガイドのその他の章で説明します。

PE-CE リンク用の MPLS VPN サービス ポリシーを定義するには、次の手順を実行します。

-
- ステップ 1** [Service Design] > [Policies] > [MPLS] を選択します。
[MPLS Policy Editor - Policy Type] ウィンドウが表示されます。
- ステップ 2** MPLS ポリシーの [Policy Name] を入力します。
- ステップ 3** [Policy Owner] を選択します。

MPLS ポリシー所有権には次の 3 種類があります。

- カスタマー所有権
- プロバイダー所有権
- グローバル所有権：任意のサービス オペレータがこの MPLS ポリシーを使用できます。

この所有権は、Prime Provisioning Role-Based Access Control (RBAC; ロールベース アクセス コントロール) が有効になると関係してきます。たとえば、カスタマー所有の MPLS ポリシーは、このカスタマー所有ポリシーでの作業が許可されているオペレータのみが参照できます。

同様に、プロバイダーのネットワークでの作業を許可されているオペレータは、特定のプロバイダー所有ポリシーを表示、使用、および展開できます。



(注) ケーブル (PE-NoCE) の場合、ポリシー所有権を「プロバイダー」に設定する必要があります。

- ステップ 4** MPLS ポリシーの所有者を選択するには、[Select] をクリックします。(グローバル所有権を選択すると、[Select] 機能を使用できません)。
[Select Customer] ウィンドウまたは [Select Provider] ウィンドウが表示され、ポリシーの所有者を選択して [Select] をクリックできます。
- ステップ 5** MPLS ポリシーの [Policy Type] の値を選択します。

MPLS ポリシーには 2 つのポリシー タイプがあります。

- 標準 PE-CE : PE から CE へのリンク
- MVRFC PE-CE : PE のマルチ VRF 機能を使用した PE から CE へのリンク

ステップ 6 Prime Provisioning がサービス アクティベーション時に CE ルータとインターフェイスを指定するようにこの MPLS ポリシーを使用するサービス オペレータに尋ねるようにするには、[CE Present] チェックボックスをオンにします。デフォルトでは、サービスに CE が存在します。

[CE Present] チェックボックスをオンにしない場合、Prime Provisioning は、PE-CLE または PE-POP ルータおよびカスタマー方向のインターフェイスについてのみ、サービス アクティベーション時にサービス オペレータに尋ねます。

ステップ 7 [Next] をクリックします。

この例を続行するには、次の項、「[PE および CE インターフェイス パラメータの指定](#)」(P.5-45) を参照してください。

PE および CE インターフェイス パラメータの指定

この MPLS ポリシーの PE、UNI セキュリティ、および CE インターフェイスを指定するには、次の手順を実行します。



ヒント

この時点では、PE および CE に対して特定のインターフェイス タイプを選択する必要はありません。フィールドがデフォルトで [Editable] に設定されていることに注意してください。インターフェイス パラメータが [Editable] に設定されていると、サービス オペレータはサービス要求の作成時に正確なインターフェイス タイプと形式を指定できます。

サービス要求の作成時にこのサービス ポリシーのデバイス インターフェイス情報を指定する場合は、フィールドを現在デフォルトで設定されているままにして、[Next] をクリックします。

PE Information

ステップ 1 [Interface Type] : ドロップダウン リストから、PE のインターフェイス タイプを選択します。

Cisco IP Solution Center は、次のインターフェイス タイプをサポートします (PE および CE の両方)。

- Any
- ATM (非同期転送モード)
- BRI (基本速度インターフェイス)
- Bundle-Ether (詳細については、「[ステップ 2\[Interface Format\] : オプションで、PE インターフェイスのスロット番号およびポート番号を指定できます。](#)」(P.5-46) を参照してください)。
- イーサネット
- ファスト イーサネット
- FDDI (ファイバ分散データ インターフェイス)
- GE-WAN (ギガビット イーサネット WAN)
- ギガビット イーサネット
- HSSI (高速シリアル インターフェイス)

- ループバック
- MFR
- マルチリンク
- PoS (Packet over Sonet)
- ポート チャネル
- シリアル
- スイッチ
- トンネル
- VLAN

ステップ 2 [Interface Format] : オプションで、PE インターフェイスのスロット番号およびポート番号を指定できます。

標準命名法 : **スロット番号/ポート番号** で形式を指定します (たとえば、**1/0** は、インターフェイスがスロット 1、ポート 0 にあることを示します)。

これは、サービス内のすべてまたは大部分のネットワーク デバイスにある特定のインターフェイスのスロットまたはポートの位置をリンクが常に通過することがわかっている場合に、ここで指定しておくのと特に役立ちます。このパラメータを編集可能のままにしておくと、サービス オペレータがサービス要求を作成するときに変更できます。

インターフェイス形式をチャネライズド インターフェイスとして指定することもできます。

- **slot/subSlot/port** (たとえば、**2/3/4** は、インターフェイスがシリアル 2/3/4 にあることを示します)
- **slot/subSlot/port/T1#:channelGroup#** (たとえば、**2/0/4/6:8** は、インターフェイスがシリアル 2/0/4/6:8 にあることを示します)
- **slot/subSlot/port.STS-1Path/T1#:channelGroup#** (たとえば、**2/0/0.1/6:8** は、インターフェイスがシリアル 2/0/0.1/6:8 にあることを示します)

ステップ 3 [Interface Description] : オプションで、PE インターフェイスの説明を入力できます。

ステップ 4 [Shutdown Interface] : このチェックボックスをオンにすると、指定された PE インターフェイスはシャットダウン状態で設定されます。

ステップ 5 [Encapsulation] : 指定された PE インターフェイス タイプに使用するカプセル化を選択します。

インターフェイス タイプを選択するときに、指定されたインターフェイス タイプに対してサポートされるカプセル化タイプのドロップダウン リストが [Encapsulation] フィールドに表示されます。

表 5-2 に、サポートされる各インターフェイス タイプで使用可能なプロトコル カプセル化を示します。

表 5-2 インターフェイス タイプおよび対応するカプセル化

インターフェイス タイプ	カプセル化
ATM	AAL5SNAP
BRI	フレームリレー、フレームリレー ietf、HDLC (ハイレベル データリンク コントロール)、PPP (ポイントツーポイント プロトコル) フレームリレー ietf は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) 標準 (RFC 1490) に準拠するようにカプセル化方式を設定します。フレームリレー ネットワークを介して別のベンダーの機器に接続する場合は、この方式を使用します。

表 5-2 インターフェイス タイプおよび対応するカプセル化 (続き)

インターフェイス タイプ	(続き) カプセル化
Bundle-Ether	デフォルト フレーム、dot1q (802.1Q)
イーサネット	デフォルト フレーム、dot1q (802.1Q)
ファスト イーサネット	デフォルト フレーム、ISL (スイッチ間リンク)、dot1q (802.1Q)
FDDI (ファイバ分散データ インターフェイス)	なし
ギガビット イーサネット	デフォルト フレーム、ISL (スイッチ間リンク)、dot1q (802.1Q)
ギガビット イーサネット WAN	デフォルト フレーム、ISL (スイッチ間リンク)、dot1q (802.1Q)
HSSI (高速シリアル インターフェイス)	フレームリレー、フレームリレー ietf、HDLC (ハイレベル データリンク コントロール)、PPP (ポイントツーポイント プロトコル)
ループバック	なし。
MFR	フレームリレー、フレームリレー ietf、HDLC (ハイレベル データリンク コントロール)、PPP (ポイントツーポイント プロトコル)
マルチリンク	PPP (ポイントツーポイント プロトコル)
ポート チャネル	デフォルト フレーム、ISL (スイッチ間リンク)、dot1q (802.1Q) 注 : [Andrew が内容を提供]
POS (Packet Over Sonet)	フレームリレー、HDLC (ハイレベル データリンク コントロール)、PPP (ポイントツーポイント プロトコル)
シリアル	フレームリレー、フレームリレー ietf、HDLC (ハイレベル データリンク コントロール)、PPP (ポイントツーポイント プロトコル)
スイッチ	AAL5SNAP
トンネル	GRE (総称ルーティング カプセル化) - このリリースでは GRE はサポートされていません。 -
VLAN	なし



(注) MLFR インターフェイスは、IOS デバイスと IOS XR デバイスでサポートされます。Prime Provisioning は、MLFR インターフェイスをセットアップしません。Prime Provisioning は、MLFR インターフェイス上のレイヤ 3 サービスをプロビジョニングします。

ステップ 6 [Auto-Pick VLAN ID] : Prime Provisioning が自動的に VLAN ID を選択するようにする場合は、このチェックボックスをオンにします。



(注) [Auto-Pick VLAN ID] がオフの場合、そのポリシーに基づくサービス要求の作成時に、VLAN ID を入力するようにプロンプトが表示されます。

ステップ 7 [Use SVI] : Prime Provisioning が SVI で VRF を終了するようにするには、このチェックボックスをオンにします。

ステップ 8 [ETTH Support] : Ethernet-To-The-Home (ETTH) を設定するには、このチェックボックスをオンにします。ETTH の説明については、「Ethernet-To-The-Home (ETTH)」(P.5-154) を参照してください。

ステップ 9 [Standard UNI Port] : UNI セキュリティ パラメータにアクセスするには、このチェックボックスをオンにします。

UNI セキュリティ情報

ステップ 10 [Disable CDP] : CDP をディセーブルにするには、このチェックボックスをオンにします。

ステップ 11 [Filter BPDU] : BPDU をフィルタリングするには、このチェックボックスをオンにします。

ステップ 12 [Use existing ACL Name] : 既存の ACL 名を使用するには、このチェックボックスをオンにします。

ステップ 13 [UNI MAC Addresses] : MAC アドレス レコードを変更または作成するには、[Edit] をクリックします。

ステップ 14 [UNI Port Security] : UNI ポート セキュリティ パラメータにアクセスするには、このチェックボックスをオンにします。

- a. [Maximum MAC Address] : 有効な値を入力します。
- b. [Aging (in minutes)] : 有効な値を入力します。
- c. [Violation Action] : ドロップダウン リストから、次のいずれかを選択します。
 - PROTECT
 - RESTRICT
 - SHUTDOWN
- d. [Secure MAC Address] : セキュア MAC アドレス レコードを変更または作成するには、[Edit] をクリックします。

CE インターフェイス情報

ステップ 15 [Interface Type] : ドロップダウン リストから、CE のインターフェイス タイプを選択します。

ステップ 16 [Interface Format] : オプションで、CE インターフェイスのスロット番号およびポート番号を指定できます。

ステップ 17 [Interface Description] : オプションで、CE インターフェイスの説明を入力できます。

ステップ 18 [Encapsulation] : 指定された CE インターフェイス タイプに使用するカプセル化を選択します。

ステップ 19 インターフェイス設定に満足したら、[Next] をクリックします。

この例を続行するには、次の項、「IP アドレス スキームの指定」(P.5-48) を参照してください。

IP アドレス スキームの指定

このサービス ポリシーで使用する IP アドレス スキームを指定するには、次の手順を実行します。

ステップ 1 PE-CE リンクに適した IP アドレッシング スキームを定義します。

IP Numbering Scheme

次のオプションから選択できます。

- IPv4 Numbered

[IPv4 Numbered] を選択し、[Automatically Assign IP Address] チェックボックスもオンにすると、Prime Provisioning MPLS は、対応する IP アドレスがルータのコンフィギュレーション ファイル内に存在するかどうかを確認します。アドレスが存在し、同じサブネット内にある場合、Prime Provisioning はそれらのアドレスを使用します（アドレス プールからは割り当てません）。IP アドレスがコンフィギュレーション ファイル内に存在しない場合、Prime Provisioning は、/30 サブネット ポイントツーポイント IP アドレス プールから IPv4 アドレスを選択します。

• IPv4 Unnumbered

IPv4 アドレスは、ループバック IPv4 アドレス プールから取得されます。アンナンバード IPv4 アドレスとは、各インターフェイスがルータ上の別のインターフェイス（通常はループバック インターフェイス）からアドレスを「借用」することを意味します。アンナンバードアドレスは、ポイントツーポイント WAN リンク（シリアル、フレーム、ATM など）でのみ使用可能で、LAN リンク（イーサネットなど）では使用できません。IP アンナンバードを使用する場合、PE と CE の両方が同じ IP アンナンバードアドレッシング スキームを使用する必要があります。[IPv4 Unnumbered] を選択すると、Prime Provisioning : MPLS は、PE-CE リンクのスタティック ルートを作成します。

[IPv4 Unnumbered] を選択すると、Prime Provisioning : MPLS は、自動的にループバック インターフェイスを作成します（正しい属性のループバック インターフェイスが存在しない場合）。関連情報については、「既存のループバック インターフェイス番号の使用」(P.5-50) を参照してください。

• IPv6 Numbered

このアドレッシング スキームは、6VPE ルータをサポートするために提供されています。MPLS VPN 管理における IPv6 および 6VPE サポートの詳細については、「MPLS VPN での IPv6 および 6VPE サポート」(P.5-32) を参照してください。



(注) このオプションは、ポリシー タイプが標準 PE-CE ポリシーである場合にのみ表示されます。

• IPv4+IPv6 Numbered

6VPE デバイスの場合、PE インターフェイスを「デュアル スタック」、つまり、IPv4 アドレスと IPv6 アドレスの両方を含むことができるようにすることができます。後のステップで、IPv4 と IPv6 両方のルーティング情報を独立して入力できます。MPLS VPN 管理における IPv6 および 6VPE サポートの詳細については、「MPLS VPN での IPv6 および 6VPE サポート」(P.5-32) を参照してください。



(注) このオプションは、ポリシー タイプが標準 PE-CE ポリシーである場合にのみ表示されます。

ステップ 2 CE に追加ループバック インターフェイスが必要であるかどうかを指定します。

Extra CE Loopback Required

番号指定 IP アドレスはループバック アドレスを必要としませんが、Prime Provisioning ソフトウェアは、追加の CE ループバック インターフェイスが必要であることを指定するオプションを提供します。このオプションは、どの物理インターフェイスにも接続されていない CE ルータに IP アドレスを配置します。

[Extra CE Loopback Required] をイネーブルにすると、CE ループバック アドレスを入力できます。

ステップ 3 自動的に IP アドレスを割り当てるかどうかを指定します。

Automatically Assign IP Address

[IPv4 Unnumbered] を選択し、[Automatically Assign IP Address] チェックボックスもオンにすると、Prime Provisioning は、/32 サブネット ポイントツーポイント IP アドレス プールから 2 つの IP アドレスを選択します。

[IPv4 Numbered] を選択し、[Automatically Assign IP Address] チェックボックスもオンにすると、Prime Provisioning は、対応する IP アドレスがルータのコンフィギュレーション ファイル内に存在するかどうかを確認します。アドレスが存在し、同じサブネット内にある場合、Prime Provisioning はこれらのアドレスを使用します（アドレス プールからは割り当てません）。IP アドレスがコンフィギュレーション ファイル内に存在しない場合、Prime Provisioning は、/30 サブネット ポイントツーポイント IP アドレス プールから IP アドレスを選択します。



(注) このオプションは、[IPv6 Numbered] アドレス スキームおよび [IPv4+IPv6 Numbered] アドレス スキームの場合はサポートされません。

ステップ 4 このサービス ポリシーの IP アドレス プールおよび関連リージョンを指定します。

IP Address Pool

[IP Address Pool] オプションは、Prime Provisioning が、リージョンに接続された IP アドレス プールから自動的に IP アドレスを割り当てるようにする機能をサービス オペレータに提供します。サービス ポリシーのこの側面を定義する前に、リージョンが定義されていて、適切な IP アドレス プールがそのリージョンに割り当てられている必要があります。

ポイントツーポイント（IP 番号指定）PE-CE リンクに対して IP アドレス プール情報を指定できます。

IP アンナンバードアドレスは、ループバック IP アドレス プールから取得されます。アンナンバード IP アドレスとは、各インターフェイスがルータ上の別のインターフェイス（通常はループバック インターフェイス）からアドレスを「借用」することを意味します。アンナンバードアドレスは、ポイントツーポイント WAN リンク（シリアル、フレーム、ATM など）でのみ使用可能で、LAN リンク（イーサネットなど）では使用できません。IP アンナンバードを使用する場合、PE と CE の両方が同じ IP アンナンバード アドレッシング スキームを使用する必要があります。



(注) このオプションは、[IPv6 Numbered] アドレス スキームおよび [IPv4+IPv6 Numbered] アドレス スキームの場合はサポートされません。

ステップ 5 IP アドレス スキームに満足したら、[Next] をクリックします。

既存のループバック インターフェイス番号の使用

各 PE には、IP アンナンバードアドレスを使用しているインターフェイスについて、通常は VRF ごとに 1 つのループバック インターフェイス番号のみが存在します。ただし、IP アンナンバードアドレスと手動で割り当てた IP アドレスを使用してインターフェイスをプロビジョニングしている場合、同じ VRF で複数のループバック インターフェイス番号を持つことができます。IP アンナンバードアドレスのプロビジョニングに自動的に割り当てられる IP アドレスを使用する場合、Prime Provisioning は同じ VRF 名を持つ最初のループバック番号をインターフェイスに関連付けます。ループバック番号が存在しない場合、Prime Provisioning はループバック番号を作成します。

Prime Provisioning が既存のループバック インターフェイス番号（たとえば、Loopback0）を使用することをサービス プロバイダーが要求する場合、サービス プロバイダーは関連のあるルータ（PE または CE）のコンフィギュレーション ファイルのループバック インターフェイス記述行を変更する必要があります。

既存のループバック インターフェイス番号を使用するには、次のルータ コンフィギュレーション ファイルの例で示されているように、キーワード **VPN-SC** が含まれるようにループバック インターフェイス記述行を変更する必要があります。



(注) PE で既存のループバック インターフェイス番号を使用する場合、**ip vrf forwarding VRF_name** コマンドを設定した追加のコマンドラインを「**description**」行のすぐ後に含める必要があります。

```
interface Loopback0
description by VPN-SC
ip vrf forwarding <VRF_name> ; This line is required on the PE only
ip address 209.165.202.129 255.255.255.224
```

既存のループバック インターフェイスは、インターフェイス コンフィギュレーションが「IP アドレスを使用する WAN シリアル インターフェイスである」という条件をみたす場合にのみ使用できます。

Prime Provisioning は、ループバック インターフェイス番号を順番に選択します。**Prime Provisioning** は、要件 (CE の場合、**VPN-SC** キーワードが含まれていること。PE の場合、一致する **VRF** 名であること) を満たす最初のループバック インターフェイス番号を使用します。

たとえば、**loopback1** と **loopback2** に **VPN-SC** キーワードが含まれていて、**loopback3** には含まれていない場合、**loopback3** に **VPN-SC** キーワードを追加しても、自動的に割り当てられるアドレスの使用時に **Prime Provisioning** がアンナンバード インターフェイスに強制的に **loopback3** を選択することにはなりません。代わりに、**loopback1** が選択されます。特定のループバック インターフェイス番号を選択する唯一の方法は、必要なループバック インターフェイス番号に一致する手動割り当て IP アドレスを使用することです。



(注) 標準インターフェイスとは異なり、**Prime Provisioning** でループバック インターフェイスがプロビジョニングされる場合、結果として生成されるコンフィギュレーション ファイルには **Service Request** (SR; サービス要求) の ID 番号は含まれていません。これは、複数のインターフェイスまたはサービス要求が同じループバック インターフェイスを使用する可能性があるためです。

この例を続行するには、次の項、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

サービスのルーティング プロトコルの指定

このサービス ポリシーのルーティング プロトコル情報を指定できるようになりました。



(注) IPv4 および IPv6 のルーティングは独立しています。**Prime Provisioning GUI** を使用すると、選択したアドレッシング スキームに応じて、IPv4 および IPv6 に対して同じルーティング プロトコル、または異なるルーティング プロトコルを入力できます。IPv6 の場合、すべてのルーティング プロトコルがサポートされるわけではありません。IPv6 およびサポートされるルーティング プロトコルの詳細については、「**MPLS VPN での IPv6 および 6VPE サポート**」(P.5-32) を参照してください。

選択するルーティング プロトコルは、PE と CE の両方で実行される必要があります。次のプロトコルのいずれかを選択できます。

- [Static] : スタティック ルートを指定します (「**スタティック プロトコルの選択**」(P.5-53) を参照)。
- [RIP] : Routing Information Protocol (「**RIP プロトコルの選択**」(P.5-54) を参照)。

- [BGP] : ボーダー ゲートウェイ プロトコル (「[BGP プロトコルの選択](#)」(P.5-58) を参照)。
- [OSPF] : Open Shortest Path First (「[OSPF プロトコルの選択](#)」(P.5-64) を参照)。
- [EIGRP] : Enhanced Interior Gateway Routing Protocol (「[EIGRP プロトコルの選択](#)」(P.5-72) を参照)。
- [None] : ケーブル サービスのパラメータを指定します (「[\[None\] を選択 : ケーブル サービス](#)」(P.5-75) を参照)。

PE-CE リンクのルーティング プロトコルを指定するには、次の手順を実行します。

ステップ 1 [Routing Protocol] ドロップダウン リストから適切なプロトコルを選択します。



(注) IPv6 アドレッシングの場合、ルーティング プロトコルのサブセットのみがサポートされます。IOS XR デバイスの場合、[Static]、[BGP]、[EIGRP]、および [None] のみがサポートされません。IOS デバイスの場合、[Static]、[BGP]、および [None] のみがサポートされます。

特定のルーティング プロトコルを選択すると、そのプロトコルの関連パラメータが表示されます。

ステップ 2 選択されたルーティング プロトコルに必要な情報を入力し、[Next] をクリックします。

ステップ 3 「[VRF および VPN の情報の定義](#)」(P.5-76) で説明されているように、[MPLS Policy VRF and VPN Selection] のパラメータを定義します。

IP ルートの再配布

ルート再配布は、1 つのソースからルーティング情報を取得して、その情報を別のソースにインポートするプロセスです。再配布へのアプローチには注意が必要です。ルート再配布を実行すると、情報が失われます。メトリックを適宜リセットする必要があります。たとえば、5 ホップメトリックを使用する RIP ルートのグループを iGRP に再配布する場合、5 ホップ RIP メトリックを IGRP の複合メトリックに変換する方法はありません。RIP ルートが IGRP に再配布されるときに、RIP ルートのメトリックを適宜選択する必要があります。また、2 つのダイナミック ルーティング プロトコル ドメイン間の複数のポイントで再配布が実行されると、ルーティング ループが発生する可能性があります。

CSC サポート

Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146) で説明します。

CE へのデフォルト ルートのみの提供

[Give only default routes to CE] オプションをイネーブルにするときに、サイトが完全なルーティングまたはデフォルト ルーティングのどちらを必要とするかを示します。完全なルーティングは、VPN 内に存在するその他のルートをサイトが具体的に認識する必要がある場合です。デフォルト ルーティングは、具体的にそのサイトに対するものではないパケットをすべて VPN に送信すれば十分な場合です。

このオプションを選択すると、Prime Provisioning は、実行プロトコルで PE ルータに対して **default-info originate** コマンドを設定します (RIP、OSPF、または EIGRP の場合)。Static の場合、Prime Provisioning は、CE ルータに対して **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** コマンドを設定します。

デバイスは、デフォルト ルートを 1 つのみ持つことができます。したがって、VPN はデフォルト ルートを使用できますが、それはカスタマー サイトにまだ別のデフォルト ルートがない場合のみです。すでにデフォルト ルートがある最も一般的な理由は、VPN と独立したインターネット フィードがサイトに あるということです。

CE サイトにインターネット サービスがすでにある場合、CE は、不明な宛先へのパケットをすべてインターネットにルーティングするか、またはインターネット内のすべてのルートを学習できます。明らかな選択は、不明な宛先へのパケットをすべてインターネットにルーティングすることです。サイトにインターネット フィードがある場合、すでにデフォルト ルートがある可能性があります。そのような場合は、VPN をデフォルト ルートとして設定することは正しくありません。VPN は、その他の VPN サイト用のパケットのみをルーティングする必要があります。

スタティック プロトコルの選択

スタティック ルーティングとは、ルータに手動でリストされている宛先へのルートのことです。この場合のネットワーク到達可能性は、ネットワーク自体の存在および状態には依存しません。宛先のアップ/ダウンには関係なく、スタティック ルートはルーティング テーブルに残り、トラフィックはその宛先に送信されます。

プロトコルとして [Static] を選択すると、[CSC Support]、[Give Only Default Routes to CE]、[Redistribute Connected (BGP only)]、および [Default Information Originate (BGP only)] の 4 つのオプションがイネーブルになります。



(注)

その他の 2 つのオプション ([AdvertisedRoutes] および [Default Routes - Routes to reach other sites]) は、サービス要求を作成するときに使用できます。「[スタティック ルーティング プロトコル属性の設定 \(IPv4 と IPv6\)](#)」(P.5-96) を参照してください。

サービス ポリシーのルーティング プロトコルとして [Static] を指定するには、次の手順を実行します。

ステップ 1

[CsC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。

[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146) で説明します。

前のステップで IP アドレッシング スキームが IPv6 に設定されている場合は、この属性を使用できません。

ステップ 2

[Give Only Default Routes to CE] : スタティック ルートを使用してプロビジョニングするときに、このサービス ポリシーが CE にデフォルト ルートのみを与えるかどうかを指定します。

PE-CE リンクのスタティック ルートプロビジョニングで [Give only default routes to CE] オプションをイネーブルにすると、Prime Provisioning は PE を指すデフォルト ルートを CE に作成します。CE サイトへの VRF スタティック ルートは、VPN 内のその他のサイトの BGP に再配布されます。

このオプションを選択すると、デフォルト ルート (0.0.0.0/32) が自動的に設定されます。サイトには、インターネット フィードやその他のデフォルト ルートに対する要件は含まれません。ローカルにはルーティングされないパケットをサイトが検出すると、そのパケットを VPN に送信できます。

このオプションを選択すると、Prime Provisioning は、実行プロトコルで PE ルータに対して **default-info originate** コマンドを設定します (RIP、OSPF、または EIGRP の場合)。Static の場合、Prime Provisioning は、CE ルータに対して **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** コマンドを設定します。

ステップ 3 [Redistribute Connected (BGP Only)] : このサービス ポリシーが、VPN 内のその他の CE に接続済みルートを再配布するかどうかを示します。

[Redistribute Connected] オプションをイネーブルにすると、接続済みルート (つまり、直接接続された PE または CE へのルート) は、その特定の VPN にある他のすべての CE に配布されます。このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。



ヒント

管理 VPN に参加し、IP 番号指定アドレスも使用している場合、[Redistribute Connected] オプションをイネーブルにする必要があります。

ステップ 4 [Default Information Originate (BGP Only)] : このオプションをイネーブルにすると、Prime Provisioning は、現在指定されている VRF に対して iBGP アドレス ファミリーで **default-information-originate** コマンドを発行します。

[Default Information Originate] オプションは、特にハブ アンド スポーク トポロジ内では必須です。これは、各スポークがその他のすべてのスポークと通信できる必要があるためです (ハブ PE にスポーク PE へのデフォルト ルートを挿入することによる)。

ステップ 5 このサービス ポリシーのスタティック ルーティングの定義が完了したら、[Next] をクリックします。

[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。

RIP プロトコルの選択

Routing Information Protocol (RIP; ルーティング情報プロトコル) は、ホップ カウントをメトリックとして使用する距離ベクトル型のプロトコルです。RIP は一種の Interior Gateway Protocol (IGP) であり、単一自律システム内でルーティングを実行することを意味します。RIP は、ルーティングアップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。ルータは、エントリの変更が含まれるルーティング アップデートを受け取ると、新しいルートを反映するようにそのルーティング テーブルを更新します。パスのメトリック値は 1 ずつ大きくなり、送信者はネクスト ホップとして示されます。

RIP ルータは宛先への最善なルート (つまり、メトリック値が可能な範囲で最小のルート) のみを維持します。ルータは、そのルーティング テーブルを更新した後、他のネットワーク ルータに変更を通知するために、ルーティング アップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的にスケジュールされたアップデートとは独立して送信されます。

サービス ポリシーのルーティング プロトコルとして RIP を指定するには、次の手順を実行します。

ステップ 1 [Routing Protocol] ドロップダウン リストから [RIP] を選択します。

[RIP Routing Protocol] ウィンドウが表示されます。

ステップ 2 [CSC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。

[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「Carrier Supporting Carrier のプロビジョニング」(P.5-146) で説明します。

ステップ 3 [Give Only Default Routes to CE] : CE にデフォルト ルートのみを与えるかどうかを指定します。

インターネットワークが階層的に設計されている場合、デフォルト ルートはルーティング情報の伝搬の必要性を制限するために役立つツールです。アクセス レベル ネットワーク (ブランチ オフィスなど) は、通常は本社への接続を 1 つのみを持っています。組織のすべてのネットワーク プレフィックスがブランチ オフィスのルーティング テーブルにない場合は、デフォルト ルートを設定します。宛先プレフィックスがブランチ オフィスのルーティング テーブルにない場合は、デフォルト ルートを介してパケットを転送します。Cisco IP ルーティング テーブルでは、デフォルト ルートはルーティング テーブルの上部に「Gateway of Last Resort」として表示されます。RIP は、自動的に 0.0.0.0 0.0.0.0 ルートを再配布します。

このオプションを選択すると、Prime Provisioning は、実行プロトコルで PE ルータに対して **default-info originate** コマンドを設定します (RIP、OSPF、または EIGRP の場合)。Static の場合、Prime Provisioning は、CE ルータに対して **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** コマンドを設定します。

RIP の場合に [Give Only Default Routes to CE] オプションをイネーブルにすると、Prime Provisioning は PE にデフォルト RIP ルートを作成します。デフォルト RIP ルートは PE を指し、CE に送信されます。プロビジョニング要求は、カスタマー ネットワーク内のその他のルーティング プロトコルを CE RIP ルーティング プロトコルに再配布するというオプションを提供します。PE から CE サイトへの RIP ルートは、BGP からその他の VPN サイトに再配布されます。

RIP ルーティングの場合にこのオプションを選択すると、PE は、その他の方法ではルーティングできないトラフィックを PE に送信するように CE に指示します。CE サイトが何らかの理由 (別のインターネット ネットワーク フィールドがあるなど) でデフォルト ルートを必要とする場合は、このオプションを使用しないでください。

ステップ 4 [Redistribute Static] : (BGP および RIP) コア BGP ネットワークにスタティック ルートを再配布するかどうかを示します。

RIP の場合に [Redistribute Static] オプションをイネーブルにすると、ソフトウェアはスタティック ルートをコア ネットワーク (BGP を実行) および CE (RIP を実行) にインポートします。

ステップ 5 [Redistribute Connected] : (BGP のみ) VPN 内の CE に接続済みルートを再配布するかどうかを指定します。

BGP の場合に [Redistribute Connected] オプションをイネーブルにすると、ソフトウェアは、接続済みルート (つまり、直接接続された PE または CE へのルート) をその特定の VPN にあるその他すべての CE にインポートします。

[Redistribute Connected] オプションをイネーブルにすると、接続済みルート (つまり、直接接続された PE または CE へのルート) は、その特定の VPN にあるその他すべての CE に配布されます。このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。

ステップ 6 [RIP Metrics] : (BGP のみ) 適切な RIP メトリック値を入力します。有効なメトリック値は、1 ~ 16 です。

RIP で使用されるメトリックはホップ カウントです。直接接続されたインターフェイスすべてのホップ カウントは 1 です。隣接するルータがホップ カウント 1 の別のネットワークへのルートをアドバタイズする場合、そのネットワークのメトリックは 2 です。これは、送信元ルータが宛先ネットワークに到達するためにそのルータにパケットを送信する必要があるためです。

各ルータがルーティング テーブルをネイバーに送信すると、AS 内で各ネットワークに対するルートを決定できます。ルータからネットワークへの複数のパスが AS 内に存在する場合、ルータは最小のホップ カウントのパスを選択し、その他のパスは無視します。

ステップ 7 [Redistributed Protocols on PE] : ルーティング プロトコルを PE に配布するかどうかを指定します。

再配布により、別のルーティング プロトコルを使用して検出されたルーティング情報を現在のルーティング プロトコルのアップデート メッセージで配信できます。再配布を使用すると、ご使用の IP インターネットワークのすべてのポイントに到達できます。RIP ルータは、別のプロトコルからルーティング情報を受信すると、再配布情報をインポートするプロトコルですでに検出済みの新規ルーティング情報ですべての RIP ネイバーを更新します。

RIP が PE にルーティング情報をインポートする必要があるプロトコルを指定するには、次の手順を実行します。

- a. [Redistribute Protocols on PE] オプションから、[Edit] をクリックします。
[PE Redistributed Protocol] ダイアログボックスが表示されます。
- b. [Add] をクリックします。
[PE Redistributed Protocols] ダイアログボックスが表示されます。
- c. [Protocol Type] ドロップダウン リストから、PE にインポートするプロトコルを選択します。
次のいずれかを選択できます。[Static]、[OSPF]、または [EIGRP]。
 - Static を再配布します。RIP への再配布に **Static** ルートを選択すると、Prime Provisioning は RIP を実行している PE にスタティック ルートをインポートします。
Static ルートを PE に再配布するために必要なパラメータやメトリックはありません。
 - Open Shortest Path First (OSPF) を再配布します。RIP への再配布に **OSPF** プロトコルを選択すると、Prime Provisioning は RIP を実行している PE に OSPF ルートをインポートします。
パラメータ : OSPF プロセス番号
メトリック : 1 ~ 16 の範囲内の任意の数値
 - Enhanced IGRP (EIGRP) を再配布します。RIP への再配布に **EIGRP** プロトコルを選択すると、Prime Provisioning は RIP を実行している PE に EIGRP ルートをインポートします。
パラメータ : EIGRP 自律システム (AS) 番号
メトリック : 1 ~ 16 の範囲内の任意の数値
- d. PE の RIP に再配布するプロトコルを選択します。
- e. 選択したプロトコルに適したパラメータを入力します。
- f. [Add] をクリックします。
- g. PE の RIP に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 8 [Redistribute Protocols on CE] : CE にルーティング プロトコルを再配布するかどうかを指定します。

RIP が CE にルーティング情報をインポートする必要があるプロトコルを指定するには、次の手順を実行します。

- a. [Redistribute Protocols on CE] オプションから、[Edit] をクリックします。
[CE Redistributed Protocol] ダイアログボックスが表示されます。
- b. [Add] をクリックします。
[CE Redistributed Protocols] ダイアログボックスが表示されます。
- c. [Protocol Type] ドロップダウン リストから、CE にインポートするプロトコルを選択します。

次のいずれかのプロトコルを選択できます。[Static]、[BGP]、[Connected] (ルート)、[IGRP]、[OSPF]、[EIGRP]、または [IS-IS]。

- **Static** を再配布します。RIP への再配布に **Static** ルートを選択すると、Prime Provisioning は RIP を実行している CE にスタティック ルートをインポートします。

Static ルートを CE に再配布するために必要なパラメータはありません。

- **Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル)** を再配布します。RIP への再配布に **BGP** プロトコルを選択すると、Prime Provisioning は RIP を実行している CE に BGP ルートをインポートします。

パラメータ : BGP 自律システム (AS) 番号

- **Connected** ルートを再配布します。RIP への再配布に **Connected** ルートを選択すると、Prime Provisioning は現在のルータに接続されているインターフェイスにすべてのルートをインポートします。ネットワークをアドバタイズするが、そのネットワークにルーティング アップデートを送信しない場合は、[Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。

パラメータ : パラメータは不要

- **Interior Gateway Routing Protocol (IGRP)** を再配布します。RIP への再配布に **IGRP** (Interior Gateway Routing Protocol) を選択すると、Prime Provisioning は RIP を実行している CE に IGRP ルートをインポートします。

パラメータ : IGRP 自律システム (AS) 番号

- **Enhanced IGRP (EIGRP)** を再配布します。RIP への再配布に **EIGRP** プロトコルを選択すると、Prime Provisioning は RIP を実行している PE に EIGRP ルートをインポートします。

パラメータ : EIGRP 自律システム (AS) 番号

- **Open Shortest Path First (OSPF)** を再配布します。RIP への再配布に **OSPF** プロトコルを選択すると、Prime Provisioning は RIP を実行している CE に OSPF ルートをインポートします。

パラメータ : OSPF プロセス番号

- **Intermediate System-to-Intermediate System (IS-IS)** を再配布します。RIP への再配布に **IS-IS** プロトコルを選択すると、Prime Provisioning は RIP を実行している CE に IS-IS ルートをインポートします。

パラメータ : IS-IS タグ番号

- d. CE の RIP に再配布するプロトコルを選択します。
- e. 選択したプロトコルに適したパラメータを入力します。
- f. [Add] をクリックします。
- g. CE の RIP に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 9 このサービス ポリシーの RIP プロトコル設定が終了したら、[Next] をクリックします。

[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。



(注)

PE リンクが、最初は RIP ルーティング プロトコルを使用するように設定され、その後別のルーティング プロトコル (またはスタティック ルーティング) を使用するように変更される場合、Prime Provisioning は、インターフェイスに関連付けられた RIP CLI コマンドすべてを PE コンフィギュレーション ファイルから除去するわけではありません。特に、サービス要求に関連付けられた VRF が除去されない場合、Prime Provisioning は RIP コマンドのアドレス ファミリー サブコマンドを除去しません。これは、Prime Provisioning がアドレス ファミリーに基づくネットワーク クラス (つまり、ネットワーク a.0.0.0) を使用して RIP プロトコルを設定するためです。後でルーティング プロトコルが変更される場合、Prime Provisioning は同じネットワークの他のサービスを除去しません。

BGP プロトコルの選択

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) は、伝送制御プロトコル (TCP) の上でポート 179 を使用して動作します。TCP を使用することにより、BGP では信頼性が高い転送が保証されるため、BGP プロトコル自体にはどのような形式のエラー検出やエラー訂正もありません (TCP がこれらの機能を実行します)。BGP は、複数の中間ホップで分離されているピア間で動作できます。これは、ピアが必ずしも BGP プロトコルを実行していない場合も同様です。

BGP は、2 つのモード、内部 BGP (iBGP) または外部 BGP (eBGP)、のいずれかで動作します。このプロトコルは、どちらの場合でも同じパケット形式とデータ構造を使用します。iBGP は単一自律システム内の BGP スピーカー間で使用されますが、eBGP は Inter-AS リンクを介して動作します。

eBGP 拡張機能は、IPv6 およびデュアル スタック サービスの場合にサポートされます。eBGP 拡張機能は BGP ネイバーごとに設定されます。したがって、同じ VRF の IPv4 ネイバーと IPv6 ネイバーを異なる値のセットで設定できます。Prime Provisioning では、これらのパラメータを BGP ネイバーごとに設定できるようにすることにより、これを行いやすくしています。

サービス ポリシーのルーティング プロトコルとして BGP を指定するには、次の手順を実行します。

-
- ステップ 1** [Routing Protocol] ドロップダウン リストから [BGP] を選択します。
- [BGP Routing Protocol] ウィンドウが表示されます。
- ステップ 2** [CsC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。
- [CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146) で説明します。
- 前のステップで IP アドレッシング スキームが IPv6 に設定されている場合は、この属性を使用できません。
- ステップ 3** [Redistribute Static (BGP Only)] : BGP にスタティック ルートを再配布するかどうかを示します。
- BGP にスタティック ルートをインポートする場合は、このチェックボックスをオンにします。
- ステップ 4** [Redistribute Connected Routes (BGP Only)] : 直接接続されたルートを BGP に再配布するかどうかを示します。
- [Redistribute Connected] オプションをイネーブルにすると、現在のルータに接続されているインターフェイスにすべてのルートがインポートされます。ネットワークをアドバタイズするが、そのネットワークにルーティング アップデートを送信しない場合は、[Redistribute Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。

[Redistribute Connected] オプションをイネーブルにすると、接続済みルート（つまり、直接接続された PE または CE へのルート）は、その特定の VPN にあるその他すべての CE に配布されます。このオプションは、PE と CE 間のルーティングプロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティングプロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。

ステップ 5 [Default Information Originate] : ドロップダウン リストから適切なオプションを選択して、BGP スピーカー（ローカル ルータ）がネイバーにデフォルト ルートを送信するようにします。

これにより、ネイバー単位設定に `default-originate` コマンドが挿入されます。

このドロップダウン リストには 3 つの選択肢があります。

- [None]。これはデフォルトの選択肢です。ネイバー単位設定に `default-origination` コマンドは追加されません。デフォルト ルートは BGP ネイバーにアドバタイズされません。
- [Enable]。Prime Provisioning GUI に動的に表示される [Route-Policy (Default Information Origination)] フィールドでルート ポリシーの名前を指定できるようにします。ルート ポリシーでは、条件に応じてルート 0.0.0.0 を挿入できます。詳細については、次の使用方法に関する注釈を参照してください。
- [Disable]。default-originate コマンドの特性が親グループから継承されないようにします。

使用方法に関する注釈 :

- [Route-Policy (Default Information Origination)] フィールドへのルート ポリシーの入力はオプションです。
- 指定されるルート ポリシーは、そのデバイス上に事前に存在する必要があります。存在しない場合、Prime Provisioning はそのポリシーに基づくサービス要求の作成時にエラー メッセージを生成します。
- default-originate コマンドでは、ローカル ルータにデフォルト ルート (IPv4 では 0.0.0.0/0、IPv6 では ::/0) は必要ありません。ルート ポリシーを指定して default-originate コマンドを使用すると、このポリシーに一致するルートが BGP テーブルに存在する場合、デフォルト ルートがアドバタイズされます。
- [Default Information Originate] 属性は、IPv4 と IPv6 の両方のアドレス ファミリの MPLS ポリシーとサービス要求でサポートされます。これは、MPLS PE_CE と PE_No_CE の各ポリシーとサービス要求の場合にのみサポートされます。MVRFCPE ポリシーとサービス要求の場合にはサポートされません。
- [Default Information Originate] 属性は、IOS XR デバイスでのみサポートされます。
- 次の Prime Provisioning テンプレート変数は、この機能をサポートします。
 - IPv4 の場合 : PE_CE_NBR_DEFAULT_INFO_ORIGINATE_ROUTE_POLICY
 - IPv4 の場合 : PE_CE_NBR_DEFAULT_INFO_ORIGINATE
 - IPv6 の場合 : PE_CE_NBR_DEFAULT_INFO_ORIGINATE_ROUTE_POLICY_IPV6
 - IPv6 の場合 : PE_CE_NBR_DEFAULT_INFO_ORIGINATE_IPV6
- [Default Information Originate] オプションの使用法を示すサンプル コンフィグレットについては、「PE L3 MPLS VPN (BGP、Default Information Originate、IOS XR)」(P.5-219) を参照してください。

ステップ 6 [CE BGP AS ID] : カスタマーの BGP ネットワークの BGP 自律システム (AS) 番号を入力します。ここで CE に対して割り当てられる自律番号は、サービス プロバイダーのコア ネットワークの BGP AS 番号と異なっている必要があります。

有効な AS 番号の値として 2 バイト整数値がサポートされます。さらに、Prime Provisioning は、[0-65535].[0-65535] という形式のリモート 4 バイト AS 番号をサポートします。例：100.65535。このリモート 4 バイト AS 番号は、サービスポリシーとサービス要求で CE BGP AS 番号としてサポートされます。プラットフォームがリモート 4 バイト AS 番号をサポートしない場合、サービス展開は失敗します。リモート 4 バイト AS 番号は、IOS プラットフォームではサポートされませんが、IOS XR (IPv4 サービスと IPv6 サービスの両方) ではサポートされます。

ステップ 7 [Neighbor Allow-AS In] : 適切な場合は、[Neighbor Allow-AS-in] の値を入力します。

[Neighbor Allow-AS-in] 値を入力するときに、サービスプロバイダー自律システム (AS) 番号が自律システムパス内で発生する最大回数 (10 まで) を指定します。

ステップ 8 [Neighbor AS Override] : この VPN に必要な場合は、[Neighbor AS Override] オプションをイネーブルにします。

AS Override 機能を使用すると、MPLS VPN サービスプロバイダーは、カスタマーが別のサイトで同じ AS 番号を使用している場合でも、そのカスタマーとともに BGP ルーティングプロトコルを実行できます。この機能は、VPN カスタマーがプライベートまたはパブリックのいずれかの自律システム番号を使用している場合に使用できます。

[Neighbor AS-Override] オプションをイネーブルにするときに、VPN のすべてのサイトで同じ AS 番号を使用するように VPN Solutions Center を設定します。

ステップ 9 [Route Map/Policy In] : 着信ルートに適用するルートマップ (IOS デバイス) またはルートポリシー (IOS XR デバイス) を入力します。

この属性の詳細については、[ステップ 10](#) の後の使用方法に関する注釈を参照してください。



(注) この属性は、MVRFCE ポリシーとサービス要求で使用する場合はサポートされません。

ステップ 10 [Route Map/Policy Out] : 発信ルートに適用するルートマップ (IOS デバイス) またはルートポリシー (IOS XR デバイス) を入力します。



(注) この属性は、MVRFCE ポリシーとサービス要求で使用する場合はサポートされません。サービス要求内の IOS デバイス上の IPv6 の場合にもサポートされません。

IOS デバイスの使用方法に関する注釈 (BGP ルートマップ) :

- [Route Map/Policy In] 属性と [Route Map/Policy Out] 属性は、BGP を PE-CE プロトコルとして使用する IOS デバイスに対して **route-map** コマンドをサポートするために使用できます。それらの属性は、ルートフィルタリングを目的として着信ルートまたは発信ルートにルートマップを適用するために使用されます。
- テキストフィールドに入力された値は、次の設定例で示されているように、アドレスファミリまたはルータコンフィギュレーションモードの **neighbor route-map** コマンドに変換されます。

```
neighbor x.x.x.x route-map slmpls-in in
neighbor x.x.x.x route-map no-routes out
```

- これらの属性はオプションです。IOS デバイスの場合、デフォルト値は不要です。
- 次の Prime Provisioning テンプレート変数は、IOS デバイスの BGP ルートマップをサポートします。
 - PE_CE_NBR_ROUTE_MAP_IN_NAME
 - PE_CE_NBR_ROUTE_MAP_OUT_NAME

- サービス要求レベルでは、[Route Map/Policy In] 属性は、[Site of Origin] がイネーブルである場合はディセーブルで、クリアされています。[Site of Origin] 属性は、ポリシー レベルでは表示されませんが、サービス要求ワークフローでのみ（および IOS デバイスとコンフィギュレーションが CE を持たない PE で構成されている場合にのみ）表示されます。この動作の詳細については、[Site of Origin] 属性の使用方法に関する注釈を参照してください (P.5-101)。

IOS XR デバイスの使用方法に関する注釈（ルート ポリシー）：

- [Route Map/Policy In] 属性と [Route Map/Policy Out] 属性は、IOS XR デバイスに対して **route-policy** コマンドをサポートするために使用できます。これらの属性は、ボーダー ゲートウェイ プロトコル (BGP) ネイバーに対してアドバタイズまたは 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 ポリシーを適用する方法を提供します。ポリシーは、ルートをフィルタリングするか、またはルート属性を変更します。着信ルートまたは発信ルートのルーティングポリシーの名前を指定します。
- グローバルに定義された参照可能ルート ポリシー（たとえば、「pass all」）が存在しますが、[Route Map/Policy In] 属性と [Route Map/Policy Out] 属性は、それらのポリシーを独自の固有ルート ポリシーでオーバーライドする手段を提供します。
- このポリシーに基づくサービス要求を作成する前に、デバイスに対して実際のルート ポリシーを外部的に設定する必要があります。
- 次に示すように、GUI からの in/out 値は IOS XR デバイス設定に挿入されます。


```
route-policy <IN param> in
route-policy <OUT param> out
```
- これらの属性はオプションです。IOS XR デバイスの場合、値が指定されない場合、デフォルトで DEFAULT 値に設定されます。
- 次の Prime Provisioning テンプレート変数は、IOS XR デバイスの Prime Provisioning ルート ポリシー コマンドをサポートします。
 - PE_CE_BGP_Neighbor_Route_Map_Or_Policy_In
 - PE_CE_BGP_Neighbor_Route_Map_Or_Policy_Out

ステップ 11 [Neighbor Send Community] : ドロップダウン リストから次のいずれかを選択して、BGP ネイバーにコミュニティ属性を送信します。

- [None]。コミュニティ属性を BGP ネイバーに送信しません。
- [Standard]。標準コミュニティのみを BGP ネイバーに送信します。
- [Extended]。拡張コミュニティのみを BGP ネイバーに送信します。
- [Both]。標準コミュニティと拡張コミュニティの両方を BGP ネイバーに送信します。

このオプションは、PE-CE ルーティング プロトコルが BGP である場合にのみ使用できます。このオプションは、IOS デバイスと IOS XR デバイスの両方に適用できます。このオプションは、IPv4 と IPv6 両方の external BGP (eBGP; 外部 BGP) ネイバーに適用できます。



(注) この属性は、MVRFCPE ポリシーとサービス要求で使用する場合はサポートされません。

ステップ 12 CE にルーティング プロトコルを再配布するかどうかを指定します。

[Redistributed Protocols on CE] : MP-iBGP へのルートの再配布は、ルートが PE ルータと CE ルータ間の BGP 以外の手段で学習される場合にのみ必要です。これには、接続済みサブネットおよびスタティック ルートが含まれます。CE から BGP を介して学習されるルートの場合、再配布は自動的に実行されるため不要です。

BGP が CE にルーティング情報をインポートする必要があるプロトコルを指定するには、次の手順を実行します。

- a. [Redistribute Protocols on CE] オプションから、[Edit] をクリックします。

[CE Redistributed Protocol] ダイアログボックスが表示されます。

- b. [Add] をクリックします。

[CE Redistributed Protocols] ダイアログボックスが表示されます。

- c. [Protocol Type] ドロップダウン リストから、CE にインポートするプロトコルを選択します。

次のいずれかのプロトコルを選択できます。[Static]、[RIP]、[Connected] (ルート)、[IGRP]、[OSPF]、[EIGRP]、または [IS-IS]。

- Static を再配布します。BGP への再配布に **Static** ルートを選択すると、Prime Provisioning は BGP を実行している CE にスタティック ルートをインポートします。

パラメータ：パラメータは不要

- Routing Information Protocol (RIP) を再配布します。BGP への再配布に **RIP** プロトコルを選択すると、Cisco Prime Provisioning は BGP を実行している CE に RIP ルートをインポートします。

パラメータ：パラメータは不要

- Connected ルートを再配布します。BGP への再配布に **Connected** ルートを選択すると、Prime Provisioning は現在のルータに接続されているインターフェイスにすべてのルートをインポートします。ネットワークをアダプタイズするが、そのネットワークにルーティングアップデートを送信しない場合は、[Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。

パラメータ：パラメータは不要

- Interior Gateway Routing Protocol (IGRP) を再配布します。BGP への再配布に **IGRP** プロトコルを選択すると、IP Solution Center は BGP を実行している CE に IGRP ルートをインポートします。

パラメータ：IGRP 自律システム (AS) 番号

- Enhanced IGRP (EIGRP) を再配布します。BGP への再配布に **EIGRP** プロトコルを選択すると、Prime Provisioning は BGP を実行している CE に EIGRP ルートをインポートします。

パラメータ：EIGRP 自律システム (AS) 番号

- Open Shortest Path First (OSPF) を再配布します。BGP への再配布に **OSPF** プロトコルを選択すると、Prime Provisioning は BGP を実行している CE に OSPF ルートをインポートします。

パラメータ：OSPF プロセス番号

- Intermediate System-to-Intermediate System (IS-IS) を再配布します。BGP への再配布に **IS-IS** プロトコルを選択すると、Prime Provisioning は BGP を実行している CE に IS-IS ルートをインポートします。

パラメータ：IS-IS タグ番号

- d. CE の BGP に再配布するプロトコルを選択します。

- e. 選択したプロトコルに適したパラメータを入力します。

- f. [Add] をクリックします。

- g. PE の BGP に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 13 [Advertise Interval] : eBGP アドバタイズメント間隔を入力します。

値は 0 ~ 600 の範囲の整数で、アドバタイズメント間隔の秒数を指定します。デフォルト設定は、eBGP ピアの場合 30 秒です (明示的に設定されていない場合)。この eBGP 拡張機能は、IOS デバイスと IOS XR PE デバイスの両方の設定に使用できます。

ステップ 14 [Max Prefix Number] : ネイバーから受信できるプレフィックスの最大数を入力します。

使用方法に関する注釈 :

- この機能を使用すると、ピアから受信されたプレフィックスの数が制限を超えた場合に、ルータはそのピアを停止できます。
- 範囲は次のとおりです。
 - IOS デバイスの場合、1 ~ 2147483647
 - IOS XR デバイスの場合、1 ~ 4294967295
- このオプションおよび関連オプションは、IPv4 と IPv6 両方のアドレス ファミリでサポートされます。
- [Max Prefix Number]、[Max Prefix Threshold]、[Max Prefix Warning Only]、および [Max Prefix Restart] の各オプションの使用法を示すサンプル コンフィグレットについては、「[PE L3 MPLS VPN \(BGP、Maximum Prefix/Restart、IOS XR\)](#)」(P.5-214) を参照してください。

ステップ 15 [Max Prefix Threshold] : [Max Prefix Number] に設定するパーセントを指定する値を入力します。

範囲は 1 ~ 100 % で、デフォルトは 75 % です。このしきい値に達すると、ルータは警告メッセージを生成します。たとえば、[Max Prefix Number] が 20 で [Max Prefix Threshold] が 60 である場合、ネイバーからの BGP 学習ルート数が 20 の 60 %、つまり 12 ルートを超えると、ルータは警告メッセージを生成します。

ステップ 16 [Max Prefix Warning Only] : 最大プレフィックス制限を超えたときに、ルータがピアリングセッションを停止する代わりにログメッセージを生成できるようにするには、このチェックボックスをオンにします。

ステップ 17 [Max Prefix Restart] : 設定済み最大プレフィックス制限を超えたために停止したピアリングセッションをルータがいつ自動的に再確立かを指定する値 (分単位) を入力します。

有効な範囲は 1 ~ 65535 です。この機能がイネーブルのときには、ネットワーク オペレータの介入は必要ありません。この機能は、指定されている設定済み間隔でディセーブルになっているピアリングセッションの再確立を試みます。ただし、再起動タイマーの設定だけでは、送信しているプレフィックス数が超過しているピアを変更または修正できません。ネットワーク オペレータは、最大プレフィックス制限を再設定するか、そのピアから送信されるプレフィックス数を減らす必要があります。プレフィックスを過剰に送信するように設定されたピアは、ネットワークに不安定な状態をもたらす可能性があり、過剰な数のプレフィックスが急速にアドバタイズおよび除去されます。この場合、ネットワーク オペレータが問題の原因を修正する間に、再起動機能をディセーブルにするように [Max Prefix Warning Only] 属性を設定できます。

ステップ 18 このサービス ポリシーの BGP プロトコル設定が終了したら、[Next] をクリックします。

[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。

OSPF プロトコルの選択

MPLS VPN バックボーンは、純粋な OSPF エリア 0 バックボーンではありません。PE ルータ間に隣接性は形成されません。PE と CE 間のみです。MP-iBGP が PE 間で使用され、すべての OSPF ルートは VPN IPv4 ルートに変換されます。したがって、BGP にルートを再配布しても、これらのルートは同じ VPN の他のメンバー サイトにアドバタイズされる時に外部 OSPF ルートになりません。

サービス ポリシーのルーティング プロトコルとして OSPF を指定するには、次の手順を実行します。

-
- ステップ 1** [Routing Protocol] ドロップダウン リストから [OSPF] を選択します。
[OSPF Routing Protocol] ウィンドウが表示されます。
- ステップ 2** [CSC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。
[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146) で説明します。
- ステップ 3** [Give Only Default Routes to CE] : CE にデフォルト ルートのみを与えるかどうかを指定します。
[Give only default routes to CE] オプションをイネーブルにするときに、サイトが完全なルーティングまたはデフォルト ルーティングのどちらを必要とするかを示します。完全なルーティングは、VPN 内に存在するその他のルートをサイトが具体的に認識する必要がある場合です。デフォルト ルーティングは、具体的にそのサイトに対するものではないパケットをすべて VPN に送信すれば十分な場合です。
このオプションを選択すると、Prime Provisioning は、実行プロトコル RIP または EIGRP で PE ルータに対して **default-info originate** コマンド、および Static の実行プロトコル OSPF で PE ルータに対して **default-info originate always** コマンドを設定し、CE ルータに対して **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** コマンドを設定します。
- ステップ 4** [Redistribute Static (BGP only)] : OSPF にスタティック ルートを再配布するかどうかを示します。
スタティック ルートを OSPF にインポートする場合は、このチェックボックスをオンにします。
- ステップ 5** [Redistribute Connected Routes (BGP only)] : 直接接続されたルートを OSPF に再配布するかどうかを示します。
[Redistribute Connected] オプションをイネーブルにすると、現在のルータに接続されているインターフェイスにすべてのルートがインポートされます。ネットワークをアドバタイズするが、そのネットワークにルーティング アップデートを送信しない場合は、[Redistribute Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。
このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。
- ステップ 6** [Default Information Originate] : OSPF ルーティング ドメインにデフォルト外部ルートを生成するかどうかを示します。
[Default Information Originate] チェックボックスをオンにすると、その他のオプションが GUI に動的に表示されます。
a. ルーティング テーブルにデフォルト ルートがあるかどうかには関係なくデフォルト ルートをアドバタイズするには、[OSPF Default Information Originate Always] をオンにします。

- b. [Metric Value] には、デフォルト ルートの生成に使用する OSPF メトリックを入力します。範囲は 1 ~ 16777214 です。
- c. [Metric Type] では、ドロップダウン リストから次のいずれかを選択して、デフォルト ルートに関連付けられたリンク タイプを指定します。
 - None
 - Type-1 External Route
 - Type-2 External Route
- d. [Default Info Route Policy] には、ルート ポリシーの名前を入力します。

使用方法に関する注釈：

- [Default Information Originate] は、MPLS ポリシーとサービス要求ワークフローで使用できます。
- すべてのサブオプションは任意指定です。
- ルート ポリシー（指定される場合）は、そのデバイス上に事前に存在している必要があります。存在しない場合、この機能を使用してそのポリシーに基づくサービス要求を作成するときにエラーが生成されます。
- この機能は、IOS XR デバイスの場合にのみサポートされます。
- この機能は、IPv4 アドレス ファミリの場合にのみ使用できます。
- 次の Prime Provisioning テンプレート変数は、この機能をサポートします。
 - PE_CE_OSPF_METRIC_VALUE
 - PE_CE_OSPF_METRIC_TYPE
 - PE_CE_OSPF_ROUTE_POLICY
- [Default Information Originate] オプションの使用方法を示すサンプル コンフィグレットについては、「[L3 MPLS VPN \(OSPF、Default Information Originate、IOS XR\)](#)」(P.5-229) を参照してください。

ステップ 7 [OSPF Route Policy] : ルート ポリシーを入力します。

使用方法に関する注釈：

- これは、任意指定の属性です。
- この属性は、IOS デバイスおよび IOS XR PE デバイスでの IPv4 ルーティングの場合にのみサポートされます。
- この属性は、OSPF ルート ポリシーの再配布のサポートに使用されます。この属性は、次の例に示すようなデバイス設定に GUI から取得した値を挿入する手段を提供します。
- この属性を使用したポリシーに基づくサービス要求展開後の IOS XR 設定例：

```
vrf edn
rd 11.31.128.80:300
address-family ipv4 unicast
redistribute connected
redistribute ospf 3000 route-policy 'xxxx'
```

- IOS 設定例：

```
address-family ipv4 vrf edn
redistribute connected
redistribute ospf 3000 route-map <route-map>
```

- 文字列は GUI からそのまま取得されます。検証は実行されません。
- 有効なルート ポリシーが指定されていない場合、デフォルト ルート ポリシーが使用されます。

- このポリシーに基づくサービス要求を作成する前に、デバイスに対して実際のルート ポリシーを外部的に設定する必要があります。
- 次の Prime Provisioning テンプレート変数は、OSPF ルート ポリシーの再配布をサポートします。
 - PE_CE_Ospf_Route_Policy
 - PE_MVRFCE_Ospf_Route_Policy

ステップ 8 [OSPF Redistribute Match Internal/External (BGP only)] : OSPF ルートをその他のルーティング ドメインに再配布するときに使用する一致基準を設定するには、ドロップダウン リストから次のいずれかを選択します。

- [None] : ルート再配布の一致基準を指定しません。これはデフォルトです。
- [Internal only] : 自律システム (AS) に対して内部的であるルートを照合します。
- [External only] : AS に対して外部的であるルートを照合します。
- [Both] : AS に対して内部的であるルートおよび外部的であるルートを照合します。

使用方法に関する注釈 :

- この属性は、IOS デバイスおよび IOS XR PE デバイスでの IPv4 ルーティングの場合にのみサポートされます。
- OSPF 内部一致を再配布するための IOS XR 設定例 :


```
vrf edn
rd 11.31.128.80:300
address-family ipv4 unicast
redistribute connected
redistribute ospf 3000 match internal
```
- OSPF 内部一致を再配布するための IOS 設定例 :


```
address-family ipv4 vrf edn
redistribute connected
redistribute ospf 3000 match internal
```
- OSPF 外部一致を再配布するための IOS XR 設定例 :


```
vrf edn
rd 11.31.128.80:300
address-family ipv4 unicast
redistribute connected
redistribute ospf 3000 match external
```
- OSPF 外部一致を再配布するための IOS 設定例 :


```
address-family ipv4 vrf edn
redistribute connected
redistribute ospf 3000 match external 1 external 2
```
- [Both] オプションが選択されたときの IOS XR 設定例 :


```
redistribute ospf 3000 match internal external
```
- [Both] オプションが選択されたときの IOS 設定例 :


```
redistribute ospf 3000 match internal external 1 external 2
```
- このコマンドの IOS XR バリエーションには **external type 1** または **external type 2** のサポートは存在しませんが、IOS ではそのサポートが存在します。Prime Provisioning GUI には、**external type 1** または **external type 2** を指定するオプションはありません。唯一のオプションは [External only] です。生成されるコンフィグレットは、デバイスが IOS または IOS XR のどちらであるかに基づいて異なります。

- Prime Provisioning テンプレート変数 PE_CE_Ospf_Match_Internal_External は、この属性をサポートします。

ステップ 9 [OSPF Process ID on PE] : PE の OSPF プロセス ID を入力します。

OSPF プロセス ID は、単一ルータ内の各 OSPF ルーティング プロセスに割り当てられる固有の値です。このプロセス ID は PE のみに対して内部的です。この数値は、1 ~ 65535 の範囲内の任意の 10 進数、またはドット付き 10 進表記の数値のいずれかとして入力できます。



(注) OSPF プロセス ID が Prime Provisioning でどのように処理されるかについての詳細は、「[IGP の OSPF プロセス ID \(IOS XR のみ\)](#)」(P.5-70) を参照してください。

ステップ 10 [Use VRF or VPN Domain ID] : VRF または VPN から取得される OSPF ドメイン ID を使用するには、このチェックボックスをオンにします。

使用方法に関する注釈 :

- このチェックボックスをオンにしない場合、[OSPF Domain ID on PE] 属性のテキスト フィールド (GUI における次の属性) に PE の OSPF ドメイン ID の値を入力できます。
- [Use VPN or VRF Domain ID] チェックボックスをオンにすると、[OSPF Domain ID on PE] 属性のフィールドはディセーブルになります。
- OSPF ドメイン ID 機能は、PE-CE ポリシーおよび PE- NoCE ポリシーの場合にのみサポートされます。[OSPF Domain ID] 属性と [OSPF Domain ID on PE] 属性は、ポリシー タイプが PE-CE または PE-NoCE である場合にのみ GUI に表示されます。
- OSPF ドメイン ID 機能は、MultiVRF-CE ポリシーの場合はサポートされません。
- OSPF ドメイン ID は、IOS XR デバイスでのみサポートされます。IOS デバイスの場合、OSPF ドメイン ID を指定して VRF オブジェクトまたは VPN を使用すると、Prime Provisioning はこの属性を無視します。
- [OSPF Domain ID] 属性は、ルートの再配布元の OSPF ドメインを一意に識別します。このドメイン ID は、カスタマーごとに固有である必要があります。IOS デバイスの場合、IOS がプロセスごとに 1 つの VRF だけを許可するために、デフォルト動作では OSPF プロセス ID を OSPF ドメイン ID と見なします。IOS XR は、プロセスごとに複数の VRF をサポートしています。このため、IOS XR デバイスの場合、各 VRF に対して固有の OSPF ドメイン ID を明示的に設定する必要があります。OSPF プロセスごとに 1 つの VRF を設定することはできますが、これはスケーラブルなソリューションではありません。
- タイプ 0005 の OSPF ドメイン ID 設定のみがサポートされます。
- ポリシーに基づいて作成されるサービス要求の場合は、次の点に注意してください。
 - OSPF ドメイン ID 設定はオプションです。[Use VPN or VRF Domain ID] がイネーブルになっておらず、[OSPF Domain ID] フィールドに値が指定されていない場合、Prime Provisioning は OSPF ドメイン ID 設定を無視します。
 - [Use VPN or VRF Domain ID] がイネーブルの場合、プロビジョニング時に Prime Provisioning は選択された VPN オブジェクトから OSPF ドメイン ID を取得します。VPN オブジェクトで OSPF ドメイン ID が設定されていない場合、Prime Provisioning は OSPF ドメイン ID 設定を無視します。エラー メッセージは生成されません。
 - [Use VPN or VRF Domain ID] がイネーブルであり、そのリンク (外部) に対して複数の VPN が結合されている場合、Prime Provisioning は OSPF ドメイン設定を無視します。

ステップ 11 [OSPF Domain ID on PE] : OSPF ドメイン ID を 10 進形式で入力します。

使用方法に関する注釈 :

- [Use VPN or VRF Domain ID] チェックボックスがオンの場合、このフィールドはディセーブルです。前のステップの注釈を参照してください。
- 値を 10 進形式で入力します。[Hex value:] フィールドは、対応する 16 進数値を表示する編集不可のテキスト フィールドです。この 16 進数値は、実際にデバイスに表示される値です。
- OSPF ドメイン ID は、IOS XR デバイスでのみサポートされます。IOS デバイスの場合、OSPF ドメイン ID を指定して VRF オブジェクトまたは VPN を使用すると、Prime Provisioning はこの属性を無視します。

ステップ 12 [OSPF Process ID on CE] : CE の OSPF プロセス ID を入力します。

OSPF プロセス ID は、単一ルータ内の各 OSPF ルーティング プロセスに割り当てられる固有の値です。このプロセス ID は CE のみに対して内部的です。この数値は、1 ~ 65535 の範囲内の任意の 10 進数、またはドット付き 10 進表記の数値のいずれかとして入力できます。



(注) OSPF プロセス ID が Prime Provisioning でどのように処理されるかについての詳細は、「IGP の OSPF プロセス ID (IOS XR のみ)」(P.5-70) を参照してください。

ステップ 13 [OSPF Process Area Number] : OSPF プロセス領域番号を入力します。

PE の OSPF 領域番号は、指定された範囲内の任意の 10 進数、またはドット付き 10 進表記の数値のいずれかとして入力できます。

ステップ 14 [Redistributed Protocols on PE] : 必要な場合、PE に再配布されるプロトコルを指定します。



(注) 再配布の量を制限することは、OSPF 環境では重要である可能性があります。ルートを OSPF に再配布するときは、必ず外部 OSPF ルートとして再配布します。OSPF プロトコルでは OSPF ドメイン全体で外部ルートのフラディングが発生し、プロトコルのオーバーヘッドおよびその OSPF ドメインに参加しているすべてのルータの CPU 負荷が上昇します。

OSPF が PE にインポートする必要があるプロトコルを指定するには、次のステップを実行します。

a. [Redistribute Protocols on PE] オプションから、[Edit] をクリックします。

[PE Redistributed Protocol] ダイアログボックスが表示されます。

b. [Add] をクリックします。

[PE Redistributed Protocols] ダイアログボックスが表示されます。

c. [Protocol Type] ドロップダウン リストから、PE にインポートするプロトコルを選択します。

次のいずれかを選択できます。[Static]、[EIGRP]、または [RIP]。

- Static を再配布します。OSPF への再配布に **Static** ルートを選択すると、Prime Provisioning は OSPF を実行している PE にスタティック ルートをインポートします。
Static ルートを PE に再配布するために必要なパラメータやメトリックはありません。
- Enhanced IGRP (EIGRP) を再配布します。OSPF への再配布に **EIGRP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している PE に EIGRP ルートをインポートします。
パラメータ : EIGRP 自律システム (AS) 番号
メトリック : 1 ~ 16777214 の範囲内の任意の数値
- RIP を再配布します。OSPF への再配布に **RIP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している PE に RIP ルートをインポートします。
パラメータ : パラメータは不要
メトリック : 1 ~ 16777214 の範囲内の任意の数値

- d. PE の OSPF に再配布するプロトコルを選択します。
- e. 選択したプロトコルに適したパラメータを入力します。
- f. [Add] をクリックします。
- g. PE の OSPF に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 15 CE にルーティング プロトコルを再配布するかどうかを指定します。

[Redistribute Protocols on CE] : OSPF が CE にルーティング情報をインポートする必要があるプロトコルを指定するには、次のステップを実行します。

- a. [Redistribute Protocols on CE] オプションから、[Edit] をクリックします。
[CE Redistributed Protocol] ダイアログボックスが表示されます。
- b. [Add] をクリックします。
[CE Redistributed Protocols] ダイアログボックスが表示されます。
- c. [Protocol Type] ドロップダウン リストから、CE にインポートするプロトコルを選択します。
次のいずれかのプロトコルを選択できます。[Static]、[RIP]、[BGP]、[Connected] (ルート)、[IGRP]、[EIGRP]、または [IS-IS]。
 - Static を再配布します。OSPF への再配布に **Static** ルートを選択すると、Prime Provisioning は OSPF を実行している CE にスタティック ルートをインポートします。
Static ルートを CE に再配布するために必要なパラメータはありません。
 - RIP を再配布します。OSPF への再配布に **RIP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している CE に RIP ルートをインポートします。
パラメータ : パラメータは不要
 - Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) を再配布します。OSPF への再配布に **BGP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している CE に BGP ルートをインポートします。
パラメータ : BGP 自律システム (AS) 番号
 - Connected ルートを再配布します。OSPF への再配布に **Connected** ルートを選択すると、Prime Provisioning は現在のルータに接続されているインターフェイスにすべてのルートをインポートします。ネットワークをアダプタイズするが、そのネットワークにルーティング アップデートを送信しない場合は、[Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。
パラメータ : パラメータは不要
 - Interior Gateway Routing Protocol (IGRP) を再配布します。OSPF への再配布に **IGRP** (Interior Gateway Routing Protocol) を選択すると、IP Solution Center は OSPF を実行している CE に IGRP ルートをインポートします。
パラメータ : IGRP 自律システム (AS) 番号
 - Enhanced IGRP (EIGRP) を再配布します。OSPF への再配布に **EIGRP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している CE に EIGRP ルートをインポートします。
パラメータ : EIGRP 自律システム (AS) 番号
 - Intermediate System-to-Intermediate System (IS-IS) を再配布します。OSPF への再配布に **IS-IS** プロトコルを選択すると、Prime Provisioning は OSPF を実行している CE に IS-IS ルートをインポートします。
パラメータ : IS-IS タグ番号

- d. CE の OSPF に再配布するプロトコルを選択します。
- e. 選択したプロトコルに適したパラメータを入力します。
- f. [Add] をクリックします。
- g. CE の OSPF に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 16 このサービス ポリシーの OSPF プロトコル設定が終了したら、[Next] をクリックします。

[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。

IGP の OSPF プロセス ID (IOS XR のみ)



(注)

この項の情報は、IOS XR デバイスにのみ適用されます。これは、IOS XR が仮想 OSPF プロセスをサポートするためです。IOS デバイスには適用されません。

IOS XR デバイスの場合、Prime Provisioning は Interior Gateway Protocol (IGP) の OSPF プロセスを分離されたプロセスとして保持します。デフォルトでは、すべての PE-CE リンクの OSPF は別のプロセスです。その他の OSPF プロセスの場合、PE-CE VRF はその親の下にあります。

ユーザの責任で、OSPF プロセス ID を決定およびトラッキングします。Prime Provisioning は、PE-CE プロセス ID が IGP プロセス ID と異なっていることを確認し、そのプロセス ID がすでに使用されている場合は警告メッセージを表示します。

すでに IGP のために使用されている OSPF プロセス ID をユーザが指定すると、Prime Provisioning はサービス要求の展開時に警告メッセージを生成します。OSPF プロセスが VRF を参照している場合、その OSPF プロセスは使用中であると見なされます。その場合は、非 IGP プロセスと見なされます。それ以外の場合は、IGP プロセスと見なされます。

Prime Provisioning は、OSPF プロセスの最大数を設定するための DCPL プロパティを提供します。その DCPL プロパティは、Provisioning\Service\mpls\ospfProcessLimit です。この値のデフォルトは 2 です。Prime Provisioning は、設定されている OSPF プロセスの数をトラッキングします。制限を超えるか制限に達すると、サービス要求の展開時に警告メッセージが生成されます。警告メッセージの他には、制限を超えることによる影響はありません。



(注)

DCPL 制限は、すべての OSPF プロセス (IGP など) の合計を表します。OSPF プロセス ID がすでに VRF ベース OSPF プロセスとして存在していても、警告は生成されません。複数の VRF ベース OSPF プロセスが存在する場合、警告が生成されます (ospfProcessLimit にデフォルト値 2 が設定されていることを想定)。

次の設定例を参照してください。

例 : コア IGP (90)

```
router ospf 90
nsr
log adjacency changes
router-id 11.31.128.77
bfd minimum-interval 200
bfd multiplier 3
network point-to-point
nsf cisco
```

```

auto-cost reference-bandwidth 100000
redistribute rip metric 3 metric-type 1
redistribute isis ntt metric 10 metric-type 1
address-family ipv4 unicast
area 51
mpls traffic-eng
interface Loopback0
!
interface GigabitEthernet0/0/0/0
network broadcast
!
!
area 0.0.0.0
mpls traffic-eng
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
network point-to-point
!
interface GigabitEthernet0/0/0/4
network point-to-point
!
interface TenGigE0/3/0/0
!
!
mpls traffic-eng router-id Loopback0
mpls traffic-eng multicast-intact

```

例 : PE-CE VRF (3000)

```

router ospf 3000
vrf edn
log adjacency changes detail
router-id 1.1.1.77
domain-tag 77
area 0.0.0.100
bfd minimum-interval 250
bfd fast-detect
bfd multiplier 3
network point-to-point
stub
interface GigabitEthernet0/0/5/7.101
!
!
!
vrf regus
log adjacency changes detail
router-id 2.2.2.1
domain-tag 3177
network point-to-point
address-family ipv4 unicast
area 51
bfd minimum-interval 250
bfd fast-detect
bfd multiplier 3
network point-to-point
interface Loopback9000

```



(注)

ルータでルート ポリシーが使用されている場合、照合は適用されません。

EIGRP プロトコルの選択

Enhanced IGRP (EIGRP) はハイブリッドルーティング プロトコルであり、ディスタンス ベクトル プロトコルなどのネットワークを検出しますが (つまり IGRP)、高速再コンバージェンスのためにトポロジカル データベースを維持します。EIGRP は、可変長サブネット マスクと不連続サブネットをサポートします。IP に対して設定されている場合、同じ自律システム内に定義されている IGRP プロセスを使用するルートが自動的に再配布されます。デフォルトでは、EIGRP はクラスフル ネットワーク境界でサブネットを自動集約します。

EIGRP は、IGRP と同じメトリック集積を実行します。ただし、IGRP と EIGRP の間でメトリック計算を確認すると、EIGRP 値の方がかなり大きいことがわかります。EIGRP メトリックを 256 で割ると、同じ IGRP メトリック値が得られます。

EIGRP では、トポロジ変更に関与するすべてのルータを同時に同期化できます。トポロジ変更の影響を受けないルータは、再計算から除外されます。結果として、コンバージェンス時間が非常に速くなります。

サービス ポリシーのルーティング プロトコルとして EIGRP を指定するには、次の手順を実行します。

-
- ステップ 1** [Routing Protocol] ドロップダウン リストから [EIGRP] を選択します。
[EIGRP Routing Protocol] ウィンドウが表示されます。
- ステップ 2** [CSC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。
[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「[Carrier Supporting Carrier のプロビジョニング](#)」(P.5-146) で説明します。
前のステップで IP アドレッシング スキームが IPv6 に設定されている場合は、この属性を使用できません。
- ステップ 3** [Redistribute Static] : (BGP のみ) 適切な場合、[Redistribute Static (BGP only)] オプションをイネーブルにします。
BGP の場合に [Redistribute Static] オプションをイネーブルにすると、ソフトウェアはスタティック ルートをコア ネットワーク (BGP を実行) にインポートします。
- ステップ 4** [Redistribute Connected] : (BGP のみ) 適切な場合、[Redistribute Connected (BGP only)] オプションをイネーブルにします。
[Redistribute Connected] オプションをイネーブルにすると、接続済みルート (つまり、直接接続された PE または CE へのルート) は、その特定の VPN にあるその他すべての CE に配布されます。このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ PCP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。
-
-  **(注)** すべての接続済みルートが指定されたルーティング ドメインに無差別に再配布されるため、接続済みルートを再配布すると問題が発生する可能性があります。すべての接続済みルートを再配布することを望まない場合は、*distribute-list out* ステートメントを使用して、再配布する特定の接続済みルートを識別します。
-
- ステップ 5** [EIGRP Authentication KeyChain Name] : 1 つ以上のインターフェイスですべての EIGRP プロトコルトラフィックを認証するためのキーチェーン名を入力します。
使用方法に関する注釈 :

- キーチェーン名内ではスペース文字およびバックスラッシュ (\) 文字は使用できません。
- 名前が指定されない場合、EIGRP キーチェーン認証は導入されません。
- このオプションは、IPv4 と IPv6 の両方のアドレス ファミリの場合にサポートされます。
- このオプションは、IOS XR デバイスの場合にのみ使用できます。
- [EIGRP Authentication KeyChain Name] オプションの使用方法を示すサンプル コンフィグレットについては、次を参照してください。
「PE L3 MPLS VPN (EIGRP、Authentication Keychain Name、IOS XR)」(P.5-234)。

ステップ 6 [EIGRP AS ID on PE] : PE の EIGRP 自律システム ID を入力します。

これは固有の 16 ビット数値です。

ステップ 7 [EIGRP AS ID on CE] : CE の EIGRP 自律システム ID を入力します。

これは固有の 16 ビット数値です。

ステップ 8 次の説明に従って、EIGRP メトリックの値を入力します。

EIGRP メトリック

EIGRP は、IGRP の場合と同様にメトリックを使用します。ルート テーブル内の各ルートには関連付けられたメトリックがあります。EIGRP は、IGRP の場合とほとんど同様に複合メトリックを使用しますが、その複合メトリックは乗数 256 で変更されます。[Bandwidth]、[Delay]、[Load]、[Reliability]、および [MTU] は、サブメトリックです。IGRP の場合と同様に、EIGRP は、主として帯域幅と遅延、または数値が最も小さい複合メトリックに基づいて、ルートを選択します。EIGRP は、ルートに対してこのメトリックを計算する場合、ルートへの到達可能距離と呼びます。EIGRP は、ネットワーク内のすべてのルートへの到達可能距離を計算します。

[Bandwidth Metric] : 帯域幅はキロビット単位で表されます。帯域幅は、EIGRP が実行しているインターフェイスを正確に表すように静的に設定する必要があります。たとえば、56 kbps インターフェイスおよび T1 インターフェイスのデフォルトの帯域幅は 1,544 kbps です。

[Delay Metric] : 遅延はマイクロ秒単位で表されます。遅延も、EIGRP が実行しているインターフェイスを正確に表すように静的に設定する必要があります。インターフェイス上での遅延は、**delay time_in_microseconds** インターフェイス サブコマンドを使用して調整できます。

[Reliability Metric] : 信頼性は 1 ~ 255 の範囲内の動的数値です。ここで、255 は 100 % 信頼性があるリンク、1 は信頼性がないリンクです。

[Loading Metric] : 負荷は 1 ~ 255 の範囲内の数値で、インターフェイスの出力負荷を示します。この値は動的で、**show interfaces** コマンドを使用して表示できます。値 1 は負荷が最小であるリンクを示し、255 は負荷が 100 % であるリンクを示します。

[MTU Metric] : 最大伝送単位 (MTU) は、パス内に記録されている最小の MTU 値で、通常は 1500 です。



(注)

IGRP または EIGRP でルーティングの決定に影響する場合は、必ず Bandwidth に対して Delay メトリックを使用します。帯域幅の変更は、その他のルーティング プロトコル (OSPF など) に影響を与える可能性があります。遅延の変更は、IGRP と EIGRP にのみ影響を与えます。

ステップ 9 [Redistributed Protocols on PE] : 必要な場合、PE に再配布されるプロトコルを指定します。

IP に対して設定されている場合、同じ自律システム内に定義されている IGRP プロセスを使用するルートが自動的に再配布されます。デフォルトでは、EIGRP はクラスフル ネットワーク境界でサブネットを自動集約します。

EIGRP が PE にインポートする必要があるプロトコルを指定するには、次の手順を実行します。

- [Redistribute Protocols on PE] オプションから、[Edit] をクリックします。

[PE Redistributed Protocol] ダイアログボックスが表示されます。

- b. [Add] をクリックします。

[PE Redistributed Protocols] ダイアログボックスが表示されます。

- c. [Protocol Type] ドロップダウン リストから、PE にインポートするプロトコルを選択します。

次のいずれかを選択できます。[Static]、[RIP]、または [OSPF]。

- Static を再配布します。EIGRP への再配布に **Static** ルートを選択すると、Prime Provisioning は OSPF を実行している PE にスタティック ルートをインポートします。

Static ルートを PE に再配布するために必要なパラメータやメトリックはありません。

- RIP を再配布します。EIGRP への再配布に **RIP** プロトコルを選択すると、Prime Provisioning は EIGRP を実行している PE に RIP ルートをインポートします。

パラメータ : パラメータは不要

メトリック : 1 ~ 16777214 の範囲内の任意の数値

- Open Shortest Path First (OSPF) を再配布します。EIGRP への再配布に **OSPF** プロトコルを選択すると、Prime Provisioning は EIGRP を実行している PE に OSPF ルートをインポートします。

パラメータ : OSPF プロセス番号

メトリック : 1 ~ 16 の範囲内の任意の数値

- d. CE の EIGRP に再配布するプロトコルを選択します。

- e. 選択したプロトコルに適したパラメータを入力します。

- f. [Add] をクリックします。

- g. PE の EIGRP に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 10 [Redistribute Protocols on CE] : CE にルーティング プロトコルを再配布するかどうかを指定します。

EIGRP が CE にルーティング情報をインポートする必要があるプロトコルを指定するには、次の手順を実行します。

- a. [Redistribute Protocols on CE] オプションから、[Edit] をクリックします。

[CE Redistributed Protocol] ダイアログボックスが表示されます。

- b. [Add] をクリックします。

[CE Redistributed Protocols] ダイアログボックスが表示されます。

- c. [Protocol Type] ドロップダウン リストから、CE にインポートするプロトコルを選択します。

次のいずれかのプロトコルを選択できます。[Static]、[BGP]、[Connected] (ルート)、[IGRP]、[RIP]、[OSPF]、または [IS-IS]。

- Static を再配布します。EIGRP への再配布に **Static** ルートを選択すると、Prime Provisioning は OSPF を実行している CE にスタティック ルートをインポートします。

Static ルートを CE に再配布するために必要なパラメータはありません。

- Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) を再配布します。EIGRP への再配布に **BGP** プロトコルを選択すると、Prime Provisioning は OSPF を実行している CE に BGP ルートをインポートします。

パラメータ : BGP 自律システム (AS) 番号

- **Connected** ルートを再配布します。EIGRP への再配布に **Connected** ルートを選択すると、Prime Provisioning は現在のルータに接続されているインターフェイスにすべてのルートをインポートします。ネットワークをアドバタイズするが、そのネットワークにルーティングアップデートを送信しない場合は、[Connected] オプションを使用します。接続済みルートを再配布すると、すべての接続済みルートが無差別にルーティング ドメインに再配布されることに注意してください。

[Redistribute Connected] オプションをイネーブルにすると、接続済みルート（つまり、直接接続された PE または CE へのルート）は、その特定の VPN にあるその他すべての CE に配布されます。このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。

パラメータ：パラメータは不要

- Interior Gateway Routing Protocol (IGRP) を再配布します。EIGRP への再配布に **IGRP** (Interior Gateway Routing Protocol) を選択すると、IP Solution Center は EIGRP を実行している CE に IGRP ルートをインポートします。

パラメータ：IGRP 自律システム (AS) 番号

- RIP を再配布します。EIGRP への再配布に **RIP** プロトコルを選択すると、Cisco Prime Provisioning は EIGRP を実行している CE に RIP ルートをインポートします。

パラメータ：パラメータは不要

- Open Shortest Path First (OSPF) を再配布します。EIGRP への再配布に **OSPF** プロトコルを選択すると、Prime Provisioning は EIGRP を実行している CE に OSPF ルートをインポートします。

パラメータ：OSPF プロセス番号

- Intermediate System-to-Intermediate System (IS-IS) を再配布します。EIGRP への再配布に **IS-IS** プロトコルを選択すると、Prime Provisioning は EIGRP を実行している CE に IS-IS ルートをインポートします。

パラメータ：IS-IS タグ番号

- CE の EIGRP に再配布するプロトコルを選択します。
- 選択したプロトコルに適したパラメータを入力します。
- [Add] をクリックします。
- CE の EIGRP に再配布する追加のプロトコルすべてについてこのステップを繰り返し、[OK] をクリックします。

ステップ 11 このサービス ポリシーの EIGRP プロトコル設定が終了したら、[Next] をクリックします。

[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。

[None] を選択：ケーブル サービス

ケーブル リンクを操作する場合、リンクはルーティング プロトコルを実行しません。ルーティング プロトコルを不必要に指定することなくケーブル リンクを介したサービスを設定できるようにするために、サービス ポリシーのルーティング プロトコルのダイアログに [None] オプションが提供されています。

このサービス ポリシーがケーブル サービス用である場合は、次の手順を実行します。

- ステップ 1** ルーティング プロトコルのリストから [None] を選択します。
 図 5-4 に示されているようなダイアログボックスが表示されます。

図 5-4 ルーティング プロトコルの選択なし

Policy Editor

Policy Type: MPLS

PE-CE IPv4 Routing Information	Editable
Routing Protocol:	NONE <input checked="" type="checkbox"/>
CsC Support:	<input type="checkbox"/> <input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/> <input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/> <input checked="" type="checkbox"/>

Back Next Finish Close

- ステップ 2** [CSC Support] : Carrier Supporting Carrier (CSC) を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。
 [CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。CSC のプロビジョニングについては、「Carrier Supporting Carrier のプロビジョニング」(P.5-146) で説明します。
- ステップ 3** [Redistribute Static] : プロバイダー コア ネットワーク (BGP を実行) にスタティック ルートを配布する場合は、[Redistribute Static (BGP only)] チェックボックスをオンにします。
- ステップ 4** [Redistribute Connected] : ケーブル リンクにはルーティング プロトコルが存在しないため、VPN 内のその他すべての CE に接続済みルートを再配布することを推奨します。これを行うには、[Redistribute Connected (BGP only)] チェックボックスをオンにします。
 [Redistribute Connected] オプションをイネーブルにすると、接続済みルート (つまり、直接接続された PE または CE へのルート) は、その特定の VPN にあるその他すべての CE に配布されます。このオプションは、PE と CE 間のルーティング プロトコルが BGP 以外のプロトコルである場合は iBGP 用です。たとえば、ルーティング プロトコルが RIP、OSPF、EIGRP、または Static である場合は、このオプションは、MPLS コアの PE で設定されているルータ BGP 用です。PE ルータでは、MPLS 用に常に実行されているルータ BGP プロセスが 1 つ存在します。このオプションは BGP 用でもあります。
- ステップ 5** 必要な設定値の指定が完了したら、[Next] をクリックします。
 [MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「VRF および VPN の情報の定義」(P.5-76) を参照してください。

VRF および VPN の情報の定義

サービス ポリシーのルーティング プロトコルの定義が完了したら、このサービス ポリシーについて VRF および VPN の情報を指定する必要があります。これを行うには、次の手順を実行します。

- ステップ 1** 図 5-5 に示されているような、[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。

図 5-5 VRF 情報の指定

Policy Editor

Policy Type: MPLS

VRF Information		Editable				
Use VRF Object:	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>				
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>				
Maximum Routes (32-5000000):	<input type="text"/>	<input checked="" type="checkbox"/>				
Maximum Route Threshold (1-100):	80	<input checked="" type="checkbox"/>				
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>				
BGP Multipath Information						
BGP Multipath Load Sharing:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
BGP Multipath Action:	eBGP	<input checked="" type="checkbox"/>				
Maximum Paths (1-32) * :	22	<input checked="" type="checkbox"/>				
Import Paths (1-32):	22	<input checked="" type="checkbox"/>				
Allocate New Route Distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
VRF And RD Overwrite:	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
VPN Selection						
PE VPN Membership:		<input checked="" type="checkbox"/>				
#	Customer	VPN	Provider	Route Target	Is Hub	
						Add Delete
						Back Next Finish Close

Note: * - Required Field

ステップ 2 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。

この機能の詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。

VRF オブジェクト機能を使用していない場合は、次の手順の説明に従って VRF および VPN の属性を定義します。

ステップ 3 [Export Map] : 必要な場合は、エクスポート ルート マップの名前を入力します。

ここで入力するエクスポート ルート マップの名前は、PE に存在しているエクスポート ルート マップの名前である必要があります。



(注)

IOS は、エクスポート ルート マップを VRF ごとに 1 つのみサポートします。したがって、エクスポート ルート マップは VPN ごとに 1 つのみ存在できます。

Prime Provisioning ソフトウェアを使用して管理 VPN を定義するときに、Prime Provisioning は管理 VPN のエクスポート ルート マップを自動的に生成します。Cisco IOS はエクスポート ルート マップを VRF ごとに 1 つのみサポートし、そのルート マップは管理 VPN 用に予約されているため、VRF が管理 VPN に含まれる場合は [Export Map] フィールドは使用不可です。

エクスポート ルート マップはフィルタを適用しません。エクスポート ルート マップを使用して、ルートに関連付けられているルート ターゲットのデフォルトセットをオーバーライドできます。

ステップ 4 [Import Map] : インポート ルート マップの名前を入力します。

ここで入力するインポート ルート マップの名前は、PE に存在しているインポート ルート マップの名前である必要があります。



(注) IOS は、インポート ルート マップを VRF ごとに 1 つのみサポートします。したがって、インポート ルート マップは VPN ごとに 1 つのみ存在できます。

インポート ルート マップはフィルタを適用します。したがって、この PE の VRF から特定のルートを除外するには、送信ルータにエクスポート ルート マップを設定して現在の VRF にインポートできるルート ターゲットが含まれないようにするか、または PE にインポート ルート マップを作成してそのルートを除外します。

ステップ 5 [Maximum Routes] : この PE の VRF にインポートできるルートの最大数を指定します。



(注) [Maximum Routes] の値が設定された後は、Prime Provisioning は別の値をプロビジョニングすることを許可しません。VRF は複数のインターフェイス (リンク) で使用される可能性があるため、この値がリンクに対して設定された後は、その値を手動で変更しないことを推奨します。この VRF を使用する既存または新規サービス要求の最大ルート数の値を変更しようとする、Prime Provisioning はエラーを生成します。

ステップ 6 [Maximum Route Threshold] : 最大ルート数のしきい値を指定します。

指定された最大ルート数を超えると、Prime Provisioning は警告メッセージを送信します。

ステップ 7 [VRF Description] : オプションで、現在の VPN の VRF の説明を入力できます。

ステップ 8 [BGP Multipath Load Sharing] : BGP マルチパス ロード シェアリングおよび最大パス設定をイネーブルにするには、このチェックボックスをオンにします。

このオプションの使用の詳細については、「[BGP マルチパス ロード シェアリングおよび最大パス設定](#)」(P.5-80) を参照してください。

ステップ 9 [Allocate New Route Distinguisher] : ルート識別子 (RD) は、各 IPv4 ルートに付加される 64 ビットの数値であり、VPN で固有である IP アドレスが MPLS コアでも固有であるようにします。この拡張アドレスは、VPN-IPv4 アドレスとも呼ばれます。

[Allocate New Route Distinguisher] がイネーブルで、一致する VRF 設定がその PE に存在しない場合は、新規 VRF を作成します。存在する場合は再利用します。

[Allocate New Route Distinguisher] がディセーブルである場合、PE の範囲全体にわたって最初の一致する VRF 設定を検出します (PE には無関係)。設定されている PE でこの VRF が検出された場合は、再利用します。PE で検出されない場合は、作成します。



(注) すでに別の PE ルータで設定されている VRF をサービス要求が取得する可能性があります。

Prime Provisioning はルート ターゲット (RT) および RD の値を自動的に設定しますが、代わりに [VRF and RD] チェックボックスをオンにすることにより独自の値を割り当てることができます。



(注)

VPN の作成時に固有ルート識別子機能をイネーブルにした場合、[Allocate New Route Distinguisher] オプションはディセーブルです。詳細については、「VPN の固有ルート識別子のイネーブル化」(P.5-12) を参照してください。

ステップ 10 [VRF and RD Overwrite] : [VRF and RD Overwrite] オプションをイネーブルにすると、図 5-6 に示されているように、このダイアログボックスに 2 つの新規フィールドが表示され、デフォルトの VRF 名およびルート識別子の値を上書きできます。



注意

正しく行わない場合、VRF 名およびルート識別子のデフォルト値を変更すると、現在実行中のサービス要求が変更されるかディセーブルになる可能性があります。これらの変更は、絶対に必要な場合のみ注意をして行ってください。



(注)

VPN の作成時に固有ルート識別子機能をイネーブルにした場合、[VRF and RD Overwrite] オプションはディセーブルです。詳細については、「VPN の固有ルート識別子のイネーブル化」(P.5-12) を参照してください。

図 5-6 [VRF and RD Overwrite] オプション

VRF And RD Overwrite:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VRF Name:	<input type="text" value="VRF 3"/>	<input checked="" type="checkbox"/>
RD Value:	<input type="text" value="100:45"/>	<input checked="" type="checkbox"/>

238807

- [VRF Name] : 新規 VRF 名を入力します。次の特殊文字は使用しないことを推奨します (' ` " < > () [] { } \ / & ^ ! ? ~ * % = , . + |)。これにより、特定のデバイスの VRF 名に誤設定が生じる可能性があるためです。
- [RD Value] : 新規 RD 値を入力します。



(注)

MPLS サービス要求では、[VRF and RD Overwrite] 属性の下のサブ属性（つまり、[VRF Name] 属性と [RD Value] 属性）に一度値を指定してサービス要求を保存すると、これらのフィールドは両方ともディセーブルになり、編集不可になります。[VRF Name] および [RD Value] のデフォルト値を変更すると、現在実行中のサービス要求を変更またはディセーブルにする可能性があるために、この動作は導入されました。したがって、展開済みサービス要求でこれらの値を変更する必要がある場合の回避策は、そのサービス要求をデコミッションおよび削除し、新規サービス要求を作成することです。まだ展開されていない新規サービス要求の場合、サービス要求を強制的に削除してから新規値を使用して新規サービスを作成する必要があります。

ステップ 11 [PE VPN Membership] : チェックボックスで、このサービス ポリシーに関連付けられる VPN を指定します。

[PE VPN Membership] の情報には、カスタマー名、VPN 名、サービス プロバイダー名、CE ルーティング コミュニティ名、および CERC タイプがハブ アンド スポーク CERC またはフル メッシュ CERC のどちらであるかが含まれます。

[Is Hub] チェックボックスがオンの場合、CERC タイプがハブ アンド スポークであることを示します。

[Add] ボタンまたは [Delete] ボタンを使用して、このリストに VPN を追加、またはこのリストから VPN を削除できます。

- ステップ 12** テンプレートおよびデータ ファイルがポリシーをサポートできるようにするには、[Next] ボタンをクリックして [Template Association] ウィンドウにアクセスし、「[ポリシーのテンプレートの関連付けのイネーブル化](#)」(P.5-83) を参照してテンプレートおよびデータ ファイルの処理方法の詳細を参照します。
- ステップ 13** VRF および VPN の選択に満足したら、[Finish] をクリックします。
[Policies] ウィンドウが表示されます。

MPLS PE-to-CE サービスのサービス ポリシーが定義されたため、サービス オペレータはこのポリシーを使用して PE-CE リンクのサービス要求を作成および展開できるようになりました。詳細については、[次を参照してください。「MPLS VPN サービス要求」](#) (P.5-83)

BGP マルチパス ロード シェアリングおよび最大パス設定

Prime Provisioning は、外部 BGP (eBGP)、内部 BGP (iBGP)、外部/内部 BGP (eiBGP) の場合に、ボーダー ゲートウェイ プロトコル (BGP) マルチパス ロード シェアリングの設定をサポートします。BGP マルチパス ロード シェアリングの追加サポートとして、MPLS は、バーチャルプライベート ネットワーク (VPN) および Virtual Route Forwarding (VRF; 仮想ルーティング転送) テーブルに対して、プロバイダー エッジ (PE) ルータごとに固有ルート識別子 (RD) を設定することもできます。[図 5-7](#) に示されているように、[BGP Multipath Load Sharing] オプションを使用すると、BGP マルチパス ロード シェアリングをイネーブルまたはディセーブルにできます。

図 5-7 [VRF and VPN Membership] ウィンドウのマルチパス設定オプション

BGP Multipath Load Sharing:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BGP Multipath Action:	<input type="text" value="eBGP"/>	<input checked="" type="checkbox"/>
Maximum Paths (1-32) * :	<input type="text" value="22"/>	<input checked="" type="checkbox"/> 2-3880.08
Import Paths (1-32):	<input type="text" value="22"/>	<input checked="" type="checkbox"/>

[BGP Multipath Load Sharing] チェックボックスがオンの場合、BGP マルチパス アクション、最大パス数、インポートパス数、および不等コストルート数に対する追加のフィールドが表示されます。追加のフィールドは、選択した [BGP Multipath Action] オプションに基づいて GUI に動的に表示されません。

既存の BGP マルチパス設定がない場合、これらのフィールドを使用してマルチパス ロード シェアリングを指定すると、PE の VRF に対して新規マルチパス BGP 設定が作成されます。BGP マルチパス設定がすでに存在する場合、このアクションは既存の設定を新規マルチパス値で上書きします。除去オプションを使用すると、PE の VRF の特定タイプの既存 BGP マルチパス設定をすべて削除できます。
[BGP Multipath Load Sharing] チェックボックスがオフの場合、BGP マルチパス アクションは実行されません。サービス要求に定義されているマルチパス設定を除去する方法については、「[マルチパス設定の除去](#)」(P.5-82) を参照してください。

既存の MPLS サービス要求で BGP マルチパス設定が編集されると、同じ VPN メンバーシップを持つ同じデバイス上のすべての MPLS サービス要求は [Requested] 状態に移行します。これにより、IPv4 および IPv6 のマルチパス設定の同期が保たれます。



(注) IOS XR デバイスの BGP マルチパス サポートについては、「[IOS XR デバイスの BGP マルチパス サポート](#)」(P.5-82) を参照してください。

BGP マルチパスは、IPv6 およびデュアル スタック サービスの場合にサポートされます。BGP マルチパス設定は、VPN Routing/Forwarding (VRF; VPN ルーティング/転送) インスタンスに対して設定されます。したがって、1 つのパラメータ セットのみを IPv4 サービスと IPv6 サービスの両方に対して設定できます。

次の項では、[BGP Multipath Action] ドロップダウン リストで選択される BGP のタイプで決定される各マルチパス シナリオを説明します。ドロップダウン リストで選択可能なオプションは次のとおりです。

- [eBGP] : eBGP のマルチパス設定を指定します。これはデフォルトの選択肢です。
- [iBGP] : iBGP のマルチパス設定を指定します。
- [eiBGP] : eBGP と iBGP 両方のマルチパス設定を指定します。このオプションを使用すると、eBGP と iBGP 両方に対して最大パス数とインポートパス数の共通の共有値を設定できます。
- [eBGP+iBGP] : eBGP と iBGP 両方のマルチパス設定を指定します。このオプションを使用すると、eBGP と iBGP の両方に対して最大パス数とインポートパス数を別々に設定できます。
- [Remove] : PE の VRF に対する既存の BGP マルチパス設定をすべて削除します。

これらの各シナリオについて、次に説明します。



(注)

[MPLS Link Editor - VPN and VRF] ウィンドウでのサービス要求の作成時に、[BGP Multipath Load Sharing] チェックボックスがオンの場合、[Force Modify Shared Multipath Attributes] という追加の BGP 属性が GUI に表示されます。この属性の目的は、その他のリンクで使用されている共有 VRF 属性を強制的に変更できるようにすることです。このフィールドは持続されません。この属性は、サービス要求作成時にのみ表示され、ポリシー作成時には表示されません。

eBGP マルチパス

[eBGP] オプションを選択すると、[Maximum Paths] フィールドと [Import Paths] フィールドが表示されます。それぞれの説明は次のとおりです。

- [Maximum Paths] : ルーティング テーブルで許可されるルートの最大数を指定します。
- [Import Paths] : VRF のバックアップ マルチパスとして設定できる冗長パスの数を指定します。



(注)

eBGP マルチパス設定をセットアップするときに、[Maximum Paths] または [Import Paths] のいずれかの値を設定する必要があります。両方のフィールドをブランクにすることはできません。

iBGP マルチパス

[iBGP] オプションを選択すると、[Maximum Paths] フィールド、[Import Paths] フィールド、および [Unequal Cost] フィールドが表示されます。それぞれの説明は次のとおりです。

- [Maximum Paths] : ルーティング テーブルで許可されるルートの最大数を指定します。iBGP マルチパス設定をセットアップするときに値を指定する必要があります。
- [Import Paths] : VRF のバックアップ マルチパスとして設定できる冗長パスの数を指定します。
- [Unequal Cost] : 不等コスト マルチパスをイネーブルまたはディセーブルにします。不等コスト マルチパスを使用すると、複数の不等コスト パス間でトラフィックを配布し、全体のスループットと信頼性を大きくできます。

eiBGP マルチパス

[eiBGP] オプションを選択すると、[Maximum Paths] フィールドと [Import Paths] フィールドが表示されます。それぞれの説明は次のとおりです。

- [Maximum Paths] : ルーティング テーブルで許可されるルートの最大数を指定します。eiBGP マルチパス設定をセットアップするときに値を指定する必要があります。
- [Import Paths] : VRF のバックアップ マルチパスとして設定できる冗長パスの数を指定します。

eiBGP+iBGP マルチパス

[eiBGP+iBGP] オプションを選択すると、[Maximum Paths] フィールド、[Import Paths] フィールド、および [Unequal Cost] フィールドが表示されます。それぞれの説明は次のとおりです。

- [Maximum Paths] : ルーティング テーブルで許可されるルートの最大数を指定します。ルートの数は、eBGP と iBGP に対して別々に指定できます。
- [Import Paths] : VRF のバックアップ マルチパスとして設定できる冗長パスの数を指定します。パスの数は、eBGP と iBGP に対して別々に指定できます。
- [Unequal Cost] : 不等コスト マルチパスをイネーブルまたはディセーブルにします。不等コスト マルチパスを使用すると、複数の不等コスト パス間でトラフィックを配布し、全体のスループットと信頼性を大きくできます。



(注)

マルチパス ロード シェアリングをサポートするには、VPN (VRF) の各 PE ルータに固有 Route Distinguisher (RD; ルート識別子) が必要です。この目的は、同じ RD が異なるカスタマーに割り当てられないようにすることです。これにより、同じ RD を同じ VRF に使用できます。つまり、PE 内のすべてのサイトが同じ固有 RD を持つことができます。固有 RD 機能はオプションです。これは、グローバル VPN レベルとサービス要求レベルの両方でイネーブルです。VPN の PE ごとの固有 RD をイネーブルにするために、[Create VPN] ウィンドウには新しい [Enable Unique Route Distinguisher] フィールドが含まれています。この機能の使用の詳細については、「VPN の固有ルート識別子のイネーブル化」(P.5-12) を参照してください。

IOS XR デバイスの BGP マルチパス サポート

IOS XR デバイスでの BGP マルチパス設定のために、Prime Provisioning では次の属性がサポートされています。

- [Maximum Paths] : IOS XR の場合、この属性の範囲は 2 ~ 8 です。範囲外の値が指定されると、サービス要求を保存できず、エラーが表示されます。サービス要求は [Invalid] 状態に移行しません (展開の実行時に発生します)。
- [Unequal Cost] : この属性は iBGP の場合にのみサポートされます。

[Import Paths] 属性は、IOS ではサポートされますが、IOS XR ではサポートされません。

マルチパス設定の除去

[BGP Multipath Action] 属性のドロップダウン リストで [Remove] オプションを選択することにより、マルチパス設定を除去できます。[Remove] オプションは、PE の VRF のマルチパス設定を除去します (以前に設定されている場合)。

サービス要求がマルチパス設定とともに保存されていて、その設定を除去する必要がある場合、[Remove] オプションを使用する必要があります。



(注)

マルチパス設定は、単に [BGP Multipath Load Sharing] チェックボックスをオフにしても除去できません。これを除去するには、[BGP Multipath Action] 属性を [Remove] に設定してから、そのサービス要求を保存する必要があります。[BGP Multipath Load Sharing] チェックボックスは、マルチパス設定を除去した後でのみオフにしてください。

ポリシーのテンプレートの関連付けのイネーブル化

Prime Provisioning テンプレート機能は、MPLS サービス要求内のリンクに設定されているデバイスにフリーフォーマットの CLI をダウンロードする手段を提供します。テンプレートをイネーブルにすると、テンプレートおよびデータ ファイルを使用して、現在は Prime Provisioning でサポートされていないコマンドをダウンロードできます。

ステップ 1 ポリシーのテンプレートの関連付けをイネーブルにするには、[MPLS Policy Editor - VRF and VPN Membership] ウィンドウで [Next] ボタンをクリックします。



(注) 追加のウィンドウが [Template Association] ウィンドウの前にポリシー ワークフローに表示されます。このウィンドウを使用して、ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザー定義の属性を作成することもできます。追加情報機能の使用方法に関する背景情報については、[付録 F 「サービスに情報を追加する方法」](#) を参照してください。この機能を使用しない場合は、[Next] をクリックして [Template Association] ウィンドウに進むか、[Finish] をクリックしてポリシーを保存します。

[Template Association] ウィンドウが表示されます。このウィンドウで、テンプレート サポートをイネーブルにして、任意でテンプレートとデータ ファイルをポリシーに関連付けることができます。テンプレートをポリシーに関連付ける方法、およびこのウィンドウでの機能の使用方法については、[第 9 章 「テンプレートおよびデータ ファイルの管理」](#) を参照してください。

ステップ 2 付録の手順に従ってポリシーのテンプレートおよびデータ ファイルのセットアップが完了したら、[Template Association] ウィンドウで [Finish] をクリックして閉じます。

[Policies] ウィンドウが表示されます。

MPLS PE-to-CE サービスのサービス ポリシーが定義されたため、サービス オペレータはこのポリシーを使用して PE-CE リンクのサービス要求を作成および展開できるようになりました。詳細については、[次を参照してください。第 5 章 「MPLS VPN サービス要求」](#)

MPLS VPN サービス要求

ここでは、次の項目について説明します。

- 「サービス拡張」 (P.5-84)
- 「Prime Provisioning がネットワーク デバイスにアクセスする方法」 (P.5-84)
- 「MPLS VPN サービス要求の作成例」 (P.5-85)
- 「IOS から IOS XR への PE デバイスの移行」 (P.5-103)

ネットワーク デバイスに MPLS VPN ポリシーを適用するには、サービス要求を展開する必要があります。サービス要求を展開する際、Prime Provisioning はリポジトリ (Prime Provisioning データベース) のデバイス情報と現在のデバイス設定を比較して、コンフィグレットを生成します。さらに、サービス要求でさまざまなモニタリングや監査タスクを実行します。すべてのタイプの Prime Provisioning サービス要求に適用される共通タスクについては、[第 8 章 「サービス要求の管理」](#) で説明されています。これらのタスクの詳細についてはその項を参照してください。

サービス拡張

MPLS VPN Management のこのリリースでは、サービス機能への多数の機能拡張を使用できます。

- サービスが、同時に単一の PE-CE リンクに制限されることはなくなりました。Prime Provisioning では、サービスはサービス要求ごとに複数の PE-CE リンクで構成できます。

- マルチキャスト MPLS VPN

マルチキャストアドレスは、マシンのグループを表す 1 つのアドレスです。ただし、ブロードキャストアドレスとは異なり、マルチキャストアドレスを使用するマシンはすべて、アドレスに送信されたメッセージを受信しようとします。ブロードキャストアドレスに送信されたメッセージは、そのメッセージの内容が考慮されるかどうかに関係なく、すべての IP 通信マシンによって受信されます。たとえば、一部のルーティングプロトコルは、定期的なルーティングメッセージの宛先としてマルチキャストアドレスが使用されます。これにより、ルーティング更新が不要なマシンはこれを無視できるようになります。

マルチキャストルーティングを実装するために、Prime Provisioning で、マルチキャストトラフィックを互いに送信できるインターフェイスと関連付けられた一連の VRF であるマルチキャストドメイン (MD) の概念を採用します。VRF には、ユニキャスト用の VPN ルーティング/転送情報が含まれます。マルチキャストルーティングをサポートするために、VRF にはマルチキャストルーティングおよび転送情報も含まれています。これは、マルチキャスト VRF と呼ばれます。

- Site of Origin サポート

ルートターゲットは、どの VRF がルートを受信する必要があるかを特定するメカニズムは提供しますが、ルーティングループを防止する機能は提供しません。サイトから特定されたルートがアドバタイズされてそのサイトに戻る場合、これらのルーティングループが発生する可能性があります。これを防ぐために、Site of Origin (SOO) 機能はどのサイトがルートに起因しているのかを特定するために、どのサイトが他の PE ルータからルートを受信してはならないのかを特定します。



(注) Prime Provisioning グラフィカル ユーザ インターフェイス (GUI) は、以前は IOS デバイスの Site of Origin の eBGP のサイトをサポートしていました。このリリースでは、さらに IOS XR PE デバイスの IPv4 EBGP ネイバーに対する EBGP Site of Origin がサポートされています。

- MPLS VPN へのレイヤ 2 アクセス
- PE-Only サービス要求のプロビジョニング

Prime Provisioning がネットワーク デバイスにアクセスする方法

Prime Provisioning がルータにアクセスを試みる時は、次のアルゴリズムを使用します。

1. ターミナル サーバがデバイスに関連付けられているかどうかを確認し、それが当てはまる場合、Prime Provisioning がターミナル サーバを使用してデバイスにアクセスするかどうかを確認します。
2. ターミナル サーバがない場合は、Prime Provisioning はデバイスの管理インターフェイスを検索します。
3. 管理インターフェイスがない場合、Prime Provisioning は完全修飾ドメイン名 (ドメイン名とホスト名) を使用してデバイスにアクセスしようとします。

VPN Solutions Center のデバイスアクセス アルゴリズムのいずれかのステップに失敗する場合は、デバイス アクセス動作全体が失敗します。使用可能な再試行またはロールオーバー動作はありません。たとえば、ターミナル サーバがあるときに、Prime Provisioning がターミナル サーバを介したターゲット デバイスへのアクセス試行でエラーが発生した場合は、その時点でアクセス動作は失敗します。ターミナル サーバ アクセス方法が失敗すると、Prime Provisioning はターゲット デバイスにアクセスするための管理インターフェイスの検索を試行しません。

MPLS VPN サービス要求の作成例

サービス要求は、カスタマー エッジ ルータ (CE) とプロバイダー エッジ ルータ (PE) 間のサービス契約のインスタンスです。サービス要求のユーザ インターフェイスは、CE および PE ルータ、ルーティング プロトコル情報、および IP アドレス指定情報に関する特定のインターフェイスなど、いくつかのパラメータを入力するように要求します。または、Prime Provisioning テンプレートをサービス要求と統合し、1 つ以上のテンプレートを CE および PE に関連付けることもできます。サービス要求を作成するには、「MPLS VPN サービス ポリシー」(P.5-42) で説明されているように、サービス ポリシーがすでに定義されている必要があります。



(注)

このマニュアルの後続の章では、これらやその他の MPLS VPN サービス要求の設定例についてさらに説明します。「標準 PE-CE リンクのプロビジョニング」(P.5-104) および「マルチ VRFCE PE-CE リンクのプロビジョニング」(P.5-115) も参照してください。

MPLS VPN トポロジの例

図 5-8 には、この項のサービス要求の定義に使用されるネットワークのトポロジが示されています。

PE-CE の例

PE-CE の例では、サービス プロバイダーは、カスタマー サイト Acme_NY (ニューヨーク) の CE (mlce1) の MPLS サービスを作成する必要があります。

Multi-VRF の例

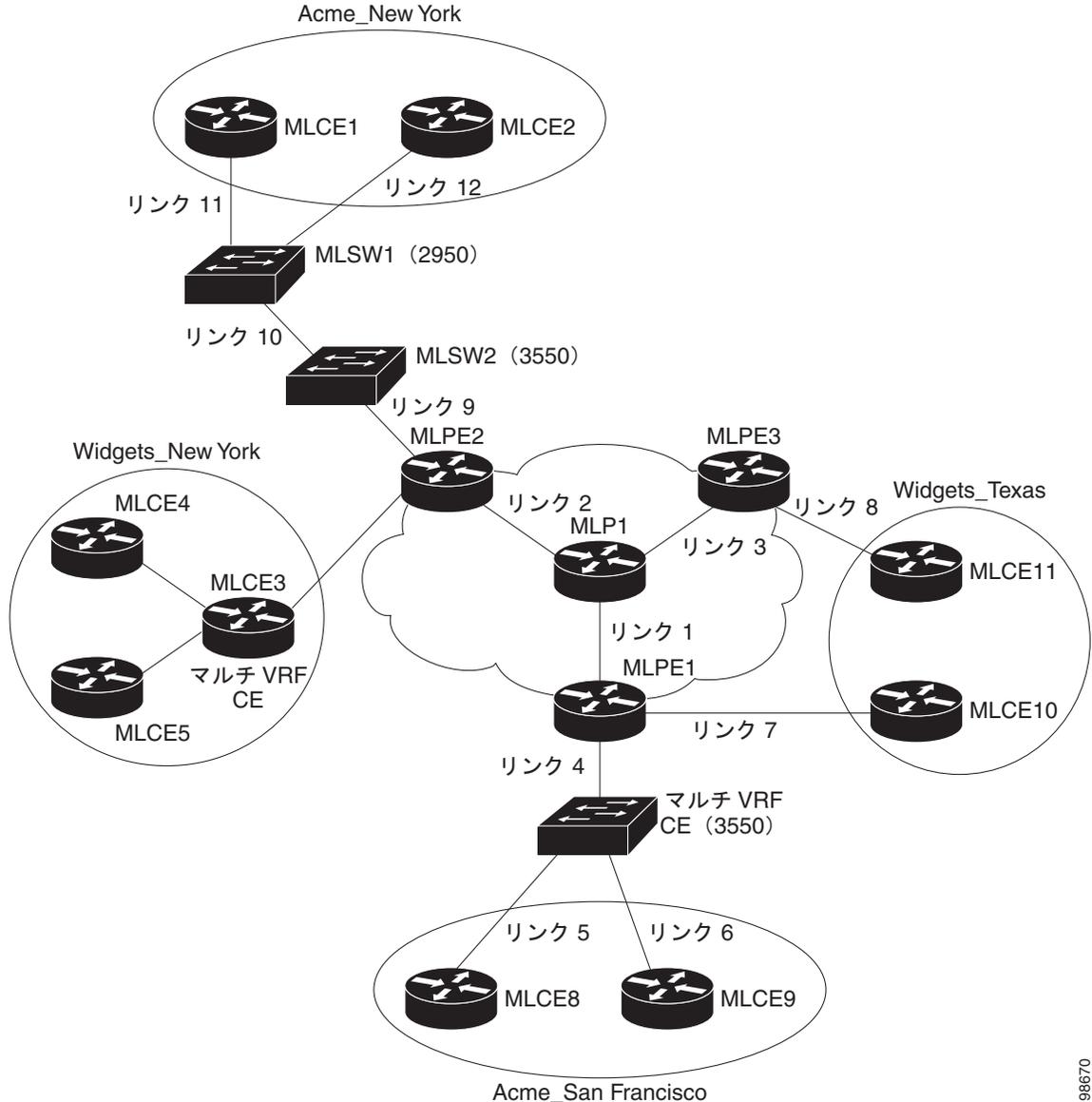
マルチ VRF の例では、サービス プロバイダーは、カスタマー サイト Widgets_NY (ニューヨーク) の CE (mlce4) とカスタマー サイト Widgets_NY (ニューヨーク) にあるマルチ VRFCE (mlce3) 間に MPLS サービスを作成する必要があります。

目的は、ニューヨークのカスタマー サイトと PE (mlpe2) 間のリンクを定義する単一のサービス要求を作成することです。

PE-Only の例

PE-Only 例では、サービス プロバイダーは、PE (mlpe2) に対して MPLS サービスを作成する必要があります。

図 5-8 ネットワーク トポロジの例



98670

MPLS VPN PE-CE サービス要求の作成

MPLS VPN PE-CE サービス要求を作成する例については、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] > [Create] を選択します。
- ステップ 2** 目的のポリシーを選択して、[OK] をクリックします。
[MPLS Service Request Editor] が表示されます。
- ステップ 3** [Add Link] をクリックします。
これで、[MPLS Service Request Editor] に一連のフィールドが表示されるようになりました。[Select CE] フィールドがイネーブルであることを確認します。このサービスのリンクの定義に必要な最初のタスクは、リンクの CE を指定することです。

- ステップ 4** [CE] : [Select CE] をクリックします。
[Select CPE Device] ウィンドウが表示されます。
- [Show CPEs with] ドロップダウン リストから、[CEs by Customer Name]、[by Site]、または [by Device Name] を表示できます。
 - [Find] ボタンを使用して、特定の CE の検索または表示の更新のいずれかを行うことができます。
 - [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。
 - このダイアログボックスには、現在定義されている CE デバイスのリストの最初のページが表示されます。情報のページ数は、ダイアログボックスの右下隅に表示されます。CE デバイスの別のページに移動するには、移動先のページ番号をクリックします。
- ステップ 5** [Select] 列で、MPLS リンクの CE の名前を選択して、[Select] をクリックします。
[Service Request Editor] ウィンドウに戻ります。ここで、選択した CE の名前が [CE] 列に表示されるようになります。
- ステップ 6** [CE Interface] : インターフェイス選択機能を使用して、CE インターフェイスを選択します。
[PE] 列で、[Select PE] オプションがイネーブルになっていることに注意してください。

Bundle-Ether インターフェイスの使用に関する注意事項

次の使用上の注意事項が Bundle-Ether インターフェイスに適用されます。

- 対応するポリシーで指定されたインターフェイス タイプに基づいて、IOS XR デバイス用の Bundle-Ether インターフェイスを選択できます。
- Bundle-Ether インターフェイスは、1 つ以上の Bundle-Ether インターフェイスが選択した PE デバイスで事前に設定されている場合に、サービス要求のみに表示されます。つまり、ポート チャネルはサービス要求を作成する前に、デバイスで事前に設定する必要があります。ポート チャネル インターフェイスは VRF の終了に使用されます。
- リンクは、IPv4 または IPv6 のいずれかにすることができます。次の点に注意してください。
 - Cisco キャリア ルーティング システム 1 (CRS-1) ルータでは、IPv4 と IPv6 の両方のリンクがサポートされます。マルチキャストは IPv6 ではサポートされません。詳細については、次のリンクを参照してください。
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8/interfaces/command/reference/hr38lbun.html#wp1410649
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8/multicast/configuration/guide/mc38mcst.html#wp1168111
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8/multicast/configuration/guide/mc38mcst.html#wp1290965
 - Cisco 12000 (別名ギガビット スイッチ ルータまたは GSR) では、IPv4 リンクのみがサポートされます。これは、デバイスの制限です。詳細については、次のリンクを参照してください。
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/lnkbnld.html
- バンドルされた物理インターフェイス機能を持つ複数のネイバーおよびピアリングは、MVRFC サービス要求ではサポートされていません。

- ステップ 7** [PE] : [Select PE] をクリックします。
[Select PE Device] ダイアログボックスが表示されます。
- [Show PEs with] ドロップダウン リストから [Customer Name]、[Site]、または [Device Name] ごとに PE を表示できます。

- b. [Find] ボタンを使用して、特定の PE の検索または表示の更新のいずれかを実行できます。
- c. [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。
- d. このダイアログボックスには、現在定義されている PE デバイスのリストの最初のページが表示されます。情報のページ数は、ダイアログボックスの右下隅に表示されます。
PE デバイスの別のページに移動するには、移動先のページ番号をクリックします。

ステップ 8 [Select] 列で、MPLS リンクの PE の名前を選択して、[Select] をクリックします。
[Service Request Editor] ウィンドウに戻ります。選択した PE の名前が [PE] 列に表示されています。

ステップ 9 [PE Interface] : インターフェイス選択機能を使用して、PE インターフェイスを選択します。
[Link Attribute] の [Add] オプションがイネーブルになっていることを確認します。
Bundle-Ether インターフェイスの指定に関する詳細については、「[Bundle-Ether インターフェイスの使用に関する注意事項](#)」(P.5-87) の項を参照してください。

ステップ 10 [Link Attribute] 列で [Add] をクリックします。
[MPLS Link Attribute Editor] ウィンドウが表示され、インターフェイス パラメータのフィールドが表示されます。
このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE および CE インターフェイス フィールドの詳細については、「[PE および CE インターフェイス パラメータの指定](#)」(P.5-45) を参照してください。

[VLAN ID] および [Second VLAN ID] 属性に関する注意事項

VLAN ID は PE および CE で共有されるため、両方で 1 個の VLAN ID です。

[Second VLAN ID] は、PE インターフェイスでの着信フレームの Q-in-Q の 2 番目の VLAN タグを照合する方式を提供するオプションの属性です。

使用方法に関する注釈 :

- この属性は、MVRFCPE ポリシーに基づくサービス要求には使用できません。
- この属性はポリシー レベルでは存在せず、サービス要求の作成中に設定する必要があります。2 つめの VLAN ID に対応する自動選択のオプションがないため、値を指定する必要があります。これは、1 ~ 4094 の整数にする必要があります。
- この属性は、標準 PE-CE リンクに対してのみ適用できます。これは CE が存在するかどうかに関係なくサポートされます。これは、管理対象と管理対象外の両方の CE デバイスでサポートされます。
- この属性は、PE インターフェイスのカプセル化タイプが dot1q である場合のみ適用できます。その他のカプセル化タイプについては、この属性は GUI に表示されません。
- この機能は、限られたプラットフォーム (Q-in-Q 照合をサポートするもののみ) に対してのみ使用できます。2 つめの VLAN ID を持つサービス要求がサポートされていないプラットフォームに展開されると、展開は失敗します。このような場合、オペレータは 2 番目の VLAN ID を削除してサービスを再展開できます。IP アドレスも変更中に削除され、再展開されるため、この操作はサービスに影響を及ぼします。
- 2 つめの VLAN ID を使用してサービス要求を作成すると、IOS デバイスに次のコマンドが表示されます。

```
encapsulation dot1q VLAN_ID second-dot1q SECOND_VLAN_ID
```

- 2 つめの VLAN ID を使用してサービス要求を作成すると、IOS XR デバイスに次のコマンドが表示されます。

```
dot1q vlan VLAN_ID SECOND_VLAN_ID
```

- Prime Provisioning は、2 つめの VLAN を適用しません。これは、PE インターフェイスで一致する 2 つめの VLAN のみをサポートします。
- 2 つめの VLAN ID 属性は、テンプレート変数 (*Second_PE_Vlan_ID*) として使用できます。
- 2 番めの VLAN ID および Q-in-Q のサポートの詳細については、次の各項を参照してください。
 - 「CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS)」 (P.5-189)
 - 「CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS XR)」 (P.5-191)
 - 「よくあるご質問」 (P.5-254)

ステップ 11 この特定のリンクに対して変更する必要があるインターフェイス値があれば編集し、[Next] をクリックします。

[MPLS Link Attribute Editor] で [IP Address Scheme] が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。[IP Address Scheme] フィールドの詳細については、「[IP アドレス スキームの指定](#)」 (P.5-48) を参照してください。

ステップ 12 この特定のリンクで変更する必要があるすべての IP アドレス スキーム値を編集し、[Next] をクリックします。

[MPLS Link Attribute Editor for Routing Information] ウィンドウが表示されます。

このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE および CE に関するルーティング情報の詳細については、「[サービスのルーティング プロトコルの指定](#)」 (P.5-51) を参照してください。

このサービスに使用されているサービス ポリシーによってルーティング プロトコルが編集可能と指定されているため、必要に応じてこのサービス要求のルーティング プロトコルを変更できます。



(注) スタティック ルーティング プロトコルには、Link Attribute Editor を使用して追加できる 2 つの追加属性があります。「[スタティック ルーティング プロトコル属性の設定 \(IPv4 と IPv6\)](#)」 (P.5-96) を参照してください。

ステップ 13 この特定のリンクに対して変更する必要があるルーティング プロトコル値があれば編集し、[Next] をクリックします。



(注) このインターフェイスがデュアル スタック (IPv4 と IPv6) である場合、IPv4 と IPv6 両方のルーティング情報を個別に入力するようにプロンプトが表示されます。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。VRF および VPN の情報の詳細については、「[VRF および VPN の情報の定義](#)」 (P.5-76) を参照してください。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、[第 5 章「独立 VRF 管理」](#) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。

ステップ 14 マルチキャストがイネーブルの場合、PIM (Protocol Independent Multicast) モードを選択します。

- SPARSE_MODE

- SPARSE_DENSE_MODE



ヒント

マルチキャスト ルーティング アーキテクチャでは、IP マルチキャスト ルーティングを既存の IP ネットワークに追加できます。PIM は、独立したユニキャスト ルーティング プロトコルです。Dense および Sparse の 2 つのモードで動作できます。

ステップ 15 この特定リンクに対して変更する必要がある VRF および VPN の値があれば編集します。



(注)

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウにあるほとんどの属性は、ポリシー ワークフローの [VRF and VPN Member] ウィンドウに含まれています。共通属性の詳細については、「[VRF および VPN の情報の定義](#)」(P.5-76) を参照してください。ただし、サービス要求に VRF および VPN 属性を定義している場合、いくつかの違いがあります。サービス要求の作成中の VRF および VPN 属性の定義については、「[MPLS サービス要求での VRF および VPN 属性の定義](#)」(P.5-91) を参照してください。

ステップ 16 テンプレートまたはデータ ファイルをサービス要求に関連付ける場合は、[Next] ボタンをクリックします。

[Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。

テンプレートをサービス要求に関連付ける手順、およびこの機能のこのウィンドウでの使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#) を参照してください。デバイスのテンプレートおよびデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じて [Service Request Editor] ウィンドウに戻ります。

ステップ 17 テンプレートを追加しなかった場合は、[MPLS Link Editor - VRF and VPN] ウィンドウで [Finish] をクリックします。

[MPLS Service Request Editor] に戻ります。前の手順で概要を示した手順に従って、このサービス要求に複数のリンクを定義できます。

ステップ 18 サービス要求のこの最初のリンクの作業を保存するには、[Save] をクリックします。

[Service Requests] ウィンドウに戻ります。これで、定義したリンクの情報が表示されるようになります。

ご覧のように、サービス要求は [Requested] 状態にあります。このサービスにすべてのリンクが定義されている場合、「[IOS から IOS XR への PE デバイスの移行](#)」(P.5-103) で説明されているように、サービスを展開する必要があります。



(注)

デフォルトでは、Prime Provisioning システムのすべてのサービス要求が [Service Request] ウィンドウに表示されます。[Show Services with]、[matching]、および [of type] ドロップダウン リストからさまざまな項目を選び、[Find] ボタンをクリックすることで、表示するサービス要求のリストをフィルタリングすることができます。



(注)

ACTIVATION、L3MPLSVPN、および VPN ライセンスのみが Prime Provisioning にインストールされている場合、使用されている VPN に基づいてすべてのサービス要求を表示することはできません ([Show Services with] ドロップダウン リストで [VPN Name] を選択します。[Type] は [All] です)。こ

れに対する回避策は、MPLS VPN タイプに基づいてサービス要求を表示することです ([of type] ドロップダウンリストで [MPLS VPN] を選択します)。この問題は、すべての Prime Provisioning ライセンスがインストールされている場合は発生しません。

MPLS サービス要求での VRF および VPN 属性の定義

[MPLS Link Attribute Editor - VRF and VPN] で使用できる大部分の属性は、MPLS ポリシー ワークフローの [VRF and VPN Member] ウィンドウの説明で示されています。これらの共通属性の定義および使用については、「MPLS VPN サービス ポリシー」(P.5-42) の「VRF および VPN の情報の定義」(P.5-76) を参照してください。ただし、VRF と VPN 属性をサービス要求に定義する場合には、いくつかの相違点があります。MPLS サービス要求が VPN を使用しているかどうかに応じた事例、または MPLS サービス要求が独立 VRF オブジェクトを使用している事例、の 2 つの事例に注意します。これらの事例については、以下の項で別個に説明します。

ケース 1 : VPN の使用

サービス要求が VPN を使用している場合、RD フォーマットおよび RD Overwrite 属性を使用してサービス要求に MPLS VPN リンクを作成できます。

次の操作を行ってください。

- ステップ 1** [Use VRF Object] : このチェックボックスはオフのままにします。
- このチェックボックスをオンにすると、このウィンドウにほとんどの属性が表示されなくなります。これについては、次の項「ケース 2 : 独立 VRF オブジェクトの使用」(P.5-94) で説明します。
- ステップ 2** [RD Format] : ドロップダウンリストから RD フォーマットを選択します。選択できる基準は、次のとおりです。

- [RD_AS] : AS フォーマットのルート識別子。これはデフォルトです。
- [RD_IPADDR] : IP アドレス形式のルート識別子。

使用方法に関する注釈 :

- RD_IPADDR を RD フォーマットとして選択すると、GUI が更新され、新しい属性 [RD IP Address Value] が表示されます。
- 表示されたテキストフィールドに [RD IP Address Value] を手動で入力することも、サービス要求で使用される PE デバイスのループバック IP アドレスを選択することもできます。後者を行う場合、[Select Loopback IP] ボタンをクリックして、ダイアログボックスから目的のループバック インターフェイスを選択します。
- 入力した IP アドレスは、Prime Provisioning によって検証されます。
- 基本的な IPv4 アドレスのみを使用できます。ネットワーク プレフィックスは許可されません。
- RD は、各プロバイダーの RD プールから選択した VPN ID にこの IP アドレスを追加することで形成されます。



(注) RD_IPADDR を RD フォーマットとして選択し、65535 より大きい VPN ID を持つ VPN を使用すると、サービス要求は [Failed Deploy] 状態に移行します。これは、RD 値の最初の部分が IP アドレス (32 ビット) である場合に、RD の 2 番目の部分が 16 ビットしかない可能性があるからです (これは、1 ~ 65535 までの値と等しい)。

- [RD] オプションは、後でサービス要求を編集するとディセーブルになります。

- RD IP アドレスに「manual/loopback IP」エントリを持つ、同じ VPN を使用する複数のサービス要求が複数の PE に展開されると、固有の RD を持つ新しい VRF が作成されます。これは、[RD IP Address] (manual/loopback IP) が、さまざまなデバイスに対して異なる可能性があるからです。
- 次の Prime Provisioning テンプレート変数は RD フォーマットをサポートしています。
 - RD_FORMAT
 - RD_IPADDRESS

ステップ 3 [RD Format] の選択に基づいて、[Unique Route Distinguisher:] および [Allocate New Route Distinguisher:] チェックボックスをオンにします。

ステップ 4 PE VPN メンバーシップ：このサービス ポリシーに関連付けられた VPN を指定します。

使用方法に関する注釈：

- [PE VPN Membership] の情報には、カスタマー名、VPN 名、サービス プロバイダー名、ルート ターゲット名、ルート ターゲット タイプ、およびルート ターゲット タイプがハブ アンド スポーク ルート ターゲットまたはフル メッシュ ルート ターゲットのどちらであるかが含まれます。
- 同じ PE を使用するサービス要求ですでに使用されている VPN を選択すると、同じ RD フォーマットと RD の IP アドレスが新しいサービス要求用に選択され、[RD Format] と [RD IP Address Value] 属性がディセーブルになります。
- IPv4、IPv6、または「デュアル スタック」（IPv4 と IPv6 の両方）VPN を選択すると、追加属性 ([Enable IPv4 Multicast] および [Enable IPv6 Multicast]) が VRF および VPN のウィンドウに表示されます。
- [CERC Type] 属性使用の詳細については、「[MPLS サービス要求への独立した IPv4 と IPv6 ルート ターゲットの追加](#)」(P.5-92) の項を参照してください。

既存のサービス要求から新しい RD フォーマットへの移行

RD フォーマットを使用できるように既存のサービス要求を移行するには、次の手順を実行する必要があります。

- サービス要求をデコミッションします。
- [RD Format] を使用してサービス要求を再運用します。または、[VRF and RD Overwrite:] チェックボックスをオンにして新しいフォーマット (*ip_address:vpn_id*) を使用して [RD Value] を上書きします。



(注)

[VRF and RD Overwrite] 属性の下にあるサブ属性（つまり、[VRF Name] および [RD Value] 属性）に値を指定し、MPLS サービス要求を保存すると、これらの両方のフィールドがディセーブルになり、編集できなくなります。[VRF Name] と [RD Value] のデフォルト値を変更すると、現在実行中のサービス要求を変更またはディセーブルにしてしまう可能性があるために、この動作が導入されました。したがって、展開済みサービス要求でこれらの値を変更する必要がある場合の回避策は、そのサービス要求をデコミッションおよび削除し、新規サービス要求を作成することです。まだ展開されていない新規サービス要求の場合、サービス要求を強制的に削除してから新規値を使用して新規サービスを作成する必要があります。

MPLS サービス要求への独立した IPv4 と IPv6 ルート ターゲットの追加

Prime Provisioning は、ルート ターゲットでは独立した IPv4 および IPv6 Route Target (RT; ルート ターゲット) をサポートしています。[Route Targets Type] 属性を使用してこの機能を設定できます。

使用方法に関する注釈：

- サービス要求の作成中に、[VRF and VPN] ウィンドウの [PE VPN Membership] セクションでルートターゲットの RT タイプを指定できます。これは、[Route Targets Type] 列のドロップダウンリストで指定されます。リスト内では、次を選択できます。
 - [IPv4]。[IPv4] を選択すると、対応するルート ターゲットがデバイス設定の **ipv4 address-family CLI** に適用されます。
 - [IPv6]。[IPv6] を選択すると、対応するルート ターゲットがデバイス設定の **ipv6 address-family CLI** に適用されます。
 - [IPv4 and IPv6] (デュアル スタック)。[IPv4 and IPv6] を選択すると、同じ RT が両方のアドレス ファミリに適用されます。
- [Route Targets Type] ドロップダウン リストで選択できる項目は、サービス要求に対して選択された IP アドレッシング スキームによって異なります。これは、MPLS リンク エディタ ワークフローの [IP Addressing Scheme] ウィンドウの [IP Number Scheme] 属性によって決まります。
- アドレス ファミリとして IPv4 および IPv6 を選択する場合、ルート ターゲットのタイプは次のいずれかにする必要があります。
 - 1 つのルート ターゲット : IPv4 および IPv6
 - 2 つ (以上) の個々のルート ターゲット : 少なくとも 1 つのタイプが IPv4 で、もう一方のタイプが IPv6
 このように設定しなければ、Prime Provisioning はエラーを出します。
- 既存のサービス要求が IPv4 のみに展開されていて、後でサービス要求をデュアルスタック (IPv4 および IPv6) に変更した場合は、Prime Provisioning はアドレス ファミリに基づいて追加したルート ターゲットのタグgingを変更します。これは、サービス要求が IPv6 からデュアルスタックに変更された場合にも適用されます (IPv4 および IPv6)。
- ルート ターゲット タイプが変更されている場合、サービス要求を変更するときに、ルート ターゲット /VPN も追加または削除できます。
- VPN アソシエーションがポリシー レベルで設定され、編集不可として指定されているときに、このポリシーを使用してサービス要求を作成する場合、ポリシーで選択されていたアドレス ファミリに基づいて、ルート ターゲット タイプのタグ付けが決定されます。
- 既存のデュアルスタック (IPv4 および IPv6) サービス要求が IPv4 または IPv6 アドレス ファミリに変更された場合、Prime Provisioning はルート ターゲット タグgingを選択したアドレス ファミリに自動的に変更します。
- Prime Provisioning は、同じ VPN を使用している他のサービス要求が同じ PE 上にあるかどうかを確認し、他のサービス要求によって使用されている RT が変更または削除されないようにします。
- IPv4 および IPv6 用の独立 RT 機能は、[VRF and RD Overwrite] オプションでサポートされます。
- IPv4 と IPv6 用の独立 RT 機能は、MVRFCSE サービス要求ではサポートされていません。
- IPv4 および IPv6 用の独立 RT 機能は、独立 VRF を使用する、独立した VRF サービス要求および MPLS サービス要求ではサポートされていません。
- この機能は、DCPL プロパティ GUI\MplsVPN\UniqueRTFeatureEnable を介して制御されます。このプロパティのデフォルト値は false です。IPv4 または IPv6 用の独立 RT 機能を使用するには、DCPL プロパティを true に設定する必要があります。DCPL プロパティを介して機能を制御すると、他のお客様 (つまり、この機能を使用したくないお客様) のフローが影響を受けないようになります。この機能を使用したいお客様は、DCPL プロパティを介してイネーブルにできます。
- 独立 RT では、次のテンプレート型変数がサポートされています。
 - MPLSExportRouteTargets : IPv4 アドレス ファミリで RT をエクスポートするためのテンプレート型変数。

- MPLSImportRouteTargets : IPv4 アドレス ファミリで RT をインポートするためのテンプレート型変数。
 - MPLSExportRouteTargets_IPV6 : IPv6 アドレス ファミリで RT をエクスポートするためのテンプレート型変数。
 - MPLSImportRouteTargets_IPV6 : IPv6 アドレス ファミリで RT をインポートするためのテンプレート型変数。
- 次に、テンプレート型変数をテンプレート ファイルで使用する例を示します。

```
vrf MyVRF2
address-family ipv4 unicast
import route-target
#foreach($name in $MPLSImportRouteTargets)
$name
#end
export route-target
#foreach($name in $MPLSExportRouteTargets)
$name
#end
address-family ipv6 unicast
import route-target
#foreach($name in $MPLSImportRouteTargets_IPV6 )
$name
#end
export route-target
#foreach($name in $MPLSExportRouteTargets_IPV6 )
$name
#end
```

- この機能のコンフィグレット例については、「[PE L3 MPLS VPN \(Outgoing Interface + Next Hop IP Address、Static Route Configuration、IOS XR、および IOS\)](#)」(P.5-251) を参照してください。

ケース 2 : 独立 VRF オブジェクトの使用

サービス要求が独立 VRF オブジェクトを使用している場合、この項で説明するように RD の属性を指定できます。VRF オブジェクトの作成、VRF サービス要求の操作、および MPLS VPN ポリシーおよびサービス要求での VRF オブジェクトの使用に関する一般的説明については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。

次の操作を行ってください。

-
- ステップ 1** [Use VRF Object] : この属性のチェックボックスをオンにします。
このチェックボックスをオンにすると、このウィンドウにほとんどの属性が表示されなくなります。
 - ステップ 2** [VRF Object] : [Select] ボタンをクリックして以前に作成した VRF オブジェクトを選択します。
[Select Independent VRF] ウィンドウが表示されます。
 - ステップ 3** オプション ボタンをクリックして、VRF オブジェクトを選択します。
 - ステップ 4** [Unique RD] : 一意の RD を割り当てる、また VPN のすべての PE の各 VRF に一意の RD を確実に割り当てるには、このチェックボックスをオンにします。



(注) Prime Provisioning 内の固有の RD 機能の詳細については、「[VPN の固有ルート識別子のイーネブル化](#)」(P.5-12) を参照してください。

- ステップ 5** [Select] をクリックして VRF オブジェクト選択を確認します。

[VRF and VPN] ウィンドウが再表示され、選択した VRF オブジェクトが [VRF Object] フィールドに表示されます。

使用方法に関する注釈：

- IP アドレス形式の RD (RD_IPADDR) を持ち、[Autopick RD] がイネーブルになっている VRF オブジェクトを選択すると、VRF を選択するときに RD 値が *IP:vpn_id* の形式で表示されます。また、manual RD を入力すると、*ip_address:vpn_id* の形式になります。*ip_address* は IPv4 アドレスで、*vpn_id* は 4 バイトの整数値です。
- 独立 VRF オブジェクトの作成中に RD_IPADDR を RD フォーマットとして選択し、[Autopick RD] をイネーブルにした場合、表示されているテキスト フィールドに手動で [RD IP Address Value] を入力するか、[Select Loopback IP] ボタンをクリックしてサービス要求に使用されている PE デバイスのループバック IP アドレスを選択することができます。
- 入力した IP アドレスは、Prime Provisioning によって検証されます。基本的な IPv4 アドレスのみを使用できます。ネットワーク プレフィックスは許可されません。
- RD は、各プロバイダーの RD プールから選択した VPN ID にこの IP アドレスを追加することで形成されます。
- 入力した IP アドレスを使用する RD を使用して VRF サービス要求を展開すると、[RD IP Address Value] フィールドはディセーブルになり変更できません。
- 同じ PE を使用するサービス要求ですでに使用された VRF を選択した場合、同じ [RD IP Address Value] が既存のサービス要求に対して選択されます。[RD IP Address Value] オプションはディセーブルになっています。
- デバイスですでに展開された VRF オブジェクトの場合に [RD Format] を新しいフォーマットに変更することは、次の条件下に限り可能です。
 - すべての関連 MPLS サービス要求がデコミッションされ、削除されます。
 - VRF サービス要求がデコミッション、削除、および再展開されている。
- 固有の RD を VRF 対応にすることができます。

ステップ 6 [Next] をクリックして MPLS リンク属性の設定を続けます。

MPLS VPN サービス要求の生成したコンフィグレットの表示

MPLS VPN サービス要求によって PE および CE デバイスで生成されたコンフィグレットを表示するには、次の手順を実行します。

- ステップ 1** 正常に展開したサービス要求の PE および CE コンフィグレットを表示するには、[Service Request] ウィンドウで表示するサービス要求を選択し、[Details] をクリックします。
- 関連付けられたジョブ番号に対応する [Service Request Details] ウィンドウが表示されます。
- ステップ 2** [Service Request Details] ウィンドウで [Configlets] をクリックします。
- [Service Request Configlets] ウィンドウが表示されます。
- ステップ 3** 目的のコンフィグレットの IP アドレスを選択し、[View Configlet] をクリックします。

展開されたサービス要求のデバイス コンフィグレットの表示については、「サービス要求コンフィグレットの表示」(P.8-5) を参照してください。サンプル コンフィグレットについては、「サンプル コンフィグレット」(P.5-172) を参照してください。

スタティック ルーティング プロトコル属性の設定 (IPv4 と IPv6)

スタティック ルーティング プロトコルの場合、サービス ポリシーで指定できる属性に加え、Link Attribute Editor を介して追加できる追加属性があります。

- [Advertised Routes for CE]: IP アドレスのリスト、CE サイトのすべてのアドレス空間を記述する PE に置くスタティック ルートの追加を許可します。
- [Routes to Reach other Sites]: IP アドレスのリスト、VPN 全体のアドレス空間すべてを記述する CE におくスタティック ルートの追加を許可します。

IPv4 ルーティング情報

IPv4 ルーティング情報を設定するには、次の手順を実行します。

-
- ステップ 1** 「MPLS VPN PE-CE サービス要求の作成」(P.5-86) の項の **ステップ 12** をスタティック ルーティング プロトコルに実行すると、[MPLS Link Attribute Editor] で [Routing Information] が表示されます。
- [Advertised Routes for CE:] および [Routes to Reach other Sites:] は、このサービス要求用に編集できます。
- ステップ 2** [Advertised Routes for CE:] を編集するには、[Edit] をクリックします。
- [Advertised Routes] ウィンドウが表示されます。
- ステップ 3** [Add] をクリックして IP アドレスを追加します。
- [Advertised Routes] ウィンドウが再表示されます。
- ステップ 4** IP アドレスおよびメトリックを入力します。
- ステップ 5** [Add] をクリックしてもう 1 つの IP アドレスを追加するか、[OK] をクリックします。
- ステップ 6** [Routes to Reach Other Sites] を編集するには、[Edit] をクリックします。
- [Routes to reach other sites] ウィンドウが表示されます。
- ステップ 7** [Add] をクリックして IP アドレスを追加します。
- [Routes to reach other sites] ウィンドウが再表示されます。
- ステップ 8** IP アドレスおよびメトリックを入力します。
- ステップ 9** [Add] をクリックしてもう 1 つの IP アドレスを追加するか、[OK] をクリックします。
- ステップ 10** [Next Hop Option:] を次から選択します。
- USE_OUT_GOING_INTF_NAME
 - USE_NEXT_HOP_IPADDR
 - OUTGOING_INTF_NAME+NEXT_HOP_IPADDR
- この選択項目の詳細については、「スタティック ルート設定でサポートされる発信インターフェイス名 + ネクスト ホップ IP アドレス」(P.5-97) を参照してください。
- ステップ 11** 必要に応じて、IP アドレス (IPv4 フォーマット) を [Next Hop IP Address:] フィールドに入力します。
-

IPv6 ルーティング情報

IPv6 ルーティング情報を設定するには、次の手順を実行します。

-
- ステップ 1** 「MPLS VPN PE-CE サービス要求の作成」(P.5-86) の項の **ステップ 12** をスタティック ルーティング プロトコルに実行すると、[MPLS Link Attribute Editor] で [Routing Information] が表示されます。

[Advertised Routes for CE:] は、このサービス要求用に編集できます。

- ステップ 2** [Advertised Routes for CE:] を編集するには、[EDIT] をクリックします。
[Advertised Routes] ウィンドウが表示されます。
- ステップ 3** [Add] をクリックして IP アドレスを追加します。
[Advertised Routes] ウィンドウが再表示されます。
- ステップ 4** IP アドレスおよびメトリックを入力します。
- ステップ 5** [Add] をクリックしてもう 1 つの IP アドレスを追加するか、[OK] をクリックします。
- ステップ 6** [Add] をクリックして IP アドレスを追加します。
- ステップ 7** [Add] をクリックしてもう 1 つの IP アドレスを追加するか、[OK] をクリックします。
- ステップ 8** [Next Hop Option:] を次から選択します。
- USE_OUT_GOING_INTF_NAME
 - USE_NEXT_HOP_IPADDR
 - OUTGOING_INTF_NAME+NEXT_HOP_IPADDR
- この選択項目の詳細については、「[スタティック ルート設定でサポートされる発信インターフェイス名 + ネクスト ホップ IP アドレス](#)」(P.5-97) を参照してください。
- ステップ 9** 必要に応じて、IP アドレス (IPv6 フォーマット) を [Next Hop IP Address:] フィールドに入力します。
IPv6 アドレスの入力でサポートされるフォーマットの詳細については、「[MPLS VPN ポリシー](#)」(P.5-37) を参照してください。

スタティック ルート設定でサポートされる発信インターフェイス名 + ネクスト ホップ IP アドレス

Prime Provisioning には、スタティック ルーティング プロトコル用の MPLS サービス要求を作成するときに、発信インターフェイス名とネクスト ホップ IP アドレスを指定する機能が備わっています。これは、MPLS サービス作成ワークフローで、[MPLS Link Attribute Editor - IPv4/IPv6 Routing Information] ウィンドウにある [Next Hop Option] 属性のドロップダウンリストから [OUTGOING_INTF_NAME+NEXT_HOP_IPADDR] を選択することで行います。

サービス要求作成時に、[MPLS Link Attribute Editor - IPv4/IPv6 Routing Information] ウィンドウでルーティング プロトコル属性を設定します。[Routing Protocol] 属性に [STATIC] を設定する場合、ウィンドウには [Next Hop Option] を含む関連する属性が表示されます。

使用方法に関する注釈：

- [Next Hop Option] ドロップダウン リストから [OUTGOING_INTF_NAME+NEXT_HOP_IPADDR] を選択すると、発信インターフェイス名およびネクスト ホップ IP アドレスが指定可能になります。Prime Provisioning では、スタティック ルート設定でこのフォーマットを次の形式でサポートしています。
network_address + outgoing_interface_name + next_hop_address
例：69.82.224.99/32 GigabitEthernet0/0/0/0 66.174.25.0.
- このフォーマットは次でサポートされています。
 - PE_CE および PE_NO_CE サービス要求
 - IPv4 および IPv6 のアドレッシング
 - IOS および IOS XR デバイス
- この機能は、PE デバイスにのみ設定されます。

- CE の属性の [Advertise Routes] の [Edit] ボタンをクリックして、ネットワーク アドレスを設定できます。
- 次のテンプレート型変数がサポートされています。
 - IPv4 アドレス ファミリ :
 - Advr_Routes_IP_Address : IPv4 アドレス ファミリのネットワーク IPv4 アドレス。
 - Advr_Routes_Metric : IPv4 アドレス ファミリのメトリック値。
 - STATIC_NEXT_HOP_IP_ADDR : IPv4 アドレス ファミリのネクスト ホップ IPv4 IP アドレス。
 - IPv6 アドレス ファミリ :
 - Advr_Routes_IPV6_Address : IPv6 アドレス ファミリのネットワーク IPv6 アドレス。
 - Advr_Routes_Metric_IPV6 : IPv6 アドレス ファミリのメトリック値。
 - STATIC_NEXT_HOP_IPV6_ADDR : IPv6 アドレス ファミリのネクスト ホップ IPv6 IP アドレス。
- 次に、IOS デバイスに対してテンプレート型変数をテンプレート ファイルで使用する例を示します。


```
ip route vrf V2:TempIOS $Advr_Routes_IP_Address 255.255.255.255 $PE_Intf_Name
$STATIC_NEXT_HOP_IP_ADDR $Advr_Routes_Metric
```
- 次に、IOS XR デバイスに対してテンプレート型変数をテンプレート ファイルで使用する例を示します。


```
router static
  vrf V21:TempIOSXR
    address-family ipv4 unicast
      $Advr_Routes_IP_Address $PE_Intf_Name $STATIC_NEXT_HOP_IP_ADDR
    $Advr_Routes_Metric
  !
  address-family ipv6 unicast
    $Advr_Routes_IPV6_Address $PE_Intf_Name $STATIC_NEXT_HOP_IPV6_ADDR
  $Advr_Routes_Metric_IPV6
```
- この機能のコンフィグレット例については、「[PE L3 MPLS VPN \(Outgoing Interface + Next Hop IP Address, Static Route Configuration, IOS XR, および IOS\)](#) (P.5-251) を参照してください。

マルチ VRF サービス要求の作成

MPLS-VPN では、セキュリティおよびプライバシーをプロバイダー ネットワークを通過するトラフィックとして提供します。CE ルータには、従来の LAN ネットワーク全体のプライベート ネットワークを保障するメカニズムがありません。従来、プライバシーを提供するためには、スイッチを展開する必要があり、また各クライアントを異なる VLAN に配置していました。または、異なる CE ルータが各クライアントの組織ごともしくは PE に属する IP アドレス グループごとに必要でした。これらのソリューションでは、追加の装置が必要であり、また各クライアント サイトのネットワーク管理とプロビジョニングがより必要であったため、カスタマーにとって高価でした。

Cisco IOS Release 12.2(4)T で導入されたマルチ VRF では、これらの問題に対処します。マルチ VRF は、制限された PE 機能を MPLS-VPN モデルの CE ルータに拡張します。MPLS-VPN のプライバシーおよびセキュリティを PE ルータ ノードだけでなく、ブランチ オフィスにも拡張して提供するために、CE ルータは異なる VRF テーブルを保持できるようになりました。

CE ルータは VRF インターフェイスを使用して、カスタマー側に VLAN と同様の設定を形成します。CE ルータ上の各 VRF は、PE ルータ上の VRF にマッピングされます。マルチ VRF では、CE ルータは VRF インターフェイスのみを設定でき、VRF ルーティング テーブルをサポートしています。

Multi-VRF は CE ルータに PE 機能の一部を拡張します。ラベル交換や、LDP 隣接関係がなく、PE と CE の間にラベル付きパケットのフローはありません。PE のような機能でサポートされているのは、CE ルータに複数の VRF を持てる機能だけです。これにより、異なるルーティングを決定できます。パケットは、IP パケットとして PE に送信されます。

マルチ VRFCE PE-CE サービス要求を作成するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] > [Create] を選択します。
 - ステップ 2** [MPLS Policy] を選択し、[OK] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
 - ステップ 3** [Add Link] をクリックします。
 - ステップ 4** [Select CE] をクリックします。
[Select CPE Device - CE] ウィンドウが表示されます。
 - ステップ 5** [CPE] デバイス (mlce4) を選択し、[Select] をクリックします。
[MPLS Service Request Editor - CE Interface] ウィンドウが表示されます。
 - ステップ 6** インターフェイス選択機能から [CE Interface] を選択します。
 - ステップ 7** [Select MVRFCE] をクリックします。
[Select CPE Device - MVRFCE] ウィンドウが表示されます。
 - ステップ 8** [MVRFCE] を選択し、[Select] をクリックします。
[MPLS Service Request Editor - MVRFCE CE Facing Interface] ウィンドウが表示されます。
 - ステップ 9** インターフェイス選択機能から [MVRFCE CE Facing Interface] を選択します。
[MPLS Service Request Editor - Choose MVRFCE PE Facing Interface] ウィンドウが表示されます。
 - ステップ 10** [Select PE] をクリックします。
[Select PE Device] ウィンドウが表示されます。
 - ステップ 11** PE を選択し、[Select] をクリックします。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。
 - ステップ 12** インターフェイス選択機能から [PE Interface] を選択します。
 - ステップ 13** [Link Attribute] セルの [Add] をクリックします。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。
 - ステップ 14** PE の VLAN ID を入力します (510)。
 - ステップ 15** [Next] をクリックします。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。
 - ステップ 16** MVRFCE の VLAN ID を入力します (530)。
 - ステップ 17** [Next] をクリックします。
[MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。
 - ステップ 18** デフォルトのまま、[Next] をクリックします。
[MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。
 - ステップ 19** デフォルトのまま、[Next] をクリックします。
[MPLS Link Attribute Editor - Routing Information] ウィンドウが再表示されます。
 - ステップ 20** デフォルトのまま、[Next] をクリックします。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが表示されます。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義](#)」(P.5-91) を参照してください。

- ステップ 21** [Add] をクリックして VPN を選択します。
[Select VPN] ウィンドウが表示されます。
- ステップ 22** [VPN] を選択します。
- ステップ 23** [Join as Hub] または [Join as Spoke] をクリックして、CERC に参加します。
- ステップ 24** [Done] をクリックします。
[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが再表示されます。
- ステップ 25** テンプレートまたはデータ ファイルをサービス要求に関連付ける場合は、[Next] ボタンをクリックします。
[Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。テンプレートをサービス要求に関連付ける手順、およびこの機能のこのウィンドウでの使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#) を参照してください。デバイスのテンプレートおよびデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じます。
[Service Request Editor] ウィンドウが表示されます。
- ステップ 26** テンプレートを追加しなかった場合は、[MPLS Link Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 27** サービス要求の説明を入力して、[Save] をクリックします。
[MPLS Service Requests] ウィンドウが表示され、サービス要求が [Requested] 状態になり展開可能になっていることを示します。

PE-Only サービス要求の作成

PE-Only サービス要求を作成するには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] > [Create] を選択します。
- ステップ 2** CE の存在しないポリシーを選択し、[OK] をクリックします。
[MPLS Service Request Editor] が表示されます。
- ステップ 3** [Add Link] をクリックします。
これで、[MPLS Service Request Editor] に一連のフィールドが表示されるようになりました。[Select PE] フィールドがイネーブルであることを確認します。このサービスのリンクの定義に必要な最初のタスクは、リンクの PE を指定することです。ただし、CLE スイッチ リンクが必要な場合を除きます。CLE スイッチが必要な場合は、「[サービス要求への CLE の追加](#)」(P.5-103) に進みます。
- ステップ 4** [PE] : [Select PE] をクリックします。

[Select PE Device] ダイアログボックスが表示されます。

- a. [Show PEs with] ドロップダウン リストから [Provider Name]、[Region]、または [Device Name] で PE を表示できます。
- b. [Find] ボタンを使用して、特定の PE の検索または表示の更新のいずれかを実行できます。
- c. [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。
- d. このダイアログボックスには、現在定義されている PE デバイスのリストの最初のページが表示されます。情報のページ数は、ダイアログボックスの右下隅に表示されます。

PE デバイスの別のページに移動するには、移動先のページ番号をクリックします。

ステップ 5 [Select] 列で、MPLS リンクの PE の名前を選択して、[Select] をクリックします。

[Service Request Editor] ウィンドウに戻ります。選択した PE の名前が [PE] 列に表示されています。

ステップ 6 [PE Interface] : インターフェイス選択機能を使用して、PE インターフェイスを選択します。

[Link Attribute] の [Add] オプションがイネーブルになっていることを確認します。

ステップ 7 [Link Attribute] 列で [Add] をクリックします。

[MPLS Link Attribute Editor] が表示され、インターフェイス パラメータのフィールドが示されます。

このウィンドウに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE インターフェイス フィールドの詳細については、「[PE および CE インターフェイス パラメータの指定](#)」(P.5-45) を参照してください。



(注) [VLAN ID] および [Second VLAN ID] 属性の設定の詳細については、「[\[VLAN ID\] および \[Second VLAN ID\] 属性に関する注意事項](#)」(P.5-88) を参照してください。

ステップ 8 この特定のリンクに対して変更する必要があるインターフェイス値があれば編集し、[Next] をクリックします。

[MPLS Link Attribute Editor] で [IP Address Scheme] が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。[IP Address Scheme] フィールドの詳細については、「[IP アドレス スキームの指定](#)」(P.5-48) を参照してください。

ステップ 9 この特定のリンクで変更する必要があるすべての IP アドレス スキーム値を編集し、[Next] をクリックします。

このウィンドウに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE のルーティング情報の詳細については、「[サービスのルーティング プロトコルの指定](#)」(P.5-51) を参照してください。

このサービスに使用されているサービス ポリシーによってルーティング プロトコルが編集可能と指定されているため、必要に応じてこのサービス要求のルーティング プロトコルを変更できます。

ステップ 10 [Site of Origin] をオンにした場合は、次の値選択に必要なステップが含まれるように画面が更新されません。

- a. [Select] をクリックします。

[Site for SOO Value] ウィンドウが表示されます。

- b. 使用可能な表示されたリストからサイトおよび SoO 値に関連するチェックボックスをオンにし、[Select] をクリックします。

使用方法に関する注釈 :

- [Site of Origin] 属性は、IOS デバイス専用です。この属性は、ポリシー レベルでは表示されません。サービス要求ワークフローの [MPLS Link Attribute Editor] ウィンドウのみに表示されます。また、PE-only サービス要求（つまり、CE が存在しない PE）の場合に限り表示されます。
- Prime Provisioning グラフィカル ユーザー インターフェイス (GUI) は、以前は IOS デバイスの Site of Origin の eBGP のサイトをサポートしていました。このリリースでは、さらに IOS XR PE デバイスの IPv4 EBGP ネイバーに対する EBGP Site of Origin がサポートされています。
- 2 つの使用例について次に説明します。
 1. カスタマーの [Site of Origin] がイネーブルで、同じカスタマーがサービス要求で使用された VPN の作成に使用された場合、[Site of Origin] オプションは [MPLS Link Attribute Editor] ウィンドウに表示されます（ルーティング プロトコルに BGP が選択されているとき）。CE が存在しない PE のサービス要求の場合、[Site of Origin] がイネーブルのときは [Route Map/Policy In] フィールドはディセーブルになりクリアされます。
 2. カスタマーの [Site of Origin] がイネーブルであり、CE デバイスが同じカスタマーを使用し、同じカスタマーが CE のある PE のサービス要求で使用された場合、[Site of Origin] フィールドはサービス要求レベルで表示されません。デフォルトでは、[Site of Origin] の値を考慮してデバイスに Site of Origin 設定を展開します。前の事例のように、[Route Map/Policy In] フィールドはディセーブルになりクリアされます。

ステップ 11 この特定リンクに対して変更する必要があるルーティング プロトコル値があれば編集してします。



(注)

このインターフェイスがデュアル スタック (IPv4 と IPv6) である場合、IPv4 と IPv6 両方のルーティング情報を個別に入力するようにプロンプトが表示されます。IPv6 ルーティング プロトコル情報を指定するときは、[MPLS Link Attribute Editor] の [Routing Information] で、一連のオプションが若干異なって表示される場合があります。IPv6 アドレスの入力でサポートされるフォーマットの詳細については、「MPLS VPN ポリシー」(P.5-37) を参照してください。

ステップ 12 [Next] をクリックします。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。VRF および VPN の情報の詳細については、「VRF および VPN の情報の定義」(P.5-76) を参照してください。



(注)

以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「独立 VRF 管理」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注)

MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

ステップ 13 この特定リンクに対して変更する必要がある VRF および VPN の値があれば編集します。

ステップ 14 テンプレートまたはデータ ファイルをサービス要求に関連付ける場合は、[Next] ボタンをクリックします。

[Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。

テンプレートをサービス要求に関連付ける手順、およびこの機能のこのウィンドウでの使用方法については、第 9 章「[テンプレートおよびデータ ファイルの管理](#)」を参照してください。デバイスのテンプレートおよびデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックします。

[Service Request Editor] ウィンドウが表示されます。前のステップ内に概要を示したステップに従って、このサービス要求に複数のリンクを定義できます。

ステップ 15 テンプレートを追加しなかった場合は、[MPLS Link Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。

[Service Request Editor] ウィンドウが表示されます。

ステップ 16 サービス要求のこの最初のリンクの作業を保存するには、[Save] をクリックします。

[Service Requests] ダイアログボックスに戻ります。ここで、定義したばかりのリンクの情報が表示されるようになります。

[Add Link] を選択し、サービスの次のリンクの属性を指定することにより、このサービス要求にさらにリンクを追加できます。ご覧のように、サービス要求は [Requested] 状態にあります。このサービスにすべてのリンクが定義されている場合、「[IOS から IOS XR への PE デバイスの移行](#)」(P.5-103) で説明されているように、サービスを展開する必要があります。

サービス要求への CLE の追加

「[PE-Only サービス要求の作成](#)」(P.5-100) で説明したサービス要求に CLE デバイスを追加するには、次の手順を実行します。

ステップ 1 「[PE-Only サービス要求の作成](#)」(P.5-100) のステップ 1 ~ 5 を実行します。

ステップ 2 [Select CLE] をクリックします。[Select PE Device] ダイアログボックスが表示されます。

- a. [Show PEs with] ドロップダウン リストから [Provider Name]、[Region]、または [Device Name] で PE を表示できます。
- b. [Find] ボタンを使用して、特定の PE の検索または表示の更新のいずれかを実行できます。
- c. [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。
- d. このダイアログボックスには、現在定義されている PE デバイスのリストの最初のページが表示されます。情報のページ数は、ダイアログボックスの右下隅に表示されます。

PE デバイスの別のページに移動するには、移動先のページ番号をクリックします。

ステップ 3 [Select] 列で、MPLS リンクの CLE の名前を選択して、[Select] をクリックします。

[Service Request Editor] ウィンドウに戻ります。ここで、選択した CLE の名前が [CLE] 列に表示されるようになります。

ステップ 4 [CLE Interface]：インターフェイス選択機能を使用して、CLE インターフェイスを選択します。

ステップ 5 「[PE-Only サービス要求の作成](#)」(P.5-100) のステップ 4 ~ ステップ 16 を続けて実行します。

IOS から IOS XR への PE デバイスの移行

IOS デバイスで展開したサービスを IOS XR デバイスに移行する際にサポートを受けるには、シスコ アドバンスド サービスにお問い合わせください。

標準 PE-CE リンクのプロビジョニング

この項では、Prime Provisioning のプロビジョニング プロセスで MPLS VPN PE-CE リンクを設定する方法を説明します。

MPLS VPN PE-CE リンクの概要

Prime Provisioning で MPLS VPN サービスをプロビジョニングするには、まず MPLS VPN サービス ポリシーを作成する必要があります。Prime Provisioning では、サービス ポリシーとはサービス要求の作成および展開における一連のデフォルト設定のことです。

Prime Provisioning は、標準 PE-CE と MVRFCPE PE-CE という、2 つの MPLS VPN サービス ポリシー タイプをサポートします。次のシナリオでは、標準 PE-CE ポリシー タイプに焦点を当てます。

標準 PE-CE ポリシー タイプは、2 つのデバイス間の通常の PE から CE へのリンクです。このポリシー タイプには 2 つのオプションがあります。

- [CE Present] イネーブル (1 つの PE と 1 つの CE、2 つのデバイス)
- [CE Present] ディセーブル (PE のみ、CE なし、1 つのデバイス)

図 5-9 に、2 つのデバイス間の通常の PE から CE へのリンクの例を示します。

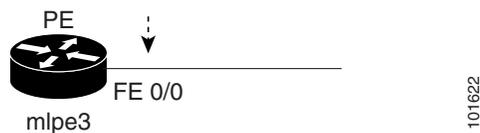
図 5-9 CE が存在する PE から CE へのリンク



[CE Present] がイネーブルである PE から CE へのリンクでは、インターフェイス S3/1 および S1/0 がサービス要求プロセス内で MPLS VPN リンクとして設定されます。

図 5-10 に、CE が存在しない PE のみのリンクの例を示します。

図 5-10 CE が存在しない PE から CE へのリンク



[CE Present] がディセーブルである PE から CE へのリンクでは、インターフェイス FE0/0 がサービス要求プロセス内で MPLS VPN リンクとして設定されます。

ネットワーク トポロジ

図 5-11 に、MPLS VPN PE-CE リンクが作成されるネットワーク トポロジの概要を示します。

図 5-11 MPLS VPN PE-CE シナリオのネットワーク トポロジ

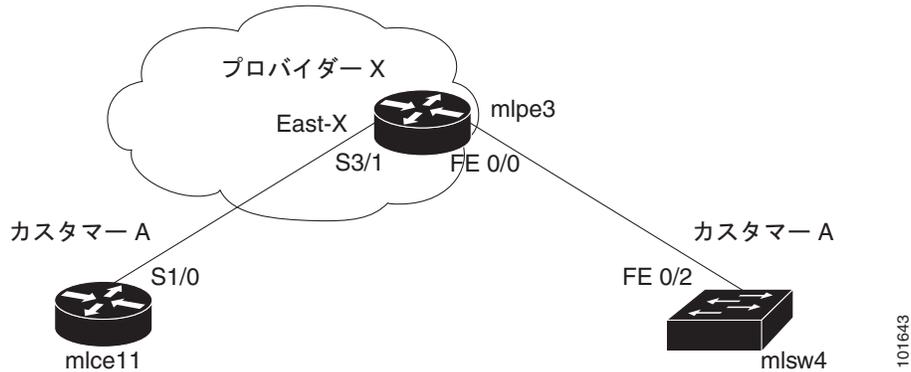


図 5-11 のネットワーク トポロジは、1 つのサービス プロバイダー (プロバイダー X) と 1 つのカスタマー (カスタマー A) のラボ環境を示しています。1 つのリージョン (East-X) と 1 つの PE (mlpe3.cisco.com) があります。各カスタマー デバイス (1 個の CE と 1 個の CLE) は、サイト (mlce11-Site および mlce4-Site) を表しています。

前提タスク

Prime Provisioning にサービス ポリシーを作成する前に、次のサービス インベントリ タスクを実行する必要があります。

-
- ステップ 1** サイトを持つカスタマーをセットアップします (「CPE デバイスの管理」(P.2-37) を参照)。
 - ステップ 2** リージョンを持つプロバイダーをセットアップします (「プロバイダー」(P.2-15) を参照)。
 - ステップ 3** デバイスのインポート、作成、検出のいずれかを行います (「デバイス」(P.2-1) を参照)。
 - ステップ 4** CPE および PE を作成します (「プロバイダー」(P.2-15) を参照)。
 - ステップ 5** 設定を収集します (「タスク」(P.10-25) を参照)。
 - ステップ 6** リソース プールを作成します (「リソース プール」(P.2-46) を参照)。
 - ステップ 7** ルート ターゲットを作成します (「ルート ターゲット」(P.2-53) を参照)。
 - ステップ 8** MPLS VPN を定義します (「MPLS VPN の作成」(P.5-7) を参照)。
-

PE-CE リンクに対する VPN の定義

サービス展開時に、Prime Provisioning は、論理 VPN 関係を設定するための Cisco IOS コマンドを生成します。プロビジョニング プロセスの開始時、サービス ポリシーの作成よりも前に、VPN を Prime Provisioning 内に定義する必要があります。

VPN を定義するには、次の手順を実行します。

-
- ステップ 1** [Inventory] > [Logical Inventory] > [VPNs] を選択します。
[VPNs] ウィンドウが表示されます。
 - ステップ 2** [Create] をクリックして VPN を 1 個作成します。
[Create New VPN] ウィンドウが表示されます。

- ステップ 3** [Name] フィールドに VPN 名を入力します。
次の特殊文字は使用しないことをお勧めします (` " < > () [] { } \ / & ^ ! ? ~ * % = , . +))。これらを VPN 名に使用すると、VRF 名を自動生成するために VPN 名が使用される場合に、特定のデバイスの VRF 名の設定ミスが生じる可能性があります。
- ステップ 4** [Customer] フィールドで、[Select] をクリックします。
[Select Customer] ウィンドウが表示されます。
- ステップ 5** 該当するカスタマーにチェックを入れ、[Select] をクリックします。
[VPNs] ウィンドウは、新しい [VPN Name] がこの新しい VPN 定義の [Customer] と関連付けられている場合に再表示されます。
- ステップ 6** [Save] をクリックします。



(注) 以前に定義された独立 VRF オブジェクトを介して VRF および VPN の属性を設定することもできます。この機能の詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義](#)」(P.5-91) を参照してください。

MPLS VPN PE-CE サービス ポリシーの作成

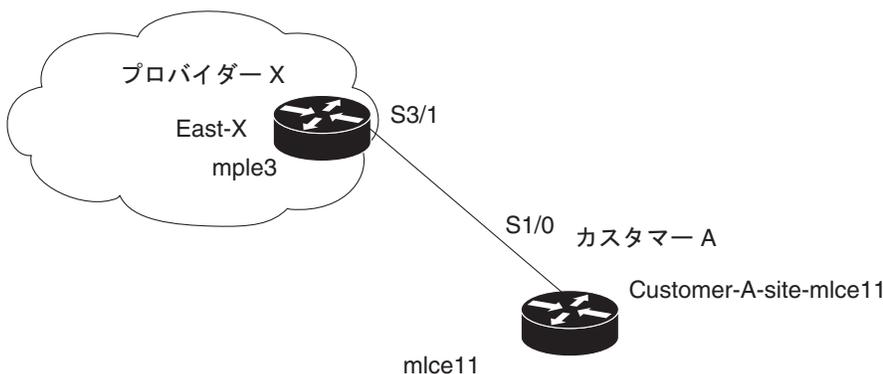
ここでは、次の項目について説明します。

- 「[PE-CE サービス ポリシーの概要](#)」(P.5-106)
- 「[MVRFCPE PE-CE サービス ポリシーの作成](#)」(P.5-118)
- 「[PE-NoCE サービス ポリシーの作成](#)」(P.5-119)

PE-CE サービス ポリシーの概要

図 5-12 に、PE-CE サービス ポリシーのシナリオで定義される PE-CE リンクの例を示します。

図 5-12 PE-CE トポロジ



101644

PE-CE サービス ポリシーの作成

PE-CE サービス ポリシーを作成するには、次の手順を実行します。

- ステップ 1** [Service Design] > [Policies] > [Policy Manager] > [Create] を選択します。
[Policy Editor] ウィンドウが表示されます。
- ステップ 2** ポリシー タイプとして [MPLS] を選択します。
[Policy Editor] ウィンドウが表示されます。
- ステップ 3** 次の属性を編集します。
- [Policy Name] : ポリシー名を入力します。
 - [Policy Owner] : ポリシー所有者を選択します。
 - [Customer] :
 - [Select] をクリックしてカスタマーを指定します。
[Customer for MPLS Policy] ウィンドウが表示されます。
 - 該当するカスタマーにチェックを入れ、[Select] をクリックします。
 - [Policy Type] : ポリシー タイプを選択します ([Regular PE-CE])。
- ステップ 4** [CE Present] : チェックして CE の存在を指定します。
- ステップ 5** [Next] をクリックします。
[MPLS Policy Editor - Interface] ウィンドウが表示されます。
- ステップ 6** [Next] をクリックしてデフォルトを受け入れます。
[MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。



(注) [Editable] チェックボックスがオンになっていることを確認します。これにより、サービス要求プロセスでこれらの属性を編集できるようになります。

- ステップ 7** 該当するすべての属性を編集します。



(注) [Automatically Assign IP Address] をオンにすると、画面が更新され、4 番目の属性 [IP Address Pool] が追加されます。

- ステップ 8** [Next] をクリックします。
[MPLS Policy Editor - Routing Information] ウィンドウが表示されます。

- ステップ 9** [Next] をクリックしてデフォルトを受け入れます。
[MPLS Policy Editor - VRF and VPN Membership] ウィンドウが表示されます。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「[独立 VRF 管理 \(P.5-15\)](#)」を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。

ステップ 10 ポリシーのテンプレートの関連付けをイネーブルにするには、[MPLS Policy Editor - VRF and VPN Membership] ウィンドウで [Next] ボタンをクリックします。



(注) 追加のウィンドウが [Template Association] ウィンドウの前にポリシー ワークフローに表示されます。このウィンドウを使用して、ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザー定義の属性を作成することもできます。追加情報機能の使用方法に関する背景情報については、[付録 F 「サービスに情報を追加する方法」](#) を参照してください。この機能を使用しない場合は、[Next] をクリックして [Template Association] ウィンドウに進むか、[Finish] をクリックしてポリシーを保存します。

[Template Association] ウィンドウが表示されます。このウィンドウで、テンプレート サポートをイネーブルにして、任意でテンプレートとデータ ファイルをポリシーに関連付けることができます。テンプレートをポリシーに関連付ける方法、およびこのウィンドウにおける機能の使用方法については、[第 9 章 「テンプレートおよびデータ ファイルの管理」](#) を参照してください。付録の手順に従ってポリシーのテンプレートとデータ ファイルの設定を完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じます。

[Policies] ウィンドウが表示されます。

ステップ 11 テンプレートをイネーブルにしなかった場合は、[MPLS Policy Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。

[Policies] ウィンドウが再表示されます。

MPLS VPN PE-CE サービス ポリシーが完成します。

PE-NoCE サービス ポリシーの作成

PE-NoCE サービス ポリシーを作成するには、次の手順を実行します。

ステップ 1 [Service Design] > [Policies] > [Policy Manager] > [Create] を選択します。
[Policy Editor] ウィンドウが表示されます。

ステップ 2 ポリシー タイプとして [MPLS] を選択します。
[Policy Editor] ウィンドウが表示されます。

ステップ 3 次の属性を編集します。

- [Policy Name] : ポリシー名を入力します。
- [Policy Owner] : ポリシー所有者を選択します。
- [Customer] :
 - [Select] をクリックしてカスタマーを指定します。
[Customer for MPLS Policy] ウィンドウが表示されます。
 - カスタマーを選択し、[Select] をクリックします。
- [Policy Type] : ポリシー タイプを選択します ([Regular PE-CE])。

- [CE Present] : チェック **しない** で CE が存在しないことを指定します (**NoCE**)。

ステップ 4 [Next] をクリックします。

[MPLS Policy Editor - Interface] ウィンドウが表示されます。

ステップ 5 [Next] をクリックしてデフォルトを受け入れます。

[MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。



(注) [Editable] チェックボックスがオンになっていることを確認します。これにより、サービス要求プロセスでこれらの属性を編集できるようになります。

このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービスポリシーで指定された値が反映されます。

[IP Address Scheme] フィールドの詳細については、「[IP アドレススキームの指定](#)」(P.5-48) を参照してください。

ステップ 6 該当するすべての属性を編集します。



(注) [Automatically Assign IP Address] をオンにすると、画面が更新され、4 番目の属性 [IP Address Pool] が追加されます。

ステップ 7 [Next] をクリックします。

[MPLS Policy Editor - Routing Information] ウィンドウが表示されます。

ステップ 8 [Next] をクリックしてデフォルトを受け入れます。

[MPLS Policy Editor - VRF and VPN Membership] ウィンドウが表示されます。



(注) プロトコルタイプについては、「[サービスのルーティングプロトコルの指定](#)」(P.5-51) を参照してください。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。この項では、MPLS VPN サービスポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。

ステップ 9 ポリシーのテンプレートの関連付けをイネーブルにするには、[MPLS Policy Editor - VRF and VPN Membership] ウィンドウで [Next] ボタンをクリックします。



(注) 追加のウィンドウが [Template Association] ウィンドウの前にポリシーワークフローに表示されます。このウィンドウを使用して、ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザ定義の属性を作成することもできます。追加情報機能の使用方法に関する背景情報については、[付録 F 「サービスに情報を追加する方法」](#) を参照してください。この機能を使用しない場合は、[Next] をクリックして [Template Association] ウィンドウに進むか、[Finish] をクリックしてポリシーを保存します。

[Template Association] ウィンドウが表示されます。このウィンドウで、テンプレート サポートをイネーブルにして、任意でテンプレートとデータ ファイルをポリシーに関連付けることができます。テンプレートをポリシーに関連付ける方法、およびこのウィンドウにおける機能の使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。付録の手順に従ってポリシーのテンプレートとデータ ファイルの設定を完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じます。

[Policies] ウィンドウが表示されます。

- ステップ 10** テンプレートをイネーブルにしなかった場合は、[MPLS Policy Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。

[Policies] ウィンドウが再表示されます。

MPLS VPN PE-NoCE サービス ポリシーが完成しました。

MPLS VPN PE-CE サービス要求の作成

ここでは、次の項目について説明します。

- 「[MVRFCE PE-CE サービス要求の作成](#)」(P.5-121)
- 「[MVRFCE PE-NoCE サービス要求の作成](#)」(P.5-123)

PE-CE サービス要求の作成

PE-CE サービス要求を作成するには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] > [Create] を選択します。
[Service Request Editor] ウィンドウが表示されます。
- ステップ 2** MPLS PE-CE タイプのポリシーを選択します。
- ステップ 3** [OK] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 4** [Add Link] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 5** [Select CE] をクリックします。
[CPE for MPLS VPN Link] ウィンドウが表示されます。
- ステップ 6** CPE デバイスを選択し、[Select] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 7** インターフェイス選択機能から [CE Interface] を選択します。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 8** [Select PE] をクリックします。
[PE for MPLS VPN Link] ウィンドウが表示されます。
- ステップ 9** PE デバイスを選択し、[Select] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 10** インターフェイス選択機能から [PE Interface] を選択します。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 11 [Select PE] をクリックします。

[PE for MPLS VPN Link] ウィンドウが再表示されます。

ステップ 12 [Link Attribute] セルで、[Add] をクリックします。

[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

PE Information

ステップ 13 [Interface Name] : インターフェイスを識別する値を入力します。

ステップ 14 [Interface Description] : オプションで、PE インターフェイスの説明を入力できます。

ステップ 15 [Shutdown Interface] : このチェックボックスをオンにすると、PE インターフェイスはシャットダウン状態で設定されます。

ステップ 16 [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します

ドロップダウン リストで使用可能な選択肢は、インターフェイス タイプで決定されます。

ステップ 17 [VLAN ID] : VLAN ID を入力します。VLAN ID は PE および CE で共有されるため、両方で 1 個の VLAN ID です。

ステップ 18 [Auto-Pick VLAN ID] : Prime Provisioning に VLAN プールから VLAN ID を自動選択させる場合は、このチェックボックスをオンにします。

このボックスがオンの場合、[VLAN ID] フィールドは GUI に表示されません。

ステップ 19 [Second VLAN ID] : Second VLAN ID は、PE インターフェイスでの着信フレームの Q-in-Q の 2 番目の VLAN タグを照合する方式を提供するオプションの属性です。

この属性の使用方法の詳細については、「[\[VLAN ID\] および \[Second VLAN ID\] 属性に関する注意事項](#)」(P.5-88) を参照してください。

ステップ 20 [Use SVI] : Prime Provisioning が SVI で VRF を終了するようにするには、このチェックボックスをオンにします。

CE Information

ステップ 21 [Interface Name] : インターフェイスを識別する値を入力します。

ステップ 22 [Interface Description] : オプションで、PE インターフェイスの説明を入力できます。

ステップ 23 [Encapsulation] : ドロップダウン リストから CE カプセル化を選択します。

ドロップダウン リストで使用可能な選択肢は、インターフェイス タイプで決定されます。

ステップ 24 [Next] をクリックします。

[MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。

ステップ 25 デフォルトを受け入れて、[Next] をクリックします。

[MPLS Link Attribute Editor - Routing Information] ウィンドウが表示されます。



(注) プロトコル タイプについては、「[サービスのルーティング プロトコルの指定](#)」(P.5-51) を参照してください。

ステップ 26 [Next Hop Option:] を次から選択します。

- USE_OUT_GOING_INTF_NAME
- USE_NEXT_HOP_IPADDR

- OUTGOING_INTF_NAME+NEXT_HOP_IPADDR



(注) このインターフェイスがデュアルスタック (IPv4 と IPv6) である場合、IPv4 と IPv6 両方のルーティング情報を個別に入力するようにプロンプトが表示されます。[IPv6 Routing Information] ウィンドウのフィールドは、IPv4 のバージョンとは少し異なっています。IPv6 のルーティング情報のセットアップについては、「[スタティック ルーティング プロトコル属性の設定 \(IPv4 と IPv6\)](#)」(P.5-96) を参照してください。

ステップ 27 続行するには、[Next] をクリックします。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが表示されます。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「[独立 VRF 管理](#)」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義](#)」(P.5-91) を参照してください。

ステップ 28 [Add] をクリックして VPN に参加します。

[Select CERCs] ウィンドウが表示されます。

ステップ 29 ドロップダウン リストからカスタマーを選択します。

ステップ 30 ドロップダウン リストから VPN を選択します。

ステップ 31 リストから該当する VPN を選択します。

ステップ 32 [Join As Hub] または [Join As Spoke] をクリックします。

ステップ 33 [Done] をクリックします。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが再表示されます。

ステップ 34 テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。

[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。



(注) 上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、次のステップ 37 に進みます。

ステップ 35 デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。

前のステップで示されている説明に従って、このサービス要求に複数のリンクを定義できます。

ステップ 36 作業内容を保存するには、[Save] をクリックします。

[MPLS Service Requests] ウィンドウが再度表示され、MPLS VPN PE-CE サービス要求が [Requested] 状態になっていて展開準備ができていることが示されます。

PE-NoCE サービス要求の作成

PE-NoCE サービス要求を作成するには、次の手順を実行します。

ステップ 1 [Operate] > [Service Requests] > [Service Request Manager] > [Create] を選択します。

ステップ 2 MPLS PE-NoCE タイプのポリシーを選択します。

ステップ 3 [OK] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 4 [Add Link] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 5 [Select PE] をクリックします。

[PE for MPLS VPN Link] ウィンドウが表示されます。

ステップ 6 PE デバイスを選択し、[Select] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 7 インターフェイス選択機能から [PE Interface] を選択します。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 8 [Link Attribute] セルで、[Add] をクリックします。

[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

ステップ 9 [Interface Name] : インターフェイスを識別する値を入力します。

ステップ 10 [Interface Description] : オプションで、PE インターフェイスの説明を入力できます。

ステップ 11 [Shutdown Interface] : このチェックボックスをオンにすると、PE インターフェイスはシャットダウン状態で設定されます。

ステップ 12 [PE Encapsulation] : ドロップダウン リストから PE カプセル化を選択します

ドロップダウン リストで使用可能な選択肢は、インターフェイス タイプで決定されます。このフィールドは、PE/UNI カプセル化を決定するために必要です。

ステップ 13 [VLAN ID] : VLAN ID を入力します。VLAN ID は PE および CE で共有されるため、両方で 1 個の VLAN ID です。

ステップ 14 [Auto-Pick VLAN ID] : Prime Provisioning に VLAN プールから VLAN ID を自動選択させる場合は、このチェックボックスをオンにします。

このボックスがオンの場合、[VLAN ID] フィールドは GUI に表示されません。

ステップ 15 [Second VLAN ID] : Second VLAN ID は、PE インターフェイスでの着信フレームの Q-in-Q の 2 番目の VLAN タグを照合する方式を提供するオプションの属性です。

この属性の使用方法の詳細については、「[VLAN ID] および [Second VLAN ID] 属性に関する注意事項」(P.5-88) を参照してください。

- ステップ 16** [Use SVI] : Prime Provisioning が SVI で VRF を終了するようにするには、このチェックボックスをオンにします。
- ステップ 17** [Standard UNI Port] : 追加の UNI セキュリティ パラメータにアクセスするには、このボックスをオンにします。
- ステップ 18** [Next] をクリックします。
[MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。
- ステップ 19** デフォルトを受け入れて、[Next] をクリックします。



(注) このインターフェイスがデュアル スタック (IPv4 と IPv6) である場合、IPv4 と IPv6 両方のルーティング情報を個別に入力するようにプロンプトが表示されます。

[MPLS Link Attribute Editor - Routing Information] ウィンドウが表示されます。

- ステップ 20** コンフィギュレーションでの必要に応じて、ルーティング情報の属性を設定します。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

- ステップ 21** [Next] をクリックします。
[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが表示されます。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「独立 VRF 管理」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

- ステップ 22** [Add] をクリックして VPN に参加します。
[Join VPN] ダイアログボックスが表示されます。
- ステップ 23** 該当する VPN にチェックを入れます。
- ステップ 24** [Join as Hub] または [Join as Spoke] をクリックします。
- ステップ 25** [Done] をクリックします。
[MPLS Service Request Editor] ウィンドウが再表示されます。
- ステップ 26** テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。
[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。



(注)

上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、次のステップ 30 に進みます。

ステップ 27 デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。

前のステップで示されている説明に従って、このサービス要求に複数のリンクを定義できます。

ステップ 28 作業内容を保存するには、[Save] をクリックします。

[MPLS Service Requests] ウィンドウが再度表示され、MPLS VPN PE-NoCE サービス要求が [Requested] 状態になっており、展開準備ができていたことが示されます。

マルチ VRFCE PE-CE リンクのプロビジョニング

この項では、Prime Provisioning のプロビジョニング プロセスで MPLS VPN Multi-VRFCE PE-CE リンクを設定する方法を説明します。

MPLS VPN MVRFCE PE-CE リンクの概要

ここでは、次の項目について説明します。

- 「ネットワーク トポロジ」(P.5-116)
- 「前提タスク」(P.5-116)

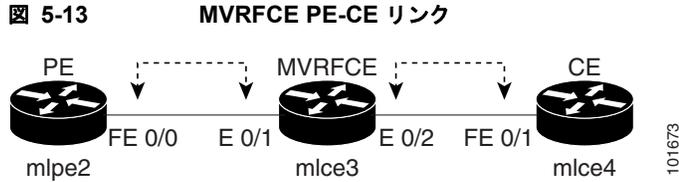
Prime Provisioning で MPLS VPN サービスをプロビジョニングするには、まず MPLS VPN サービス ポリシーを作成する必要があります。Prime Provisioning では、サービス ポリシーとはサービス要求の作成および展開における一連のデフォルト設定のことです。Prime Provisioning は、標準 PE-CE と MVRFCE PE-CE の 2 種類のタイプの MPLS VPN サービス ポリシーをサポートしています。次のシナリオは、MVRFCE PE-CE ポリシー タイプに焦点を当てたものです。MVRFCE PE-CE ポリシー タイプは、次の 3 個のデバイスを使用する PE と CE の間のリンクです。

- PE
- マルチ VRF CE
- CE

このポリシー タイプには 2 つのオプションがあります。

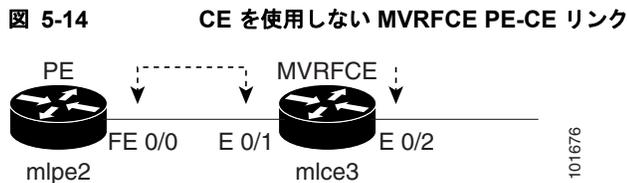
- CE Present *enabled* (1 個の PE に対して 1 個の MVRFCE と 1 個の CE を使用します。デバイスは 3 個です)
- CE Present *disabled* (1 個の PE に対して 1 個の MVRFCE を使用します。デバイスは 2 個です)

図 5-13 は、3 個のデバイスを使用した MVRFCE PE-CE リンクの例です。



CE Present をイネーブルにした MVRFCE PE-CE リンクの場合、インターフェイスの FE 0/0、E 0/1、E 0/2、FE 0/1 はサービス要求プロセスで MPLS VPN リンクとして構成されます。

図 5-14 は、CE を使用しない、PE と MVRFCE 間のリンクの例です。



CE Present をディセーブルにした MVRFCE PE-CE リンクの場合、インターフェイスの FE 0/0、E 0/1、E 0/2 はサービス要求プロセスで MPLS VPN リンクとして構成されます。

ネットワーク トポロジ

図 5-15 は、MPLS VPN MVRFCE PE-CE リンクが作成されるネットワーク トポロジの概要です。

図 5-15 MPLS VPN MVRFCE PE-CE シナリオのネットワーク トポロジ

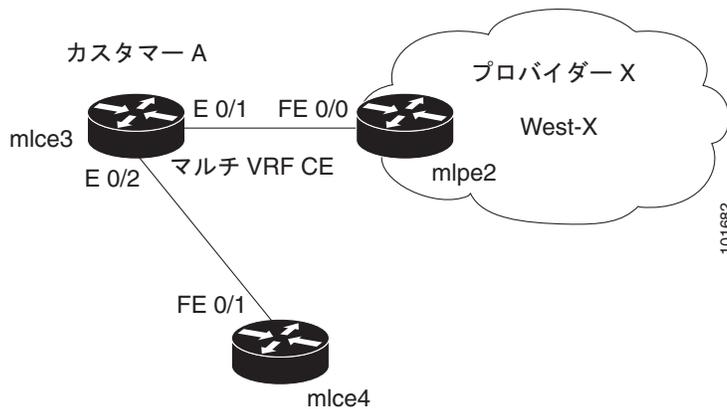


図 5-15 のネットワーク トポロジは、1つのサービス プロバイダー (プロバイダー X) と1つのカスタマー (カスタマー A) のラボ環境を示しています。1つのリージョン (West-X) と1つの PE (mlpe2.cisco.com) があります。各カスタマー デバイス (1個の MVRFCE と1個の CE) は、サイト (mlce3-Site および mlce4-Site) を表しています。

前提タスク

Prime Provisioning でサービス ポリシーを作成する前に、次のインベントリ管理タスクを完了しておく必要があります。

-
- ステップ 1** サイトを持つカスタマーをセットアップします（「CPE デバイスの管理」(P.2-37) を参照）。
 - ステップ 2** リージョンを持つプロバイダーをセットアップします（「プロバイダー」(P.2-15) を参照）。
 - ステップ 3** デバイスのインポート、作成、検出のいずれかを行います（第 2 章「デバイス」を参照）。
 - ステップ 4** CPE および PE を作成します（「プロバイダー」(P.2-15) を参照）。
 - ステップ 5** 設定を収集します（「タスク」(P.10-25) を参照）。
 - ステップ 6** リソース プールを作成します（「リソース プール」(P.2-46) を参照）。
 - ステップ 7** CE ルーティング コミュニティ (CERC) を作成します（「ルート ターゲット」(P.2-53) を参照）。
 - ステップ 8** MPLS VPN を定義します（「MPLS VPN の作成」(P.5-7) を参照）。
-

MVRFCE PE-CE リンクに対する VPN の定義

サービス展開時に、Prime Provisioning は、論理 VPN 関係を設定するための Cisco IOS コマンドを生成します。

プロビジョニング プロセスの開始時、サービス ポリシーの作成よりも前に、VPN を Prime Provisioning 内に定義する必要があります。VPN 定義の最初の要素は、VPN 名です。

VPN 名を作成するには、次の手順を実行します。

-
- ステップ 1** [Inventory] > [Logical Inventory] > [VPNs] を選択します。
[VPNs] ウィンドウが表示されます。
 - ステップ 2** [Create] をクリックして VPN を 1 個作成します。
[Create New VPN] ウィンドウが表示されます。
 - ステップ 3** 次の属性を編集します。
 - [Name] : VPN 名を入力します。
次の特殊文字は使用しないことをお勧めします (' ` " < > () [] { } \ / & ^ ! ? ~ * % = , . + |)。これらを VPN 名に使用すると、VRF 名を自動生成するために VPN 名が使用される場合に、特定のデバイスの VRF 名の設定ミスが生じる可能性があります。
 - [Customer] : [Select] をクリックします。
[Select Customer] ウィンドウが表示されます。
 - ステップ 4** カスタマーを選択し、[Select] をクリックします。
 - ステップ 5** [Save] をクリックします。
-



(注) 独立 VRF の関連付けは、MVRFCE ベースのサービス ポリシーとサービス要求ではサポートされていません。

MPLS VPN MVRFCE PE-CE サービス ポリシーの作成

ここでは、次の項目について説明します。

- 「MVRFCE PE-CE サービス ポリシーの作成」(P.5-118)
- 「PE-NoCE サービス ポリシーの作成」(P.5-119)

MVRFCE PE-CE サービス ポリシーの作成

MVRFCE PE-CE サービス ポリシーを作成するには、次の手順を実行します。



(注)

[Editable] チェックボックスが有効な箇所にチェックされているかを確認します。これにより、サービス要求プロセスでこれらの属性を編集できるようになります。

-
- ステップ 1** [Service Design] > [Policies] > [Policy Manager] を選択します。
[Policy Manager] ウィンドウが表示されます。
編集するポリシーを選択し、[Edit] ボタンをクリックします。
- ステップ 2** 次の属性を編集します。
- [Policy Name] : ポリシー名を入力します。
 - [Policy Owner] : ポリシー所有者を選択します。
 - [Customer] :
 - [Select] をクリックしてカスタマーを指定します。
[Customer for MPLS Policy] ウィンドウが表示されます。
 - カスタマーを選択し、[Select] をクリックします。
 - [Policy Type] : ポリシータイプを選択します (**MVRFCE : PE-CE**)
 - [CE Present] : チェックして CE の存在を指定します。
- ステップ 3** [Next] をクリックします。
[MPLS Policy Editor - PE Interface] ウィンドウが表示されます。
- ステップ 4** [Next] をクリックします。
[MPLS Policy Editor - Interface] ウィンドウが表示されます。
- ステップ 5** 該当するすべての属性を編集します。
- ステップ 6** [Next] をクリックします。
[PE-MVRFCE] に対して [MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。
- ステップ 7** 該当するすべての属性を編集します。
- ステップ 8** [Next] をクリックします。
- ステップ 9** [MVRFCE-CE] に対して、別セットの [MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。
- ステップ 10** 上記のように、該当するすべての属性を編集します。
- ステップ 11** [Next] をクリックします。
PE-MVRFCE に対応する [MPLS Policy Editor - Routing Information] ウィンドウが表示されます。



(注)

プロトコルタイプについては、「サービスのルーティングプロトコルの指定」(P.5-51) を参照してください。

- ステップ 12** [Next] をクリックしてデフォルトを受け入れます。
MVRFCCE-CE に対応する [MPLS Policy Editor - Routing Information] ウィンドウが表示されます。
- ステップ 13** [Next] をクリックしてデフォルトを受け入れます。
[MPLS Policy Editor - VRF and VPN Membership] ウィンドウが表示されます。
- ステップ 14** ポリシーのテンプレートの関連付けをイネーブルにするには、[MPLS Policy Editor - VRF and VPN Membership] ウィンドウで [Next] ボタンをクリックします。



(注) 追加のウィンドウが [Template Association] ウィンドウの前にポリシー ワークフローに表示されます。このウィンドウを使用して、ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザ定義の属性を作成することもできます。追加情報機能の使用方法に関する背景情報については、[付録 F 「サービスに情報を追加する方法」](#) を参照してください。この機能を使用しない場合は、[Next] をクリックして [Template Association] ウィンドウに進むか、[Finish] をクリックしてポリシーを保存します。

[Template Association] ウィンドウが表示されます。このウィンドウで、テンプレート サポートをイネーブルにして、任意でテンプレートとデータ ファイルをポリシーに関連付けることができます。テンプレートをポリシーに関連付ける方法、およびこのウィンドウにおける機能の使用方法については、[第 9 章 「テンプレートおよびデータ ファイルの管理」](#) を参照してください。付録の手順に従ってポリシーのテンプレートとデータ ファイルの設定を完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じます。

[Policies] ウィンドウが表示されます。

- ステップ 15** テンプレートをイネーブルにしなかった場合は、[MPLS Policy Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。
[Policies] ウィンドウが再表示されて、MPLS VPN MVRFCCE PE-CE サービス ポリシーの設定が完了していることがわかります。

PE-NoCE サービス ポリシーの作成

PE-NoCE サービス ポリシーを作成するには、次の手順を実行します。

- ステップ 1** [Service Design] > [Policies] > [Policy Manager] を選択します。
[Policy Manager] ウィンドウが表示されます。
- ステップ 2** 次の属性を編集します。
- [Policy Name] : ポリシー名を入力します。
 - [Policy Owner] : ポリシー所有者を選択します。
 - [Customer] :
 - [Select] をクリックしてカスタマーを指定します。
[Customer for MPLS Policy] ウィンドウが表示されます。
 - カスタマーを選択し、[Select] をクリックします。
 - [Policy Type] : ポリシー タイプを選択します ([Regular PE-CE])。
 - [CE Present] : チェック **しない** で CE が存在しないことを指定します (**NoCE**)。
- ステップ 3** [Next] をクリックします。

[MPLS Policy Editor - Interface] ウィンドウが表示されます。

ステップ 4 [Next] をクリックしてデフォルトを受け入れます。

MVRFCE-CE 接続情報を示す [MPLS Policy Editor - Interface] ウィンドウが表示されます。

ステップ 5 [Next] をクリックしてデフォルトを受け入れます。

PE-MVRFCE-CE インターフェイス Address/Maskを示す [MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。

a. 次のように属性を編集します。

b. [IP Numbering Scheme] : [IP Numbered] スキームを選択します。

c. [Automatically Assign IP Address] : Prime Provisioning に自動的に IP アドレスを割り当てさせるには、チェックボックスをチェックします。

d. [IP Address Pool] : IP アドレス プールを選択します。

ステップ 6 [Next] をクリックします。

MVRFCE-CE インターフェイス Address/Maskを示す [MPLS Policy Editor - IP Address Scheme] ウィンドウが表示されます。

a. 次のように属性を編集します。

b. [IP Numbering Scheme] : [IP Numbered] スキームを選択します。

c. [Automatically Assign IP Address] : Prime Provisioning に自動的に IP アドレスを割り当てさせるには、チェックボックスをチェックします。

d. [IP Address Pool] : IP アドレス プールを選択します。

ステップ 7 [Next] をクリックします。

PE-MVRFCE ルーティング情報を示す [MPLS Policy Editor - Routing Information] ウィンドウが表示されます。



(注) プロトコルタイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

ステップ 8 [Next] をクリックしてデフォルトを受け入れます。

MVRFCE-CE ルーティング情報を示す [MPLS Policy Editor - Routing Information] ウィンドウが表示されます。

ステップ 9 [Next] をクリックしてデフォルトを受け入れます。

[MPLS Policy Editor - VRF and VPN Membership] ウィンドウが表示されます。

ステップ 10 [Add] をクリックして VPN に参加します。[VPN] ダイアログボックスが表示されます。

ステップ 11 [Join as Hub] をクリックしてから、[Done] をクリックします。

[MPLS Policy Editor - VRF and VPN Membership] ウィンドウが表示されます。

ステップ 12 ポリシーのテンプレートの関連付けをイネーブルにするには、[MPLS Policy Editor - VRF and VPN Membership] ウィンドウで [Next] ボタンをクリックします。



(注) 追加のウィンドウが [Template Association] ウィンドウの前にポリシー ワークフローに表示されます。このウィンドウを使用して、ポリシー（およびそのポリシーに基づくサービス要求）に従って、ユーザー定義の属性を作成することもできます。追加情報機能の使用方法に関する背景情報については、付録 F

「サービスに情報を追加する方法」を参照してください。この機能を使用しない場合は、[Next] をクリックして [Template Association] ウィンドウに進むか、[Finish] をクリックしてポリシーを保存します。

[Template Association] ウィンドウが表示されます。このウィンドウで、テンプレート サポートをイネーブルにして、任意でテンプレートとデータ ファイルをポリシーに関連付けることができます。テンプレートをポリシーに関連付ける方法、およびこのウィンドウにおける機能の使用方法については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。付録の手順に従ってポリシーのテンプレートとデータ ファイルの設定を完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じます。

[Policies] ウィンドウが表示されます。

ステップ 13 テンプレートをイネーブルにしなかった場合は、[MPLS Policy Editor – VRF and VPN] ウィンドウで [Finish] をクリックします。

[Policies] ウィンドウが再表示されて、MPLS VPN MVRFCE PE-NoCE サービス ポリシーの設定が完了していることがわかります。

MPLS VPN MVRFCE PE-CE サービス要求の作成

ここでは、次の項目について説明します。

- 「MVRFCE PE-CE サービス要求の作成」(P.5-121)
- 「MVRFCE PE-NoCE サービス要求の作成」(P.5-123)

MVRFCE PE-CE サービス要求の作成

MVRFCE PE-CE サービス要求を作成するには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
- ステップ 2** MPLS ポリシーを選択します ([mpls-mvrfce-pe-ce])。
- ステップ 3** [OK] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 4** [Add Link] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 5** [Select CE] をクリックします。
[CPE for MPLS VPN Link] ウィンドウが表示されます。
- ステップ 6** CPE デバイスを選択して [Select] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 7** インターフェイス選択機能から [CE Interface] を選択します。
- ステップ 8** [Select MVRFCE] をクリックします。
[MVRFCE for MPLS VPN Link] ウィンドウが表示されます。
- ステップ 9** MVRFCE を選択して [Select] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 10 インターフェイス選択機能から [MVRFCE PE Facing Interface] を選択します。

ステップ 11 [Link Attribute] セルで [Add] をクリックします。

[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

PE Information

ステップ 12 [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。

ステップ 13 [VLAN ID] : PE VLAN ID を入力します。

MVRFCE PE Facing Information

ステップ 14 [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。

ステップ 15 [Next] をクリックします。

[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

MVRFCE CE Information

ステップ 16 [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。

ステップ 17 [VLAN ID] : PE VLAN ID を入力します。

MVRFCE PE-Facing Information

ステップ 18 [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。

ステップ 19 [Next] をクリックします。

PE-MVRF-CE インターフェイス Address/Mask を示す [MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。

ステップ 20 デフォルトを受け入れて、[Next] をクリックします。

MVRFCE-CE インターフェイス Address/Mask を示す [MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。

ステップ 21 デフォルトを受け入れて、[Next] をクリックします。

PE-MVRF-CE ルーティング情報を示す [MPLS Link Attribute Editor - Routing Information] ウィンドウが再表示されます。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

ステップ 22 デフォルトを受け入れて、[Next] をクリックします。

MVRFCE-CE ルーティング情報を示す [MPLS Link Attribute Editor - Routing Information] ウィンドウが再表示されます。

ステップ 23 デフォルトを受け入れて、[Next] をクリックします。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが表示されます。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

ステップ 24 [Add] をクリックして VPN に参加します。

[Select CERCs] ウィンドウが表示されます。

ステップ 25 ドロップダウン リストからカスタマーを選択します。

ステップ 26 ドロップダウン リストから VPN を選択します。

ステップ 27 リストから該当する VPN を選択します。

ステップ 28 [Join As Hub] または [Join As Spoke] をクリックします。

ステップ 29 [Done] をクリックします。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが再表示されます。

ステップ 30 テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。

[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。



(注)

上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、この後のステップ 34 に進みます。

ステップ 31 デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。

[MPLS Service Request Editor] ウィンドウが再表示されます。

ステップ 32 サービス要求の説明 (`mpls-mvrfce-pe-ce`) を入力して、[Save] をクリックします。

[MPLS Service Requests] ウィンドウが再表示されて、MPLS VPN MVRFCE PE-CE サービス要求が [Requested] 状態にあり、すぐに展開できることがわかります。

MVRFCE PE-NoCE サービス要求の作成

MVRFCE PE-NoCE サービス要求を作成するには、次の手順を実行します。

ステップ 1 [Operate] > [Service Requests] > [Service Request Manager] を選択します。

ステップ 2 MPLS ポリシーを選択します ([`mpls-mvrfce-pe-noce`])。

ステップ 3 [OK] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 4 [Add Link] をクリックします。

[MPLS Service Request Editor] ウィンドウが表示されます。

ステップ 5 [Select MVRFCE] をクリックします。

[CPE for MPLS VPN Link] ウィンドウが表示されます。

- ステップ 6** MVRFCE を選択し、[Select] をクリックします。
[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 7** インターフェイス選択機能から [MVRFCE CE Facing Interface] を選択します。
- ステップ 8** [Link Attribute] セルで [Add] をクリックします。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

PE Information

- ステップ 9** [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。
- ステップ 10** [VLAN ID] : PE VLAN ID を入力します。

MVRFCE PE Facing Information

- ステップ 11** [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。
- ステップ 12** [Next] をクリックします。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。

MVRFCE CE Information

- ステップ 13** [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。
- ステップ 14** [VLAN ID] : PE VLAN ID を入力します。

MVRFCE PE Facing Information

- ステップ 15** [Encapsulation] : ドロップダウン リストから PE カプセル化を選択します ([DOT1Q])。
- ステップ 16** [Next] をクリックします。

PE-MVRF-CE インターフェイス Address/Mask を示す [MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。

- ステップ 17** [Next] をクリックしてデフォルトを受け入れます。

MVRFCE-CE インターフェイス Address/Mask を示す [MPLS Link Attribute Editor - IP Address Scheme] ウィンドウが表示されます。

- ステップ 18** [Next] をクリックしてデフォルトを受け入れます。

PE-MVRF-CE ルーティング情報を示す [MPLS Link Attribute Editor - Routing Information] ウィンドウが再表示されます。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

- ステップ 19** [Next] をクリックしてデフォルトを受け入れます。

MVRFCE-CE ルーティング情報を示す [MPLS Link Attribute Editor - Routing Information] ウィンドウが再表示されます。

- ステップ 20** [Next] をクリックしてデフォルトを受け入れます。

[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが表示されます。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

- ステップ 21** [Add] をクリックして VPN に参加します。
[Select CERCs] ウィンドウが表示されます。
- ステップ 22** ドロップダウン リストからカスタマーを選択します。
- ステップ 23** ドロップダウン リストから VPN を選択します。
- ステップ 24** リストから該当する VPN を選択します。
- ステップ 25** [Join As Hub] または [Join As Spoke] をクリックします。
- ステップ 26** [Done] をクリックします。
[MPLS Link Attribute Editor - VRF and VPN] ウィンドウが再表示されます。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義 \(P.5-91\)](#)」を参照してください。

- ステップ 27** テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。
[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。



(注) 上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、この後のステップ 34 に進みます。

- ステップ 28** デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。
[MPLS Service Request Editor] ウィンドウが再表示されます。
- ステップ 29** サービス要求の説明を入力して、[Save] をクリックします (`mpls-mvrfce-pe-noce`)。
[MPLS Service Requests] ウィンドウが再表示されて、MPLS VPN MVRFCE PE-NoCE サービス要求が [Requested] 状態にあり、すぐに展開できることがわかります。

管理対象外 MVRFCE の作成

管理対象外 MVRFCE の機能は、サービス プロバイダーが Prime Provisioning を CPE へのコンフィギュレーションのアップロードおよびダウンロードに使用しない点において、管理対象外 CE の機能と似ています。また、この機能は、Prime Provisioning が PE、MVRFCE、CE の 3 個のデバイスでリンクを作成する点で、管理対象 MVRFCE の機能と似ています。

管理対象外シナリオでは、カスタマーが CPE を手動でコンフィギュレーションします。管理対象外 MVRFCE の設定プロセスを自動化するために、サービス プロバイダーは Prime Provisioning を使用して設定を生成してから、手動による実装用にそれをカスタマーに送信を実行できます。

図 5-16 は、MPLS VPN MVRFCE PE-CE リンクを使用したネットワーク トポロジの概要です。

図 5-16 管理対象外 MVRFCE PE-CE ネットワーク トポロジ

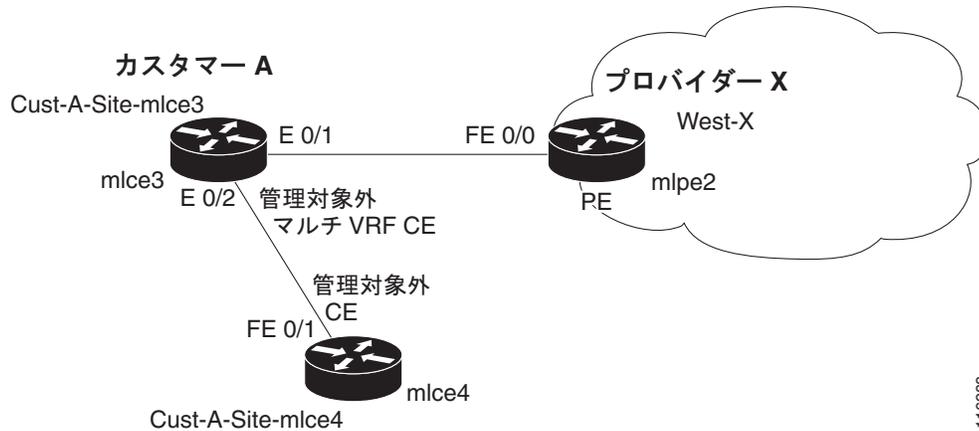


図 5-16 のネットワーク トポロジは、サービス プロバイダー (プロバイダー X) と 1 人のカスタマー (カスタマー A) を示しています。プロバイダーには、1 つのリージョン (West-X) と 1 個の PE (mlpe2) が含まれています。カスタマーには、1 個の MVRFCE (mlce3) と 1 個の CE (mlce4) が含まれています。これらの CPE は両方とも管理対象外です。

プロビジョニング管理 VPN

この項では、Prime Provisioning 管理サブネットの観点から、カスタマー エッジ ルータ (CE) を管理するための基本的な概念と考慮事項を説明します。Prime Provisioning を適切に展開してサービスをカスタマーに提供できるようにするには、CE がサービス プロバイダーによって管理されるかどうかについての質問に答える必要があります。

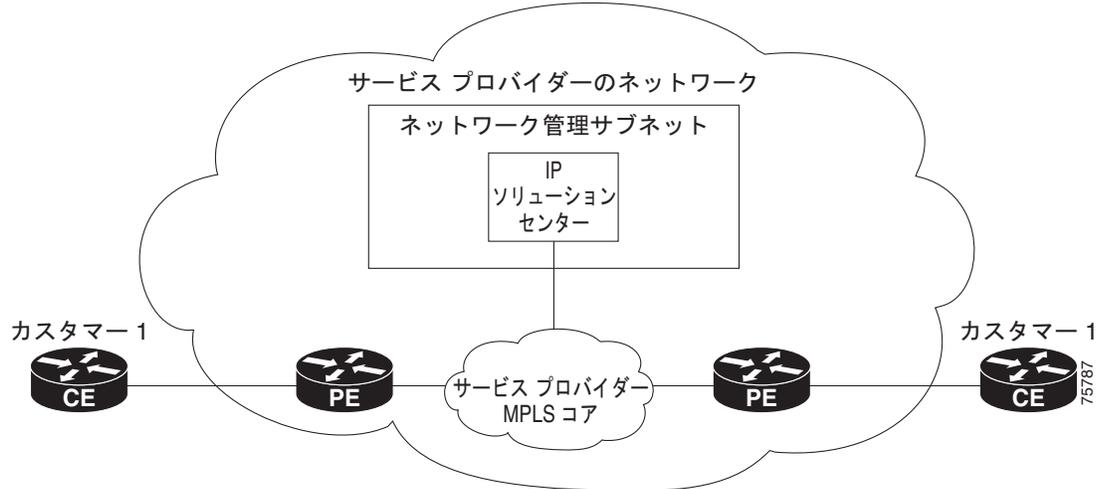
管理対象外のカスタマー エッジ ルータ

サービス プロバイダーは、サービス プロバイダー ネットワークに接続されたカスタマー エッジ ルータ (CE) を管理しないように選択することができます。サービス プロバイダーの場合、管理対象外 CE を採用する主な利点は管理の容易さです。

CE が管理対象外になると、プロバイダーはすべての管理トラフィックに IPv4 接続を使用できるようになります。Prime Provisioning は管理対象外 CE のプロビジョニングまたは管理には使用されません。

図 5-17 には、管理対象外 CE を含む基本的なトポロジが示されています。ネットワーク管理サブネットには、サービス プロバイダー MPLS コア ネットワークへの直接リンクがあります。

図 5-17 サービス プロバイダー ネットワークおよび管理対象外 CE



管理対象外 CE に関して、サービス プロバイダーは次の考慮事項に注意する必要があります。

- 管理対象外 CE はサービス プロバイダーの管理ドメインの外部にあるため、サービス プロバイダーは管理対象外 CE を保持または設定しません。
- サービス プロバイダーは、管理対象外 CE で次の要素を管理しません。
 - IP アドレス
 - ホスト名
 - ドメイン ネーム サーバ
 - 障害管理（およびネットワーク タイム プロトコルによるタイムスタンプの調整）
 - CE 設定の収集、アーカイブ、および復元
 - 管理対象外 CE のパスワードや SNMP 文字列などのアクセス データ
- プロトタイプ CE のコンフィグレットが生成されますが、ルータに自動的にダウンロードされません。
- 設定管理は行われません。
 - 設定管理が行われなため、設定履歴は維持されず、設定変更管理も行われません。
 - サービス要求への変更（PE-CE リンク上）は CE に展開されません。
- 現在の CE 設定を取得する手段がないため、監査の設定はありません。
- ルーティング監査を実行できます。
- Service Assurance Agent (SA エージェント) を使用してシャドウ ルータ間の応答時間を測定できますが、SA エージェントを使用して CE 間の応答時間を測定することはできません。

管理対象のカスタマー エッジ ルータ

管理対象外 CE の代替として、管理対象 CE、つまりサービス プロバイダーによって管理されているカスタマー エッジ ルータを使用します。管理対象 CE はサービス プロバイダーの管理範囲内ですべて処理することも、プロバイダーと顧客の間で共同管理することもできますが、CE を共同管理する場合、管理上、進行中の課題が多数発生するため、推奨されません。

管理対象 CE に関して、サービス プロバイダーは次の考慮事項に注意する必要があります。

- 管理対象 CE は、サービス プロバイダーの管理範囲に含まれます。したがって、サービス プロバイダー ネットワークから CE への接続が必要です。
- サービス プロバイダーは、管理対象 CE で次の要素を管理する必要があります。
 - IP アドレス
 - ホスト名
 - ドメイン ネーム サーバ
 - パスワードや SNMP 文字列などのアクセス データ
- サービス プロバイダーは障害管理（およびネットワーク タイム プロトコルによるタイムスタンプの調整）を行う必要があります。
- サービス プロバイダーは、CE 設定を収集、アーカイブ、および復元できます。
- CE コンフィグレットが生成され、管理対象の CE にダウンロードされます。
- サービス要求へ変更は、現在の CE 設定に基づいて行われ、自動的にダウンロードされます。
- CE 設定は監査されます。
- カスタマーのルーティングとサービス プロバイダーのルーティングは対話する必要があります。
- CE からネットワーク管理サブネットの管理ホストへのアクセスが必要です。
- 設定の監査とルーティングの監査は、両方とも機能します。
- サービス保証エージェント（SA エージェント）を使用して、CE とシャドウ ルータ間の応答時間を測定できます。

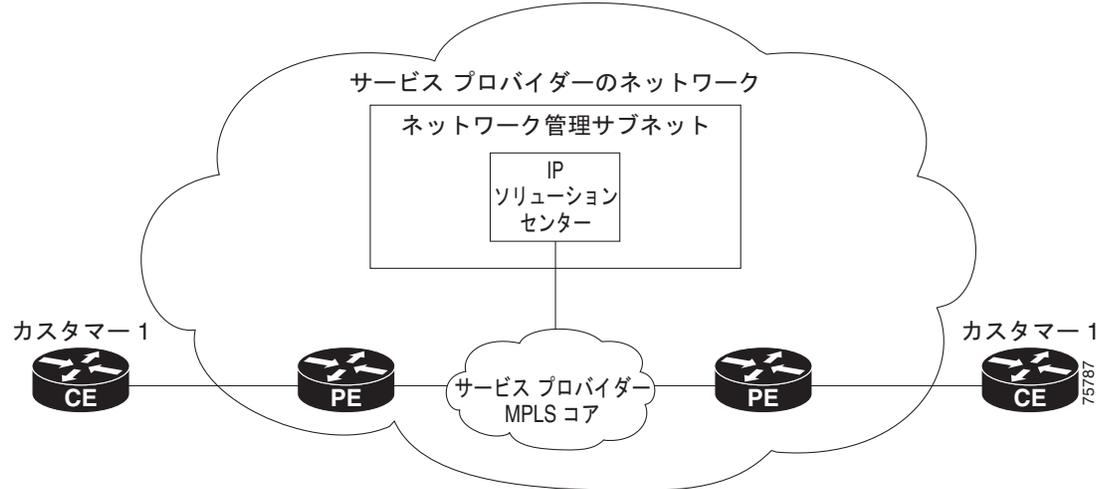
次の項では、管理対象 CE の環境を管理するために必要な概念と問題について説明します。

ネットワーク管理サブネット

ネットワーク管理サブネットは、プロバイダーのサービスに CE の管理が含まれている場合に必要です。CE が VPN にある場合、この項で説明するいずれかの技術が採用されていない限り、従来の IPv4 ルーティングでは利用できなくなります。

図 5-18 には、Prime Provisioning ネットワーク管理サブネットと、それに接続するために必要になる可能性のあるデバイスが示されています。

図 5-18 Prime Provisioning ネットワーク管理サブネット



VPN へのアクセスに関する問題

VPN へのアクセスに関する主な問題を次に示します。

- 不要なカスタマー ルートからプロバイダー空間を使用されないように保つ方法
- プロバイダーと他のカスタマーのルートのどちらによっても、カスタマー空間が「使用されない」ようにする方法
- 効果的なセキュリティを提供する方法
- ルーティング ループを回避する方法



(注) Prime Provisioning はこれらの作業のどちらも処理しません。これを行うには、サービス プロバイダーが設計および実装する必要があります。

- 到達可能性は、Prime Provisioning を採用することで受ける直接的な影響によって異なります。

Prime Provisioning で CE をプロビジョニングする前に、IPv4 接続によって CE に到達できる場合がありますが、製品がサービス要求を展開する時点ではその CE に到達することはできません。事前にネットワーク管理サブネットを設定しておく必要があります。

実装手法

ネットワーク管理サブネットでは、Management CE (MCE; 管理 CE) および PE にアクセスする必要があります。インバンド接続を介して管理対象 CE を接続する予定の場合、ネットワーク管理サブネットは適切であり、必要になります。インバンドとは単一のリンクまたは相手先固定接続 (PVC) を示し、カスタマーの VPN トラフィックとプロバイダーのネットワーク管理トラフィックの両方を実行します。

管理 CE (MCE)

ネットワーク管理サブネットは管理 CE (MCE) に接続されます。MCE は、カスタマー エッジ ルータ (CE) のロールをエミュレートしますが、MCE はプロバイダー空間に存在し、ネットワーク オペレーションセンターのゲートウェイ ルータとして動作します。MCE は、Prime Provisioning で定義されているように、管理サイトの一部です。Prime Provisioning の管理 LAN の一部として CE を識別し、MCE を設定します。

管理 PE (MPE)

管理 PE (MPE) は、プロバイダー コア ネットワークの PE ロールをエミュレートします。MPE はプロバイダーのコア ネットワークに MCE を接続します。MPE は、PE と MPE の両方として、二重の役割を持つことができます。

MPE は次のデバイスにアクセスする必要があります。

デバイス	接続	機能
1. カスタマー エッジ ルータ (CE)	ネットワーク管理サブネットから VPN へのアクセス	設定をプロビジョニングまたは変更し、SA エージェントのパフォーマンス データを収集します。
2. シャドウ CE	ネットワーク管理サブネットから VPN へのアクセス	2 台のデバイス間のデータの移行時間を測定するために使用されるシミュレートされた CE。シャドウ CE はイーサネットでは PE に直接接続されます。
3. プロバイダー エッジ ルータ (PE)	標準 IP 接続	設定をプロビジョニングまたは変更します。

現時点では、Prime Provisioning は次の 2 種類の主要なネットワーク管理サブネット内での実装手法を推奨します。

- 管理 VPN 手法

MPE-MCE リンクは管理 VPN (「[管理 VPN](#)」(P.5-131) を参照) を使用して、管理対象 CE に接続します。PE に接続するために、MPE-MCE リンクはパラレル IPv4 リンクを使用します。

- アウトオブバンド手法

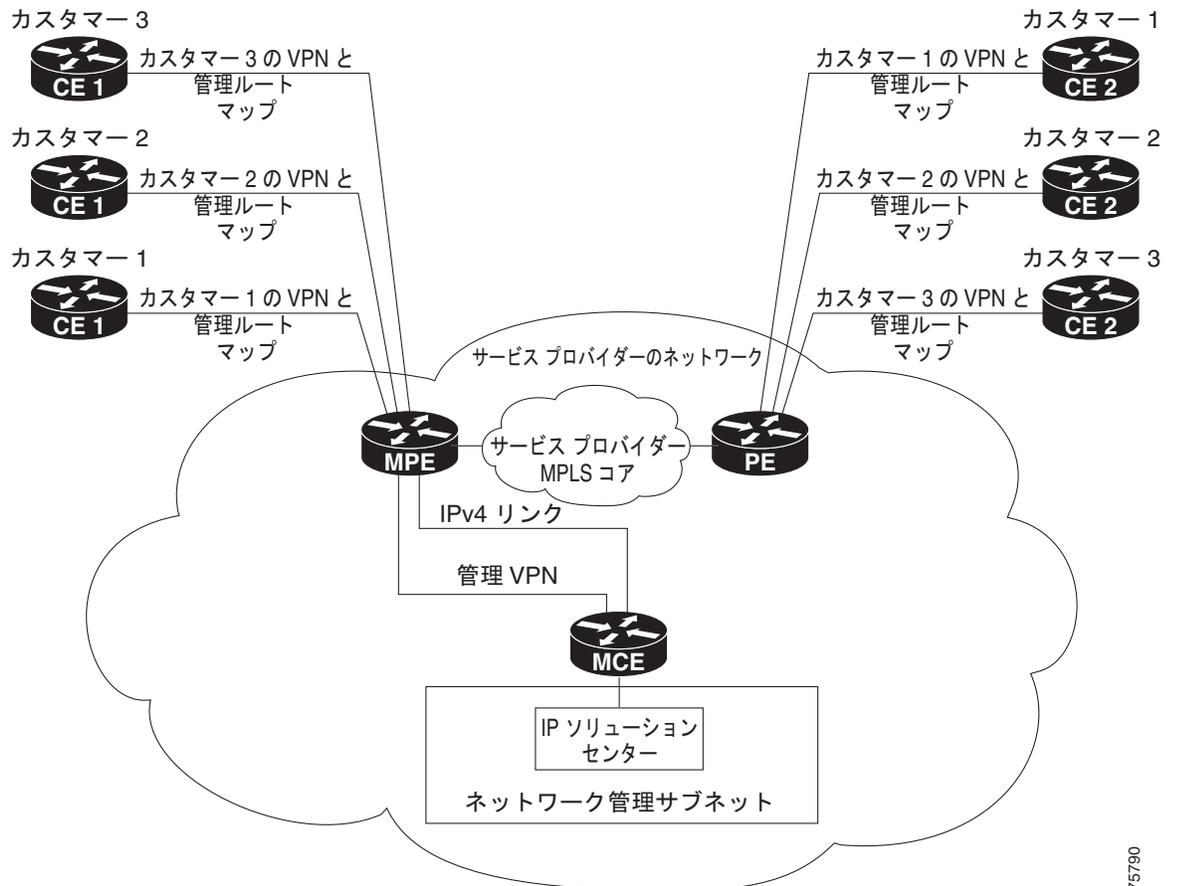
アウトオブバンド手法では、MCE にネットワークのすべての CE への IPv4 接続 (つまり、MPLS VPN 接続ではない) と PE があります (「[アウトオブバンド手法](#)」(P.5-132) を参照)。このため、アウトオブバンドではプロバイダーの管理トラフィックを伝送する別個のリンクが PE 間に示されます。

プロバイダーが実装するように選択するネットワーク管理サブネットの手法は、この項の後半で説明する多くの要因によって異なります。

管理 VPN

管理 VPN 手法は、Prime Provisioning によってプロビジョニングされるデフォルト方式です。この実装手法の重要な概念は、ネットワーク内のすべての CE が管理 VPN のメンバーであるということです。PE に接続するために、MPE-MCE リンクは平行 IPv4 リンクを使用します。図 5-19 には、管理 VPN 手法の一般的なトポロジが示されています。

図 5-19 管理 VPN ネットワークの一般的なトポロジ



75790

管理 VPN 手法を採用すると、MPE-MCE リンクは、管理 VPN を使用して管理対象 CE に接続します。PE に接続するために、MPE-MCE リンクは平行 IPv4 リンクを使用します。

カスタマー VPN の各 CE も、サービス要求ユーザ インターフェイスで [Join the management VPN] オプションを選択することで、管理 VPN に追加されます。

管理ルート マップの機能は、特定の CE へのルートのみを管理対象 VPN に許可することです。Cisco IOS では、VRF ごとに 1 つのエクスポート ルート マップと 1 つのインポート ルート マップのみをサポートします。

図 5-19 に示すように、PE まで到達するために、MPE と MCE の間に別の平行非 MPLS VPN リンクが必要です。



(注) 管理 VPN 手法の実装には、Cisco IOS 12.07 以降が必要です。

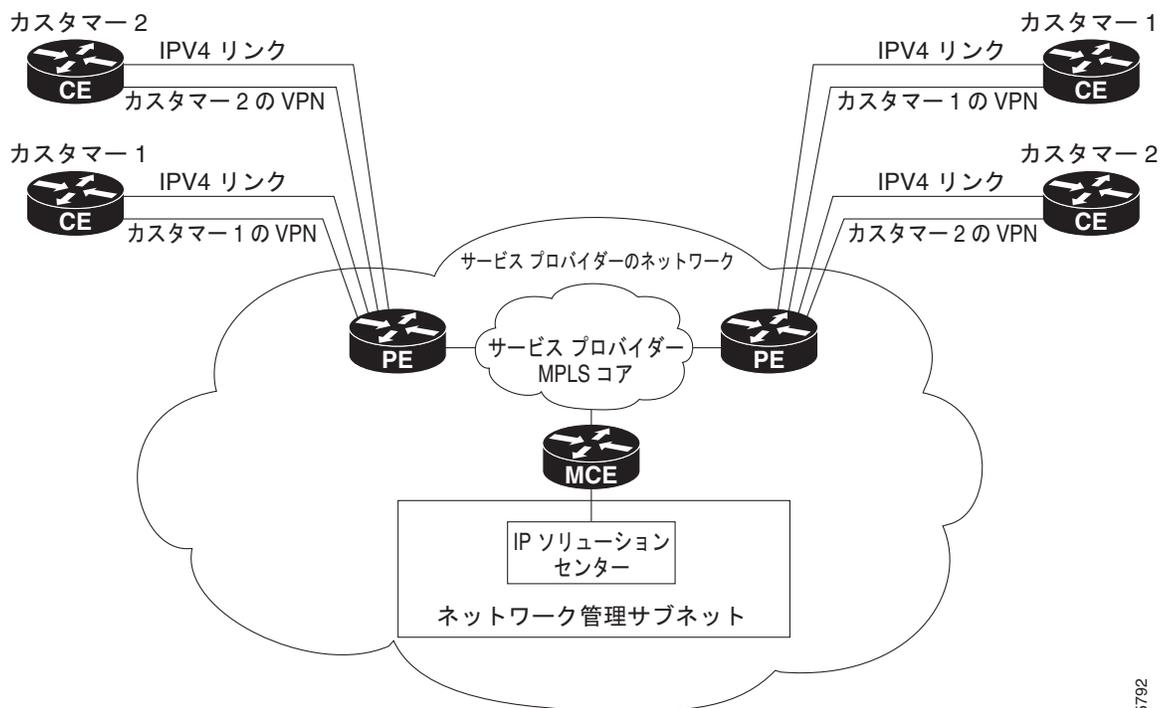
管理 VPN 手法を実装する利点は、次のとおりです。

- この方法でプロビジョニングすると、サービス要求が 1 回しか必要ありません。
- ネットワーク管理サブネットに与えられた唯一のルートは CE へのルートです。つまり、PE への CE リンクのアドレス、または CE ループバック アドレスです。一般的な VPN ルートは、ネットワーク管理サブネットに与えられません。
- 独自の VPN 内に CE が持つロールに関係なく、管理 VPN 手法の CE は管理 VPN へのスポークになります。したがって、CE を不適切なルートに誤って公開することはできません。CE が学習できる唯一の管理ルートは、管理 VPN のハブから出されている必要があります。

アウトオブバンド手法

アウトオブバンド手法では、管理 VPN を使用した CE の管理は行われません。アウトオブバンド接続は IPv4 リンクで提供されます。アウトオブバンドでは、プロバイダーの管理トラフィックを伝送する別個のリンクが PE 間に示されます。図 5-20 に示されているように、MCE はプロバイダーのルートとカスタマーのルートを分離します。

図 5-20 アウトオブバンド手法



アウトオブバンド手法には、設定が比較的容易であり、管理 VPN が不要であるという利点があります。ただし、各 CE に IPv4 接続が必要なため、コストが高いことが欠点です。また、この技術のステージングの要件は詳細であるため、アウトオブバンド実装は非常に複雑になります。

75792

Prime Provisioning での管理 CE のプロビジョニング

Prime Provisioning のネットワーク管理サブネットは管理 CE (MCE) に接続されます。MCE は、カスタマー エッジルータ (CE) のロールをエミュレートしますが、MCE はプロバイダー空間に存在し、ネットワーク オペレーション センターのゲートウェイ ルータとして動作します。MCE は、Prime Provisioning で定義されているように、管理サイトの一部です。

MCE としての CE の定義

Prime Provisioning ソフトウェアの管理 LAN の一部として CE を識別し、MCE を設定します。これを行うには、次の手順を実行します。

-
- ステップ 1** [Inventory] > [Resources] > [Customer Devices] を選択します。
現在定義されているすべてのカスタマーの CPE デバイスのリストが表示されます。
- ステップ 2** 管理 VPN 内の MCE として機能する CE を選択し、[Edit] をクリックします。
[Edit CPE Device] ダイアログボックスが表示され、選択した CPE に関連する情報が表示されます。
- ステップ 3** [Management Type] : ドロップダウン リストから、管理タイプを [Managed—Management LAN] に設定します。
- ステップ 4** [Save] をクリックします。
CPE デバイスのリストに戻ります。ここには、選択した CE の新しい管理タイプ (この例では、3. mlce8.cisco.com) が表示されます。
-

MCE サービス要求の作成

MCE サービス要求を作成するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
[Service Request Manager] ウィンドウが表示されます。
このウィンドウには、Prime Provisioning に定義されているすべての MPLS サービス ポリシーのリストが表示されます。
- ステップ 2** 目的のポリシーを選択して、[OK] をクリックします。
[MPLS Service Request Editor] が表示されます。
- ステップ 3** [Add Link] をクリックします。
これで、[MPLS Service Request Editor] に一連のフィールドが表示されるようになりました。[Select CE] フィールドがイネーブルであることを確認します。このサービスのリンクの定義に必要な最初のタスクは、リンクの CE を指定することです。
- ステップ 4** [CE] : [Select CE] をクリックします。
[Select CPE Device] ダイアログボックスが表示されます。
- [Show CPEs with] ドロップダウン リストから、[CEs by Customer Name]、[by Site]、または [by Device Name] を表示できます。
 - [Find] ボタンを使用して、特定の CE の検索または表示の更新のいずれかを行うことができます。
 - [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

- d. このダイアログボックスには、現在定義されている CE デバイスのリストの最初のページが表示されます。情報のページ数は、ダイアログボックスの右下隅に表示されます。

CE デバイスの別のページに移動するには、移動先のページ番号をクリックします。

- ステップ 5** [Select] 列で、MPLS リンクの MCE の名前を選択して、[Select] をクリックします。
[Service Request Editor] ウィンドウに戻ります。ここで、選択した CE の名前が [CE] 列に表示されるようになります。
- ステップ 6** [CE Interface] : インターフェイス選択機能を使用して、CE インターフェイスを選択します。
[PE] 列で、[Select PE] オプションがイネーブルになっていることに注意してください。
- ステップ 7** [PE] : [Select PE] をクリックします。
[Select PE Device] ダイアログボックスが表示されます。
- ステップ 8** [Select] 列で、MPLS リンクの PE の名前を選択して、[Select] をクリックします。
[Service Request Editor] ウィンドウに戻ります。選択した PE の名前が [PE] 列に表示されています。
- ステップ 9** [PE Interface] : インターフェイス選択機能を使用して、PE インターフェイスを選択します。
[Link Attribute] の [Add] オプションがイネーブルになっていることを確認します。
- ステップ 10** [Link Attribute] 列で [Add] をクリックします。
[MPLS Link Attribute Editor] ウィンドウが表示され、インターフェイス パラメータのフィールドが表示されます。

このウィンドウに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE および CE インターフェイス フィールドの詳細については、「[PE および CE インターフェイス パラメータの指定](#)」(P.5-45) を参照してください。



(注)

VLAN ID は PE および CE で共有されるため、両方で 1 個の VLAN ID です。[Second VLAN ID] は、PE インターフェイスでの着信フレームの Q-in-Q の 2 番目の VLAN タグを照合する方式を提供するオプションの属性です。これらの属性を使用する場合の詳細については、「[\[VLAN ID\] および \[Second VLAN ID\] 属性に関する注意事項](#)」(P.5-88) を参照してください。

- ステップ 11** この特定のリンクに対して変更する必要があるインターフェイス値があれば編集し、[Next] をクリックします。
[MPLS Link Attribute Editor] で [IP Address Scheme] が表示されます。
このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。[IP Address Scheme] フィールドの詳細については、「[IP アドレススキームの指定](#)」(P.5-48) を参照してください。
- ステップ 12** この特定のリンクで変更する必要があるすべての IP アドレス スキーム値を編集し、[Next] をクリックします。
[MPLS Link Attribute Editor for Routing Information] が表示されます。
このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。PE および CE に関するルーティング情報の詳細については、「[サービスのルーティング プロトコルの指定](#)」(P.5-51) を参照してください。
このサービスに使用されているサービス ポリシーによってルーティング プロトコルが編集可能と指定されているため、必要に応じてこのサービス要求のルーティング プロトコルを変更できます。
- ステップ 13** この特定のリンクに対して変更する必要があるルーティング プロトコル値があれば編集し、[Next] をクリックします。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。VRF および VPN の情報の詳細については、「[VRF および VPN の情報の定義 \(P.5-76\)](#)」を参照してください。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義 \(P.5-91\)](#)」を参照してください。

ステップ 14 この特定のリンクで変更する必要があるすべての VRF 値を編集します。

ステップ 15 テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。

[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。



(注) 上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、この後のステップ 34 に進みます。

ステップ 16 デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。

[MPLS Service Request Editor] ウィンドウが再表示されます。

ステップ 17 [Add Link] を選択し、サービスの次のリンクの属性を指定することにより、このサービス要求にさらにリンクを追加できます。

ステップ 18 [MPLS Service Request Editor] ウィンドウに作業を保存するには、[Save] をクリックします。

[Service Requests] ウィンドウに戻ります。ここでは、サービス要求が [Requested] 状態になっており、展開の準備が整っています。

管理 VPN への PE-CE リンクの追加

管理 VPN の作成を完了すれば、管理 VPN に参加させる PE-CE リンク用のサービスの追加に進むことができます。これを行うには、次の手順を実行します。

ステップ 1 選択した CE の [MPLS Link Attribute Editor - VRF and VPN] ウィンドウに移動します。

ステップ 2 [Join the management VPN] オプションをオンにします。

この手順で管理 VPN を使用して CE に参加すると、Prime Provisioning によって適切なルート マップ ステートメントが PE コンフィグレットに生成されます。管理ルート マップの機能は、特定の CE へのルートのみを管理対象 VPN に許可することです。Cisco IOS では、VRF ごと（したがって VPN ごと）に 1 つのエクスポート ルート マップおよび 1 つのインポート ルート マップだけをサポートします。

ステップ 3 サービス要求のユーザ インターフェイスを実行します。

ケーブル サービスのプロビジョニング

MPLS VPN テクノロジーを使用して、サービス プロバイダーは共有ハイブリッド ファイバの同軸 (HFC) ネットワークとインターネット プロトコル (IP) インフラストラクチャを使用してスケラブルかつ効率的にプライベート ネットワークを作成できます。ケーブル MPLS VPN ネットワークは、次の 2 種類の主要要素で構成されています。

- ケーブルおよび IP バックボーンを介してトラフィックを伝送するためにインターネット サービス プロバイダー (ISP) の VPN を作成し、物理インフラストラクチャを持つマルチプル サービス オペレータ (MSO) またはケーブル会社。
- HFC ネットワークおよび IP インフラストラクチャを使用して、ケーブル カスタマーにインターネット サービスを提供する ISP。

ケーブル MPLS VPN の利点

MPLS VPN によるケーブル サービスのプロビジョニングには、次のような利点があります。

- MPLS VPN は、ケーブル MSO および ISP に、ケーブル プラントへの複数のアクセスをサポートする管理可能な方法を提供します。

サービス プロバイダーは、ネットワークのコア上にスケラブルで効率的な VPN を構築できます。MPLS VPN は、ケーブル転送インフラストラクチャおよび管理についてシステムのサポート スケーラビリティを提供します。

- 各 ISP は、加入者の PC から MSO の物理ケーブル設備を経由して ISP のネットワークに至るインターネット アクセス サービスをサポートできます。
- MPLS VPN により、MSO は ISP を介して付加価値のあるサービスを提供できるようになるため、より広い範囲の潜在顧客に接続を提供できます。

MSO は ISP と連携して複数の ISP から複数のサービスを配信し、VPN 技術を使用して MSO の独自のネットワーク内の値を追加できます。

- 加入者はさまざまなサービス プロバイダーからのサービスを組み合わせて選択できます。
- サービスを確保するために Cable Modem Termination Server (CMTS) および DOCSIS 1.0 拡張にビルドされた Cisco IOS MPLS VPN ケーブル機能セットは信頼でき、ケーブル設備を介して配信するのが最適です。

MPLS VPN は、システム サポートのドメイン選択、加入者ごとの認証、QoS の選択、ポリシー ベース ルーティング、および QoS と課金のためにケーブル モデムの背後にある加入者エンド デバイスに到達する機能を提供し、同時にセッション スプーフィングを防止しています。

- MPLS VPN テクノロジーは、共有ケーブル インフラストラクチャ全体にわたるセキュアなアクセスとサービスの整合性の両方を実現します。

ケーブル MPLS VPN ネットワーク

図 5-21 に示すように、各 ISP は、MSO の物理ネットワーク インフラストラクチャを介して、加入者の PC に対するトラフィックを ISP のネットワークに移動します。MPLS VPN は、レイヤ 3 で作成され、VPN のルートの振り分けをそのネットワークに属するルータだけに制限することで、プライバシーとセキュリティを提供します。したがって、各 ISP の VPN は同じ MSO インフラストラクチャを使用する他の ISP から絶縁されています。

MPLS ベースのケーブル方式では、VPN は共有ケーブル設備と MPLS コア バックボーンに組み込まれているプライベート ネットワークです。パブリック ネットワークは、共有ケーブル設備またはバックボーン接続ポイントです。ケーブル設備はインターネット アクセス サービスをサポートし、MSO とその加入者のトラフィックに加え、複数のインターネット サービス プロバイダー (ISP) とその加入者のトラフィックを伝送できます。

MPLS VPN は、各 VPN に固有の VPN ルーティングおよび転送 (VRF) インスタンスを割り当てます。VRF インスタンスは、1 つの IP ルーティング テーブル、取得された転送テーブル、フォワーディング テーブルを使用する一連のインターフェイス、および転送テーブルの内容を決定する一連のルールとルーティング プロトコルで構成されています。

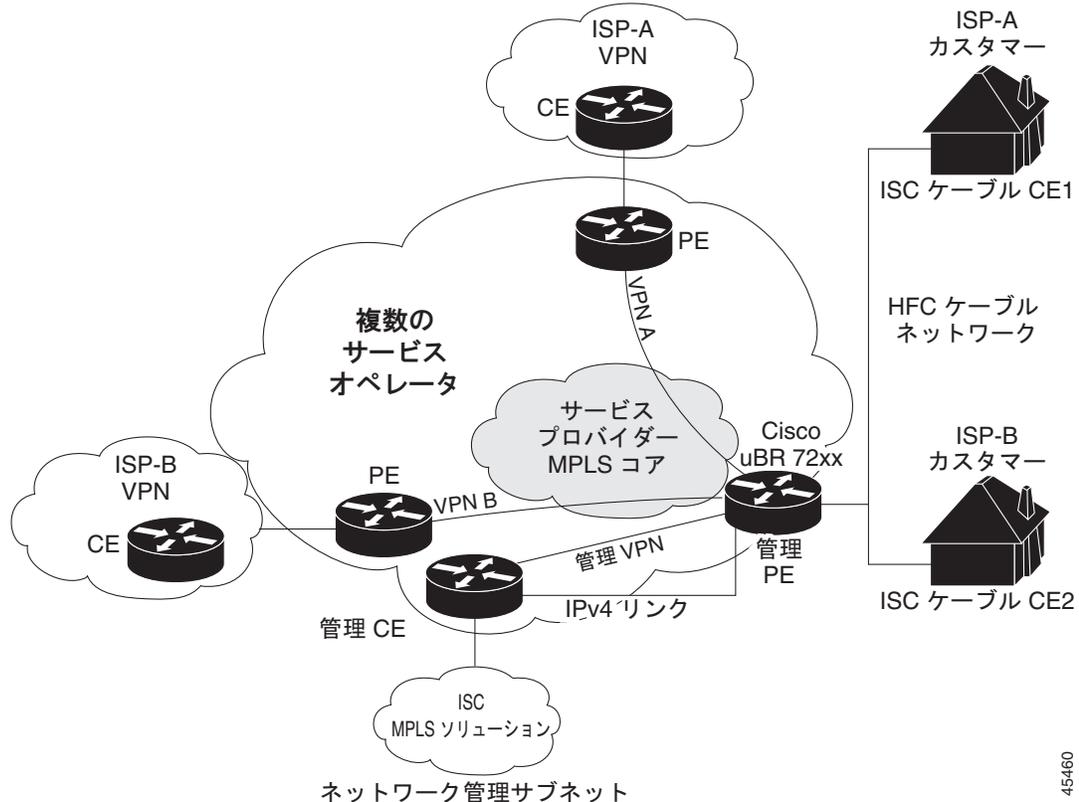
各 PE ルータは 1 つ以上の VRF テーブルを維持します。パケットが特定の VRF に関連付けられたインターフェイスから直接到着すると、PE は適切な VRF テーブルでパケットの IP 宛先アドレスを検索します。MPLS VPN は BGP と IP アドレス解決の組み合わせを使用してセキュリティを保証します。

ケーブル ネットワークのルータは次のとおりです。

- プロバイダー (P) ルータ：サービス プロバイダー ネットワークの MPLS コアのルータ。P 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 (PE ルータによって割り当てられた、各ルート内の MPLS ラベル) を付加しません。VPN ラベルは、データ パケットを正しい出カールータに誘導します。
- プロバイダー エッジ (PE) ルータ：着信パケットが受信されるインターフェイスまたはサブインターフェイスに基づいて、着信パケットに VPN ラベルを付加するルータ。PE ルータは、CE ルータに直接接続します。MPLS-VPN 手法では、それぞれの Cisco uBR72xx シリーズ ルータが PE ルータとして動作します。
- Customer (C; カスタマー) ルータ：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：MSO のネットワークの PE ルータに接続する ISP のネットワークのエッジルータ。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。
- 管理 CE (MCE) ルータ：MCE は、カスタマー エッジルータ (CE) のロールをエミュレートしますが、MCE はプロバイダー空間に存在し、ネットワーク オペレーション センターのゲートウェイ ルータとして動作します。ネットワーク管理サブネットは管理 CE (MCE) に接続されます。MCE は、Prime Provisioning で定義されているように、管理サイトの一部です。
- Management PE (MPE; 管理 PE) ルータ：MPE は、プロバイダー コア ネットワーク内で PE のロールをエミュレートします。MPE はプロバイダーのコア ネットワークに MCE を接続します。MPE は、PE と MPE の両方として、二重の役割を持つことができます。

共有ケーブル設備は、ISP A からその加入者、および ISP B からその加入者へのインターネット接続をサポートします。

図 5-21 MPLS VPN ケーブル ネットワークの例



45/60

ケーブル ネットワークの管理 VPN

MPLS ネットワークには固有の VPN があり、この VPN は排他的に MSO デバイスを管理するため、管理 VPN と呼ばれます。その他の VPN がアクセスできるデバイス、およびサーバが含まれます。管理 VPN は管理 CE (MCE) ルータと管理サブネットを MSO PE ルータ (uBr72xx ルータまたは同等のもの) に接続します。Prime Provisioning や、Dynamic Host Configuration Protocol (DHCP)、Cisco Network Registrar (CNR) Time of Day (ToD) などの管理サーバは、管理サブネットの一部であり、ISP 接続用の管理 VPN 内に含まれます。管理 VPN の説明については、「[プロビジョニング管理 VPN \(P.5-126\)](#)」を参照してください。

図 5-21 に示されているように、管理 VPN はネットワーク管理サブネット (ここに Prime Provisioning ワークステーションがおかれている) で構成されており、これは管理 CE (MCE) に直接接続されます。管理 VPN は MCE とケーブル VPN ゲートウェイ間の特別な VPN です。通常、ケーブル VPN ゲートウェイは標準 PE と管理 PE の両方として機能する Cisco uBR 72xx ルータです。MCE と MPE の間には、パラレル IPv4 リンクもあることに注目してください。

ケーブル VPN 設定の概要

ケーブル VPN 設定には、次のものがあります。

- 各企業ネットワークへの直接ピアリングが必要な MSO ドメイン (Prime Provisioning)、個人用および商用の加入者向けプロビジョニングサーバ、商用ユーザ向けのダイナミック DNS。MSO は、ケーブルインターフェイス IP アドレッシング、Data Over Cable Service Interface Specifications

(DOCSIS; データオーバーケーブル サービス インターフェイス仕様) のプロビジョニング、ケーブル モデムのホスト名、ルーティングの修正、特権レベル、およびユーザ名とパスワードを管理します。

- 加入者または在宅勤務者のホスト デバイス用の DHCP サーバ、MSO アドレス空間内のエンタープライズ ゲートウェイ、および在宅勤務者のサブネットに戻るスタティック ルートがある、ISP またはエンタープライズ ドメイン。



(注) シスコは、MSO でエンド ユーザ デバイスとゲートウェイ インターフェイスにすべてのアドレスを割り当てることを推奨します。MSO では分割管理を使用して ISP でトンネルとセキュリティを設定できるようにすることもできます。

ケーブル サービスの MPLS VPN を設定するには、MSO で次を設定する必要があります。

- Cable Modem Termination System (CMTS)。通常、CMTS は Cisco uBR72xx シリーズ ルータです。MSO では ISP が動作する Cisco uBR72xx シリーズ ルータを設定する必要があります。
- PE ルータ。MSO は VPN の PE として ISP に接続する PE ルータを設定する必要があります。



ヒント ケーブル サービス用の MPLS VPN を設定する場合、PE にケーブル メンテナンス用のサブ インターフェイスを設定する必要があります。ケーブル メンテナンス用のインターフェイスを使用することで、ケーブルのデバイスはその IP アドレスを取得できます。このため、ケーブル サービスのプロビジョニングを実行するには、メンテナンス用のサブ インターフェイスを設定しておく必要があります。

- CE ルータ。
- P ルータ。
- ISP あたり 1 つの VPN。
- すべてのケーブル モデムのカスタマーの DOCSIS サーバ。MSO は管理 VPN に DOCSIS サーバを接続し、ネットワークで認識されるようにする必要があります。

MSO はプライマリ IP アドレスの範囲を決定する必要があります。プライマリ IP アドレスの範囲は、ISP の加入者に属するすべてのケーブル モデムの MSO のアドレス範囲です。

ISP はセカンダリ IP アドレスの範囲を決定する必要があります。セカンダリ IP アドレスは、その加入者 PC の ISP のアドレス範囲です。

セキュリティ違反を減らし、DHCP 要求と VPN または特定の ISP 管理でのケーブル モデムを区別するために、MSO は、Cisco IOS ソフトウェアで **cable helper-address** コマンドを使用できます。MSO は、ISP の VPN でのみアクセスできるようにホスト IP アドレスを指定できます。これにより、ISP はその DHCP サーバを使用して IP アドレスを割り当てることができるようになります。ケーブル モデム IP アドレスは、管理 VPN からアクセスできることが必要です。

Prime Provisioning に、メンテナンス ヘルパー アドレスとホスト ヘルパー アドレス、およびケーブル サブインターフェイスのセカンダリ アドレス指定します。

ケーブル VPN インターフェイスおよびサブインターフェイス

ケーブル加入者環境では、数千もの加入者が単一の物理インターフェイスを共有します。複数の論理サブインターフェイスを使用した設定は、ケーブルを介した MPLS VPN ネットワークに不可欠な要素です。複数のサブインターフェイスを設定し、各サブインターフェイスに特定の VRF を関連付けることができます。1 つの物理インターフェイス (ケーブル設備) を複数のサブインターフェイスに分割できます。この場合、各サブインターフェイスは特定の VRF に関連付けられます。各 ISP は、物理イン

ターフェイス上でアクセスすることが必要で、各自のサブインターフェイスが与えられます。MSO の管理者は、ケーブル物理インターフェイス上にサブインターフェイスを定義し、レイヤ 3 設定を各サブインターフェイスに割り当てます。

個々の ISP またはお客様に対して VPN を作成する MPLS VPN の手法では、サブインターフェイスをケーブル インターフェイスに設定する必要があります。各 ISP には 1 つのサブインターフェイスが必要です。サブインターフェイスは、それぞれの ISP の VPN ルーティングおよび転送 (VRF) テーブルに関連付けられます。

ケーブル インターフェイスにメンテナンス用のサブインターフェイスを作成し、それを管理 VPN に関連付ける必要があります。メンテナンス用のインターフェイスは、ISP で使用されるためのものであり、VPN 接続に加え、ISP と管理 VPN 間のエクストラネットを使用する管理 VPN 用に使用されます。

Prime Provisioning は VRF に基づいてサブインターフェイス番号を自動的に選択します。現在の VRF に関連付けられているサブインターフェイスがまだ存在しない場合、Prime Provisioning はサブインターフェイスを作成し、それを適切な VRF に割り当てます。サブインターフェイス番号には、選択したケーブル インターフェイスに現在割り当てられている最大のサブインターフェイス番号よりも 1 つ大きい番号が割り当てられます。

管理 VPN を使用して ISP の VPN から管理 CE (MCE) への 1 つのフィルタリング済みルートに接続できるため、ネットワーク管理サブネット (CNR、ToD、および Prime Provisioning を含む) はケーブル モデムに応答できます。同様に、管理要求 (CNR への DHCP 更新など) を転送するために、ISP VPN は管理 VPN の MCE にルートをインポートする必要があります。

Cisco uBR7200 シリーズ ソフトウェアは、ケーブルの物理インターフェイスを介した論理ネットワーク レイヤ インターフェイスの定義をサポートしています。システムは、物理ケーブル インターフェイスでのサブインターフェイスの作成をサポートしています。

サブインターフェイスを使用して、トラフィックを単一の物理インターフェイスで区別し、複数の VPN に関連付けることができます。各 ISP は、物理インターフェイス上でアクセスすることが必要で、各自のサブインターフェイスが与えられます。特定の VPN の (および ISP) 加入者に関連付けられた各サブインターフェイスを使用して、加入対象のサービスを提供する ISP を反映する論理サブインターフェイスに接続します。適切に設定されると、加入者トラフィックは適切なサブインターフェイスと VPN に入ります。

Prime Provisioning でのケーブル サービスのプロビジョニング

Prime Provisioning でケーブル サービスをプロビジョニングするために完了する必要がある作業は次のとおりです。

- ケーブル インターフェイスを持つ PE を該当する領域に追加します。
- ケーブル メンテナンス インターフェイスのプロビジョニングを行うサービス要求を PE で生成します。
- 2 番目のサービス要求を生成して、MPLS ベースのケーブル サービスをプロビジョニングします。このケーブル サービス要求は各 VPN に対して生成する必要があります。

Prime Provisioning を使用してケーブル サービスをプロビジョニングする場合、標準 MPLS VPN をプロビジョニングする場合と同様の理由で、CE はありません。このため、PE-Only ポリシーを使用するか、CE なしのケーブル ポリシーを作成する必要があります。

サービス要求の作成

ここでは、次の内容について説明します。

- 「[MPLS VPN PE-CE サービス要求の作成](#)」 (P.5-86)

- 「ケーブルのリンクのサービス要求の作成」 (P.5-143)

ケーブルのサブインターフェイスのサービス要求の作成

PE のケーブル メンテナンス用のサブインターフェイスを使用することで、ケーブルのデバイスはその IP アドレスを取得できます。このため、ケーブル サービスをプロビジョニングする前に、メンテナンス用のサブインターフェイスを設定しておく必要があります。ケーブルのサブインターフェイス サービス要求を作成するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
[MPLS Policy Selection] ダイアログボックスが表示されます。このダイアログボックスには、Prime Provisioning に定義されているすべての MPLS サービス ポリシーのリストが表示されます。
- ステップ 2** PE だけのポリシー（上記の例の場合 **cable**）を選択して、[OK] をクリックします。
[MPLS Service Request Editor] が表示されます。
- ステップ 3** [Add Link] をクリックします。
これで、[MPLS Service Request Editor] に一連のフィールドが表示されるようになりました。[Select PE] フィールドがイネーブルであることを確認します。このサービスのリンクの定義に必要な最初のタスクは、リンクの PE を指定することです。
- ステップ 4** [PE] : [Select PE] をクリックします。
[Select PE Device] ダイアログボックスが表示されます。
- ステップ 5** [Select] 列で、MPLS リンクの PE の名前を選択して、[Select] をクリックします。
[Service Request Editor] ウィンドウに戻ります。選択した PE の名前が [PE] 列に表示されています。
- ステップ 6** [PE Interface] : インターフェイス選択機能を使用して、PE インターフェイスを選択します。
主要なインターフェイス名だけがリストに表示され選択できるようになっています。Prime Provisioning は、各 VPN に適切なサブ インターフェイス番号を割り当てます。
[Link Attribute] の [Add] オプションがイネーブルになっていることを確認します。
- ステップ 7** [Link Attribute] 列で [Add] をクリックします。
[MPLS Link Attribute Editor] が表示され、インターフェイス パラメータのフィールドが示されます。
- ステップ 8** [Interface Description] フィールドにサブインターフェイス名を入力します。
- ステップ 9** [Cable Maintenance Interface] のチェックボックスをオンにして、[Edit beside Cable Helper Addresses] をクリックします。
[Cable Helper Addresses] ウィンドウが表示されます。
- ステップ 10** [Add] をクリックします。
[Cable Helper Addresses] ウィンドウが表示されます。
- ステップ 11** IP アドレスを [IP Address] フィールドに入力し、[IP Type] に [Both] を選択します。
ケーブル モデムと接続先 CPE デバイス（ホスト）は、宛先 IP アドレスに DHCP パケットをブロードキャストします。この宛先 IP アドレスは設定済みのケーブルのヘルパー アドレスです。このため、設定済みのケーブルのヘルパー アドレスから、ケーブル モデムと接続先 CPE（ホスト）は（CM と CPE）IP アドレスを受信します。
[IP Type] には次の値があります。

- [Host] : これを選択されると、ホスト (CPE デバイス) からの UDP ブロードキャストのみがその特定の宛先 IP アドレスに転送されます。(たとえば、ホストのみが当該ヘルパー アドレスからの IP アドレスを受信します)。
- [Modem] : これを選択されると、ケーブル モデムからの UDP ブロードキャストのみがその特定の宛先 IP アドレスに転送されます。(たとえば、ケーブル モデムだけが当該ヘルパー アドレスからの IP アドレスを受信します)。
- [Both] : これを選択されると、ホスト (CPE デバイス) とケーブル モデムからの UDP ブロードキャストがその特定の宛先 IP アドレスに転送されます。(たとえば、ケーブル モデムとホストのみが当該ヘルパー アドレスからの IP アドレスを受信します)。

ステップ 12 [OK] をクリックします。

[MPLS Link Attribute Editor] が再表示されます。

ステップ 13 [Next] をクリックします。

[MPLS Link Attribute Editor - IP Address Scheme] が表示されます。

ステップ 14 この特定のリンクで変更する必要があるすべての IP アドレス スキーム値を編集し、[Next] をクリックします。[MPLS Link Attribute Editor for Routing Information] が表示されます。

次のルーティング プロトコル オプションがサポートされています。

- STATIC
- RIP
- OSPF
- EIGRP
- None

このサービスに使用されているサービス ポリシーによってルーティング プロトコルが編集可能と指定されているため、必要に応じてこのサービス要求のルーティング プロトコルを変更できます。

ステップ 15 この特定のリンクに対して変更する必要があるルーティング プロトコル値があれば編集し、[Next] をクリックします。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「独立 VRF 管理」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

ステップ 16 [Join the Management VPN] のチェックボックスをオンにします。

ステップ 17 この特定リンクに対して変更する必要がある VRF および VPN の値があれば編集します。

- ステップ 18** テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。
- [MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。



(注) 上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、この後のステップ 34 に進みます。

- ステップ 19** デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。



(注) このサービス要求に複数のリンクを定義できます。

- ステップ 20** このサービス要求の作業を保存するには、[Save] をクリックします。
- [MPLS Service Requests] ウィンドウが再表示され、サービス要求が [Requested] 状態になり、展開可能になっていることが示されます。

ケーブルのリンクのサービス要求の作成

ケーブル リンクのサービス要求を作成するには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
- [MPLS Policy Selection] ダイアログボックスが表示されます。このダイアログボックスには、Prime Provisioning に定義されているすべての MPLS サービス ポリシーのリストが表示されます。
- ステップ 2** 目的のポリシーを選択して、[OK] をクリックします。
- [MPLS Service Request Editor] が表示されます。
- ステップ 3** [Add Link] をクリックします。
- これで、[MPLS Service Request Editor] に一連のフィールドが表示されるようになりました。[PE] 列で、[Select PE] オプションがイネーブルになっていることに注意してください。
- ステップ 4** [PE] : [Select PE] をクリックします。
- [Select PE Device] ダイアログボックスが表示されます。
- ステップ 5** [Select] 列で、MPLS リンクの PE の名前を選択して、[Select] をクリックします。
- [Service Request Editor] ウィンドウに戻ります。選択した PE の名前が [PE] 列に表示されています。
- ステップ 6** [PE Interface] : インターフェイス選択機能を使用して、PE インターフェイスを選択します。
- [Link Attribute] の [Add] オプションがイネーブルになっていることを確認します。

- ステップ 7** [Link Attribute] 列で [Add] をクリックします。
[MPLS Link Attribute Editor] が表示され、インターフェイス パラメータのフィールドが表示されます。



(注) [Cable Maintenance Interface] のボックスはオンにしないでください。

- ステップ 8** この特定のリンクに対して変更する必要があるインターフェイス値があれば編集し、[Edit beside Cable Helper Addresses] をクリックします。

[Cable Helper Addresses] ウィンドウが表示されます。

- ステップ 9** [Add] をクリックします。

[Cable Helper Addresses] ウィンドウが表示されます。

- ステップ 10** IP アドレスを [IP Address] フィールドに入力し、[IP Type] の [Both]、[Modem]、または [Host] を選択します。

ケーブル モデムと接続先 CPE デバイス (ホスト) は、宛先 IP アドレスに DHCP パケットをブロードキャストします。この宛先 IP アドレスは設定済みのケーブルのヘルパー アドレスです。このため、設定済みのケーブルのヘルパー アドレスから、ケーブル モデムと接続先 CPE (ホスト) は (CM と CPE) IP アドレスを受信します。

[IP Type] には次の値があります。

- [Host]: これが選択されると、ホスト (CPE デバイス) からの UDP ブロードキャストのみがその特定の宛先 IP アドレスに転送されます。(たとえば、ホストのみが当該ヘルパー アドレスからの IP アドレスを受信します)。
- [Modem]: これが選択されると、ケーブル モデムからの UDP ブロードキャストのみがその特定の宛先 IP アドレスに転送されます。(たとえば、ケーブル モデムだけが当該ヘルパー アドレスからの IP アドレスを受信します)。
- [Both]: これが選択されると、ホスト (CPE デバイス) とケーブル モデムからの UDP ブロードキャストがその特定の宛先 IP アドレスに転送されます。(たとえば、ケーブル モデムとホストのみが当該ヘルパー アドレスからの IP アドレスを受信します)。

- ステップ 11** [OK] をクリックします。

[MPLS Link Attribute Editor] が再表示されます。

- ステップ 12** セカンダリ アドレスの横の [Edit] をクリックします。

[Cable Secondary Addresses] ウィンドウが表示されます。セカンダリ IP アドレスは、ケーブル モデムに接続された CPE デバイス (ホスト) をイネーブルにして、CMTS と通信します。(通常、これは PC がインターネットにアクセスできるようにするためのパブリック IP アドレスです)。

- ステップ 13** IP アドレスを [IP address/Mask] フィールドに入力し、[OK] をクリックします。

[MPLS Link Attribute Editor] が再表示されます。

- ステップ 14** [Next] をクリックします。

- ステップ 15** [MPLS Link Attribute Editor] で [IP Address Scheme] が表示されます。

- ステップ 16** この特定のリンクで変更する必要があるすべての IP アドレス スキーム値を編集し、[Next] をクリックします。

[MPLS Link Attribute Editor for Routing Information] が表示されます。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

ステップ 17 この特定のリンクに対して変更する必要があるルーティング プロトコル値があれば編集し、[Next] をクリックします。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。このダイアログボックスに表示されるフィールド値には、このサービスに関連付けられたサービス ポリシーで指定された値が反映されます。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「[独立 VRF 管理 \(P.5-15\)](#)」を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義 \(P.5-91\)](#)」を参照してください。

ステップ 18 [Join the Management VPN] のチェックボックスをオンにします。

ステップ 19 この特定リンクに対して変更する必要がある VRF および VPN の値があれば編集し、[Add] をクリックします。

[Select CERCs/VPN] ダイアログボックスが表示されます。

ステップ 20 カスタマー名と VPN を選択します。

ステップ 21 [Join as Spoke] をクリックして、[Done] をクリックします。

[MPLS Link Attribute Editor] で VRF 属性および VPN 属性が表示されます。

ステップ 22 この特定リンクに対して変更する必要がある VRF および VPN の値があれば編集します。

ステップ 23 テンプレートまたはデータ ファイルをサービス要求に関連付けるには、[Next] ボタンをクリックします。

[MPLS Link Attribute Editor - Template Association] ウィンドウが表示されます。このウィンドウでは、デバイスの [Template/Data File] 列で [Add] ボタンをクリックして、テンプレートとデータ ファイルをデバイスに関連付けることができます。[Add] ボタンをクリックすると、[Add/Remove Templates] ウィンドウが表示されます。サービス要求へのテンプレートの関連付け方法、およびこのウィンドウでの機能の使用方法については、[第 9 章「テンプレートおよびデータ ファイルの管理」](#)を参照してください。



(注) 上記の手順では、サービス要求の基盤となるポリシーでテンプレートの関連付けがイネーブルになっていることを想定しています。なっていない場合は、GUI に [Next] ボタンは表示されません。その場合は、[Finish] をクリックして [MPLS Service Request Editor] ウィンドウに戻り、次のステップ 27 に進みます。

ステップ 24 デバイスのテンプレートとデータ ファイルの設定が完了したら、[Template Association] ウィンドウで [Finish] をクリックしてこのウィンドウを閉じ、[MPLS Service Request Editor] ウィンドウに戻ります。



(注) このサービス要求に複数のリンクを定義できます。

ステップ 25 このサービス要求の作業を保存するには、[Save] をクリックします。

[MPLS Service Requests] ウィンドウが再表示され、サービス要求が [Requested] 状態になり、展開可能になっていることが示されます。

Carrier Supporting Carrier のプロビジョニング

この項では、Prime Provisioning プロビジョニング プロセスを使用し、Carrier Supporting Carrier (CSC) 機能を設定する方法について説明します。次の事項について説明します。

- 「Carrier Supporting Carrier の概要」 (P.5-146)
- 「CSC のサービス ポリシーの定義」 (P.5-150)
- 「CSC サービス要求のプロビジョニング」 (P.5-150)

Carrier Supporting Carrier の概要

Carrier Supporting Carrier (CSC) 機能を使用すると、MPLS VPN ベース サービス プロバイダーは、バックボーン ネットワークのセグメントの使用を他のサービス プロバイダーに許可できます。他のプロバイダーにバックボーン ネットワークのセグメントを提供するサービス プロバイダーは、バックボーン キャリアと呼ばれます。バックボーン ネットワークのセグメントを使用するサービス プロバイダーは、カスタマー キャリアと呼ばれます。

このマニュアルでは、Border Gateway Protocol および Multiprotocol Label Switching (BGP/MPLS) VPN サービスを提供するバックボーン キャリアに焦点を当てます。カスタマー キャリアには、次の 2 つのタイプがあります。

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

このマニュアルでは、両タイプのカスタマー キャリアについて説明します。

これは、基本的な MPLS VPN CSC に必要な機能がバックボーン ネットワークで実装された後、いずれかのシナリオが使用されている場合に、バックボーン プロバイダーに対して透過的です。

Prime Provisioning で、カスタマー キャリア PE デバイスは CE デバイスとしてモデル化され、バックボーン キャリア PE デバイスは N-PE デバイスとしてモデル化されます。CSC オプションを含む MPLS サービス要求は、これらの PE および CE デバイスで作成できます。CSC 機能は IOS および IOS XR PE デバイスで設定できます。

CSC サービスは次の PE-CE リンク設定の適用されます。

- IPv4 ユニキャスト
- IPv4 マルチキャスト

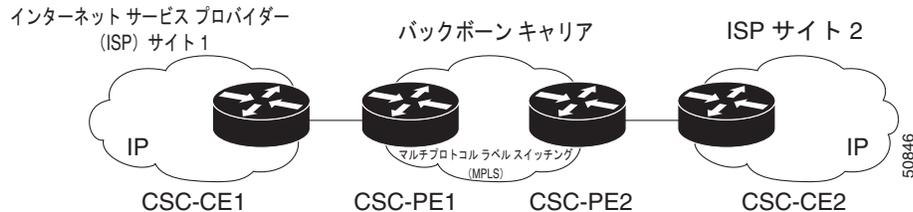
CSC サービスは、IOS XR デバイスでの BGP PE-CE ルーティング プロトコルに適用されます。

ISP カスタマー キャリアを含むバックボーン ネットワーク

このネットワーク設定では、カスタマー キャリアに 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、MPLS を使用するバックボーン 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。ISP サイトは IP を使用します。ISP サイトとバックボーン キャリア間のパケット転送をイネーブルにするには、ISP をバックボーン キャリアに接続する CSC-CE ルータで MPLS が実行されている必要があります。

図 5-22 に、カスタマー キャリアが ISP である Carrier Supporting Carrier ネットワーク設定を示します。このカスタマー キャリアには 2 つのサイトがあり、それぞれが Point of Presence (POP) です。カスタマー キャリアは、バックボーン キャリアによって提供される VPN サービスを使用してこれらのサイトを接続します。バックボーン キャリアは MPLS を使用します。ISP サイトは IP を使用します。ISP サイトとバックボーン キャリア間の packet 転送をイネーブルにするには、ISP をバックボーン キャリアに接続する CSC-CE ルータで MPLS が実行されている必要があります。

図 5-22 ISP カスタマー キャリアを含む Carrier Supporting Carrier ネットワーク



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

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

内部ルートと外部ルートは、次の方法で区別されています。

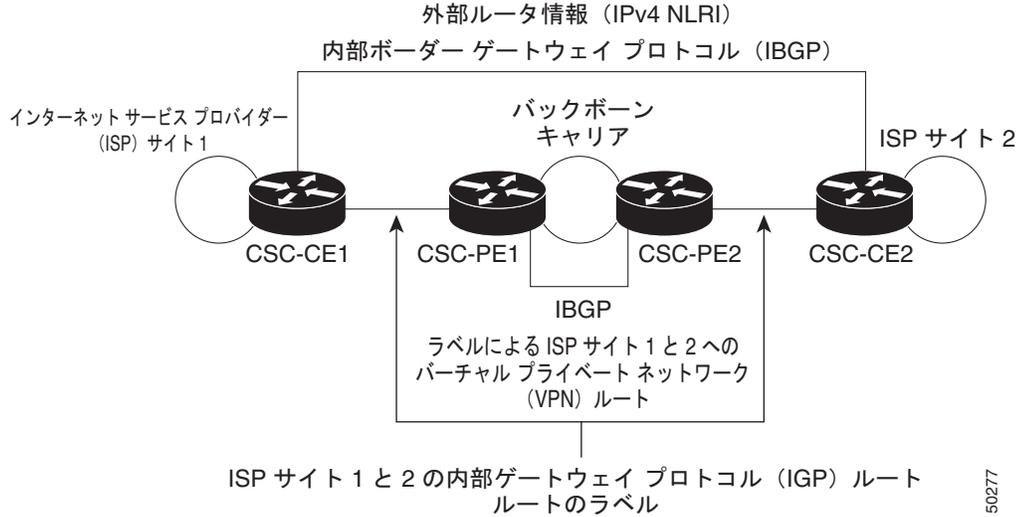
- 内部ルートは、ISP 内のいずれかのルータに進みます。
- 外部ルートはインターネットに進みます。

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

CSC-PE ルータは、VRF ルーティング テーブル内の外部ルートを伝送する必要がないため、パケット内の着信ラベルを使用して、カスタマー キャリアのインターネット トラフィックを転送できます。MPLS をルータに追加すると、カスタマー キャリアからバックボーン キャリアへの packet 転送を一貫した方法で行うことができます。MPLS により、CSC-PE ルータと CSC-CE ルータ間で、すべての内部カスタマー キャリア ルートの MPLS ラベルを交換できます。カスタマー キャリアのルータには、インターネットに接続するために、IBGP またはルート再配布のいずれかを経由するすべての外部ルートが含まれています。

図 5-23 に、ネットワークがこの方法で設定されている場合に、情報が交換される方法を示します。

図 5-23 バックボーン キャリアと、ISP であるカスタマー キャリアとの間のルーティング情報の交換



BGP/MPLS VPN サービス プロバイダーのカスタマー キャリアを持つバックボーン ネットワーク

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

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

図 5-24 には、カスタマー キャリアが MPLS VPN プロバイダーである Carrier Supporting Carrier ネットワーク設定が示されています。カスタマー キャリアには 2 つのサイトがあります。バックボーン キャリアおよびカスタマー キャリアは、MPLS を使用します。iBGP セッションは、ISP の外部ルーティング情報を交換します。

図 5-24 MPLS VPN プロバイダーであるカスタマー キャリアを含む Carrier Supporting Carrier ネットワーク

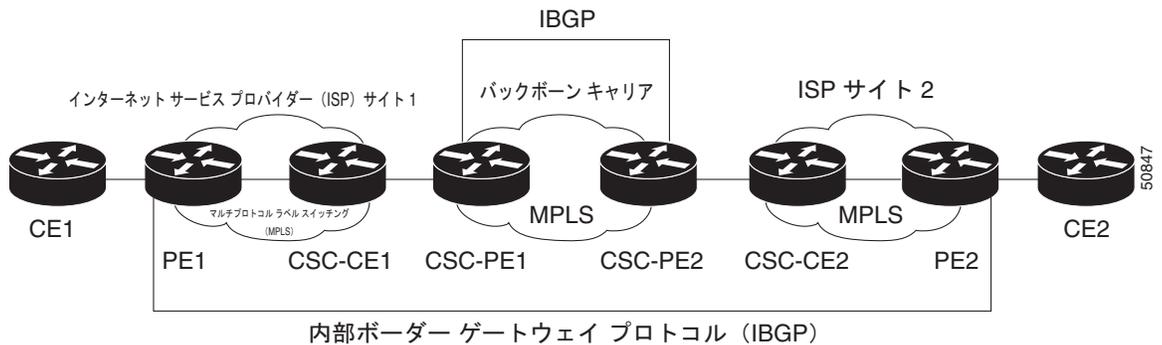
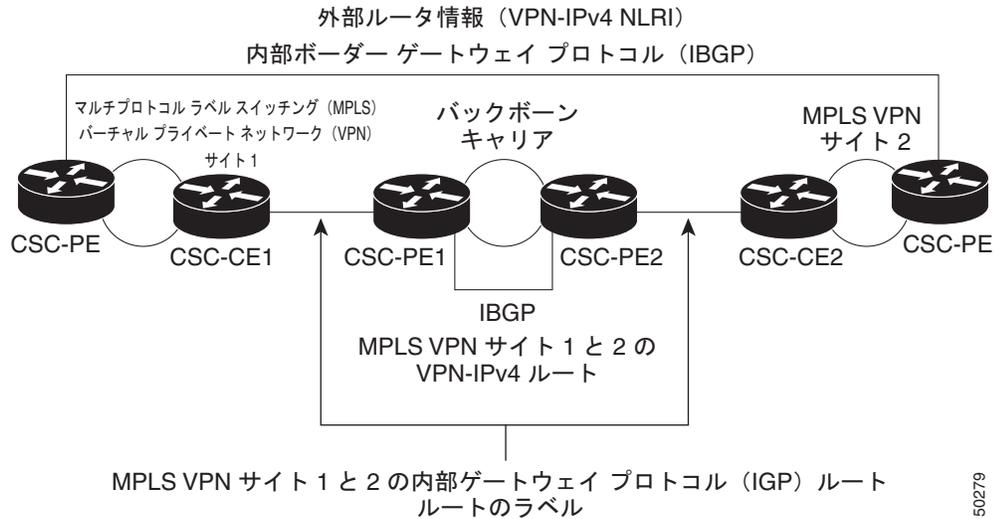


図 5-25 には、MPLS VPN サービス プロバイダーであるカスタマー キャリアと情報を交換するバックボーン キャリアが示されています。

図 5-25 バックボーン キャリアと、MPLS VPN サービス プロバイダーであるカスタマー キャリアとの間の情報の交換



Prime Provisioning 設定オプション

バックボーン キャリア プロバイダー エッジ (CSC-PE) ルータとカスタマー キャリア カスタマー エッジ (CSC-CE) ルータの間でルータを交換し、ラベルを伝送するように CSC ネットワークを設定するには、ラベル配布プロトコル (LDP) を使用してラベルと Interior Gateway Protocol (IGP) を伝送し、ルータを伝送します。

LDP/IGP

バックボーン キャリアをカスタマー キャリアに接続する CSC-PE ルータと CSC-CE ルータの間には、ルーティング プロトコルが必要です。ルーティング プロトコルにより、カスタマー キャリアは IGP ルーティング情報をバックボーン キャリアと交換できます。ルーティング プロトコルとして RIP、OSPF、またはスタティック ルーティングを選択できます。

バックボーン キャリアをカスタマー キャリアに接続する CSC-PE ルータと CSC-CE ルータ間でラベル配布プロトコル (LDP) が必要です。VPN ルーティング/転送 (VRF) 用の CSC-PE と CSC-CE の間のインターフェイスについても LDP が必要です。

IPv4 BGP ラベル配布

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 の代わりに使われます。BGP を使用して、ルートおよび MPLS ラベルを配布できます。2 つではなく単一のプロトコルを使用すると、設定およびトラブルシューティングが簡単になります。

BGP は、2 つの ISP を接続する場合の優先ルーティング プロトコルです。主な理由は、そのルーティング ポリシーと拡張性です。ISP では、通常、2 つのプロバイダー間で BGP を使用します。この機能を使用すると、これらの ISP は BGP を使用できます。

BGP (eBGP と iBGP の両方) 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。

CSC のサービス ポリシーの定義

CSC を使用してサービス ポリシーを定義するには、[MPLS Policy Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。

[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。

CSC サービス要求のプロビジョニング

CSC を使用してサービス要求をプロビジョニングするには、[MPLS Link Attribute Editor - Routing Information] で [CSC Support] チェックボックスをオンにします。

[CSC Support] をオンにすると、MPLS VPN サービスに対して CSC 機能がイネーブルになります。

複数のデバイスのプロビジョニング

この項では、Prime Provisioning のプロビジョニング処理を使用して、複数のデバイス、レイヤ 2 (L2) 「スイッチ」、およびレイヤ 3 (L3) 「ルータ」設定する方法を説明します。次の事項について説明します。

- 「NPC のリング トポロジ」 (P.5-150)
- 「Ethernet-To-The-Home (ETTH)」 (P.5-154)

NPC のリング トポロジ

この項では、Prime Provisioning のプロビジョニング処理を使用して、リング トポロジの作成、CE 開始ポイントと PE-POP 終了ポイントの接続、およびエンドツーエンドからの名前付き物理回線 (NPC) の設定についての各方法を説明します。

ここでは、次の項目について説明します。

- 「リング トポロジの概要」 (P.5-150)
- 「3 つの PE-CLE リングの作成」 (P.5-151)
- 「NPC のリング トポロジの設定」 (P.5-152)

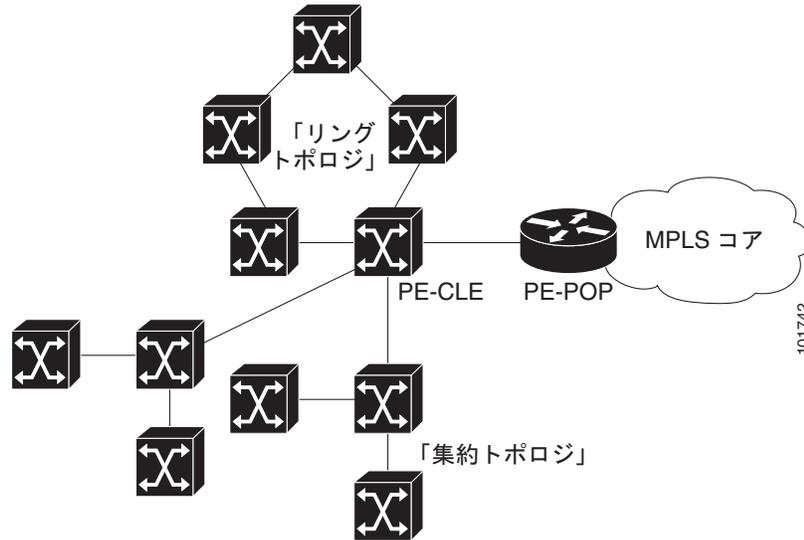
リング トポロジの概要

現在、サービス プロバイダーは、共通の MPLS インフラストラクチャと統合する必要のある L2 および L3 サービスを提供することに関心があります。Prime Provisioning は、L3 MPLS ネットワークにアクセスするための次の 2 つの基本的な L2 トポロジをサポートしています。

- リング トポロジ
- 集約トポロジ (「ハブ アンド スポーク」)

図 5-26 に、これら 2 つの基本的な L2 アクセス トポロジの例を示します。

図 5-26 L2 アクセス トポロジ

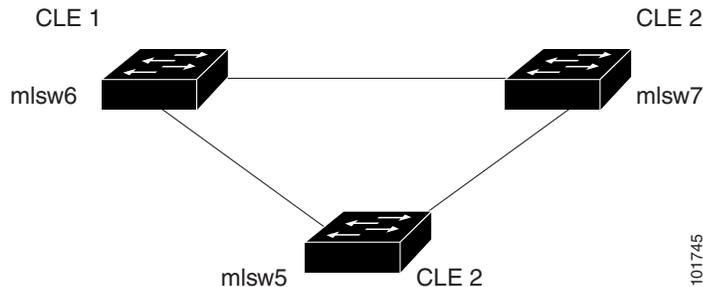


3 つの PE-CLE リングの作成

最も単純な形式では、リング トポロジは少なくとも 3 つの PE CLE を構成している 3 つに分かれた構造になります。また、PE-POP および Multi-VRF CE はリングの一部にすることができます。

図 5-27 には、3 つの Catalyst 3550 スイッチである mls w5、mls w6、および mls w7 のリングの例を示しています。

図 5-27 3 つの PE-CLE のリング



3 つの PE-CLE のリングを作成するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [Physical Rings] を選択します。
[Physical Rings] ウィンドウが表示されます。
- ステップ 2** 続行するには、[Create] をクリックします。
[Create Ring] ウィンドウが表示されます。
- ステップ 3** 最初のセルで [Select source device] をクリックします。
[Show Devices] ウィンドウが表示されます。



(注) [Show Devices] ドロップダウン ウィンドウには、*PE* ではなく *CLE* が表示されます。これは既知のアプリケーション エラーです。このプロセスは *PE-POP* または *CE* では開始できません。*PE-CLE* で開始する必要があります。

ステップ 4 特定の *CLE* を検索するには、ソース デバイスを [matching] ダイアログボックスに入力し、[Find] をクリックします。

ステップ 5 *CLE* を選択して [Select] をクリックします。

[Create Ring] ウィンドウが表示されます。

ステップ 6 独自の環境でのネットワーク ダイアグラムに基づいて、左から右、および上から下の方向でテーブル内に該当するデバイスとインターフェイスの情報を入力します。



(注) 図 5-28 でネットワーク ダイアグラムを使用して [Create Ring] テーブルにデータを取り込んだ場合、この処理の最後に上記の情報が含まれます。

ステップ 7 [Save] をクリックしてリングをリポジトリに保存します。

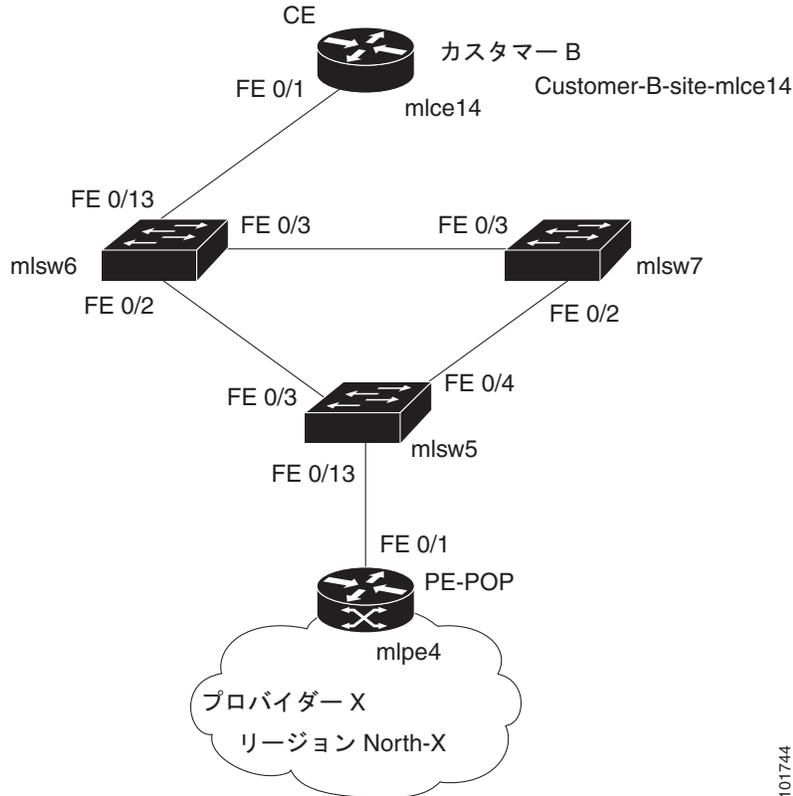
[NPC Rings] ウィンドウが表示されます。

「NPC のリング トポロジの設定」(P.5-152) に進みます。

NPC のリング トポロジの設定

図 5-28 には、*CE (mlce14)* と *PE-POP (mlpe4)* の間に挿入されたリング トポロジ (3 つの *CLE*) の例が示されています。

図 5-28 リングトポロジ



101744

エンドツーエンド接続 (CE > Ring (PE-CLE) > PE) を設定するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [Named Physical Circuits] を選択します。
[Named Physical Circuits] ウィンドウが表示されます。
- ステップ 2** [Create] をクリックします。
[Create Named Physical Circuit] ウィンドウが表示されます。
- ステップ 3** [Add Device] をクリックします。
[Select Devices] ウィンドウが表示されます。
- ステップ 4** CE を選択し、[Select] をクリックします。
[Create Named Physical Circuit] ウィンドウが表示されます。
- ステップ 5** [Add Device] をクリックします。
[Select Devices] ウィンドウが表示されます。
- ステップ 6** PE を選択し、[Select] をクリックします。
[Create Named Physical Circuit] ウィンドウが表示されます。
- ステップ 7** [Insert Ring] をクリックします。
[Show NPC Rings] ウィンドウが表示されます。
- ステップ 8** NPC のリングを選択し、[Select] をクリックします。
[Create a Named Physical Circuit] ウィンドウが表示されます。

- ステップ 9** 使用可能なチェックボックスでデバイスを選択し、[Select device] をクリックします。
[Select a device from ring] ウィンドウが表示されます。
- ステップ 10** PE-CLE を選択して、[Select] をクリックします。
[Create Named Physical Circuit] ウィンドウが表示されます。
- ステップ 11** 完了するまで、CE、CLE および PE の着信および発信インターフェイスを選択します。
- ステップ 12** 強調表示されたチェックボックスが付いた残りのデバイスを選択します。
[Create a Named Physical Circuit] ウィンドウが表示されます。
- ステップ 13** [Save] をクリックします。
[Named Physical Interfaces] ウィンドウが表示されます。
-

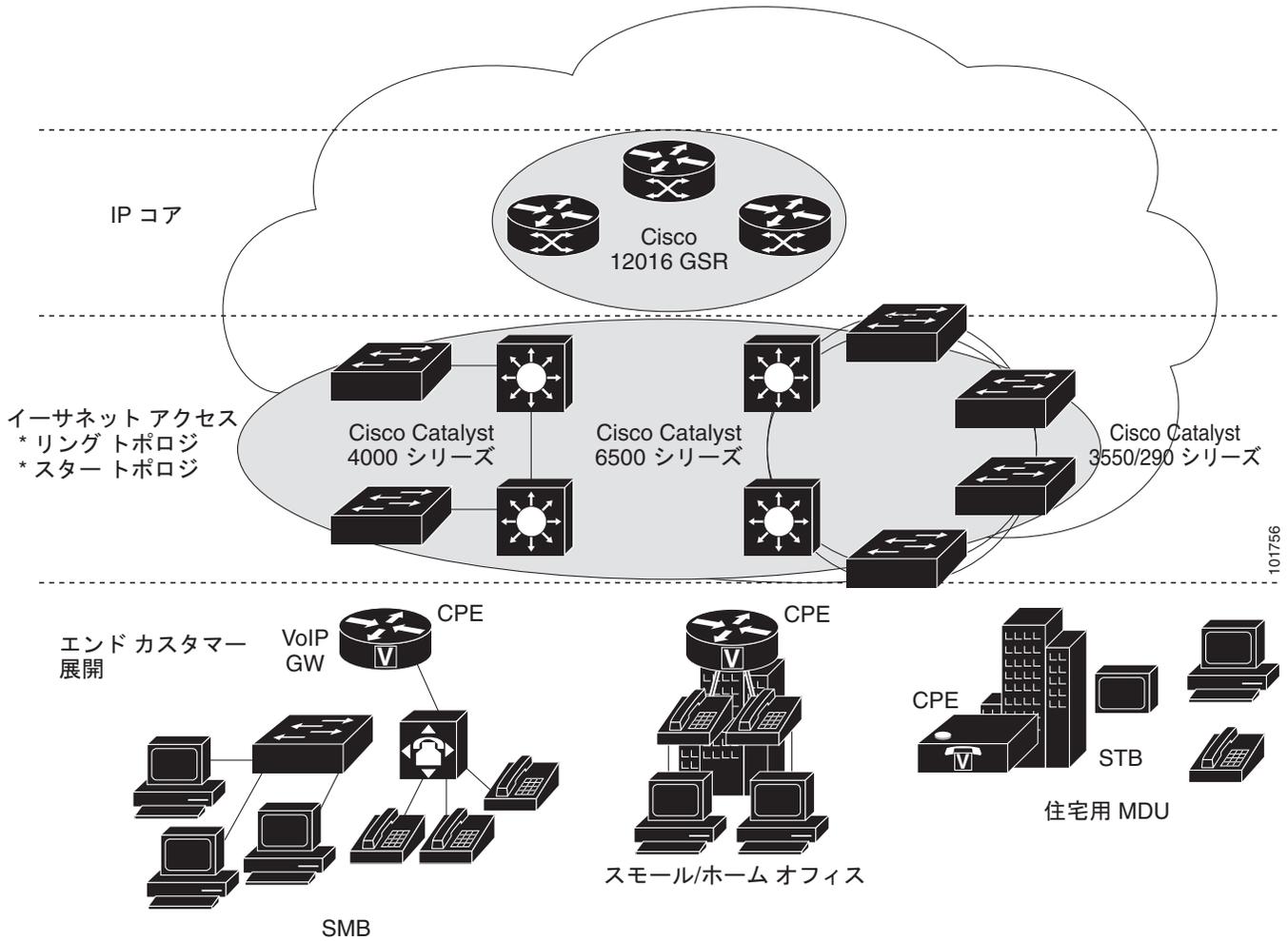
Ethernet-To-The-Home (ETTH)

この項では、Prime Provisioning プロビジョニング プロセスを使用して、Ethernet-To-The-Home (ETTH) を設定する方法を説明します。

ETTH は Cisco ETTx ソリューションの一部であり、これには ETTH と Ethernet-to-the-Business (ETTB) の両方が含まれています。ETTB は L2VPN メトロ イーサネット サービス機能を持つ Prime Provisioning でサポートされています。ユーザが主にビジネス ユーザである ETTB と異なり、ETTH は個人ユーザを対象にしています。

図 5-29 は Cisco ETTx ソリューションの概要を示しています。

図 5-29 Cisco ETTx ソリューション



プロビジョニングの観点から、ETTB と ETTH の主な相違点はソース拡張性の考慮事項です。たとえば、ETTB では、各ビジネス ユーザには 1 つ以上の VLAN が割り当てられます。

ETTH では、一意の VLAN を各個人カスタマーに割り当てることは現実的ではありません。現実的なソリューションは、すべての個人カスタマー、または個人カスタマーのグループが同じ VLAN を共有して Private VLAN (PVLAN; プライベート VLAN) や保護ポートなどの共通のテクノロジーを使用してトラフィックの分離を保障することです。

ETTB と ETTH のもう 1 つの違いは、ETTH カスタマーはアクセス ポートを使用する一方で、ETTB のカスタマーのほとんどはイーサネット トランク ポートを使用することです。Prime Provisioning では、アクセス ポートは CE の有無に関係なく完全にサポートされます。

ETTH はリングなどの共有メディアで、ビデオなどのマルチキャスト ベースのサービスをサポートする必要があります。通常、Multicast VLAN Registration (MVR) を使用するインターネット グループ管理プロトコル (IGMP) をテクノロジーとして使用して、次のサービスをサポートします。

アクセス ドメイン管理

アクセス ドメインの管理をより柔軟に行うために、管理 VLAN を定義できます。一度定義すると、すべての非 UNI ポートのトランク ポートで許可される VLAN のリストの作成に、管理 VLAN が使用されます。

リストがデバイスに存在しない場合、VLAN の許可リストがドメインのトランク ポートでどのように生成されるかを指定できます。この機能は、L2VPN DCPL パラメータに実装されます。これは、MPLS VPN へのレイヤ 2 アクセスにも使用可能です。

レイヤ 2 アクセス管理の一部として、Prime Provisioning では許可またはブロックする MAC アドレスを指定することにより、MAC アクセス リストの作成ができます。

Prime ProvisioningETTH 実装

Prime ProvisioningETTH の MPLS VPN の実装は次の 3 種類のサブ機能で構成されます。

- 「PVLAN または保護ポート」 (P.5-156)
- 「アクセス ポート」 (P.5-156)
- 「MVR を使用する IGMP」 (P.5-156)

PVLAN または保護ポート

この機能は PVLAN 内でトラフィックを分離するために使用されます。これにより、トラフィックが 2 つの UNI 間を流れないようにします。

- PVLAN は、Catalyst 4500/6500 スイッチおよび Cisco 7600 ルータでのみサポートされています。
- 保護ポートは、Catalyst 2950/3550 スイッチでのみサポートされます。

アクセス ポート

Prime Provisioning では、タグなしイーサネットのデフォルトは、CE ありおよび CE なしのシナリオでサポートされています。[DOT1Q] および [Default] の 2 つのカプセル化から選択できます。

デフォルトのカプセル化は CE から送信されるトラフィックがタグ付けされないことを示すのみです。常に dot1q ポートである UNI は、トラフィックを送信する前にタグを付けます。UNI には、このタグなしトラフィックを処理するためのオプションが 2 つあります。これは、アクセス ポートまたはトランク ポートとして機能します。このため、GUI によって 1 つ以上の項目が追加され、その中から選択できるようになります。

MVR を使用する IGMP

この機能は非常に特殊なユーザ サービスとネットワーク トポロジに適用されます。ハブアンドスポークまたはリング ネットワークのマルチキャスト ビデオに使用されます。ただし、それが使用される条件を Prime Provisioning が決定するわけではありません。Prime Provisioning はそれを使用できるようにするだけであり、Prime Provisioning で実行しているネットワーク アプリケーションは必要なときにそれを呼び出す必要があります。

ETTH ポリシーの作成

ETTH をサポートするようにポリシーを設定するには、次の手順を実行します。

-
- ステップ 1** [Service Design] > [Policies] > [Policy Manager] を選択します。
[Policy Manager] ウィンドウが表示されます。
- ステップ 2** [Policy Manager] ウィンドウで、サービス ポリシーを選択し、[Edit] をクリックします。
- ステップ 3** [Policy Type Information] ウィンドウで、[OK] をクリックします。
[MPLS Policy Editor - Interface] ウィンドウが表示されます。
- ステップ 4** ETTH をイネーブルにするには、[ETTH Support] チェックボックスをオンにします。
[ETTH UNI Information] チェックボックスが [ETTH Support] チェックボックスと [CE Information] の間に表示されます。
- ステップ 5** プライベート VLAN または保護ポートをイネーブルにするには、[Private VLAN/Protected Port] チェックボックスをオンにします。
- ステップ 6** MVR を使用する IGMP スヌーピングをイネーブルにするには、[IGMP Snooping with MVR] チェックボックスをオンにします。
3 つの新しい UNI の Information オプションが表示されます。
- ステップ 7** UNI 情報オプションを選択します。
- Mode
 - [Compatible] : マルチキャスト アドレスがデバイスにスタティックに設定されます。
 - [Dynamic] : IGMP スヌーピングがデバイスに設定されます。
 - [Query Time] : メンバーシップに対してデバイスが照会される頻度を決定します。
 - [Immediate] : セッション終了時にインターフェイスを転送テーブルからすぐに削除します。
- ステップ 8** 標準のステップを実行し、[Save] をクリックします。
-

ETTH のサービス要求の作成

ETTH のサービス要求を作成するには、次の手順を実行します。

-
- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
- ステップ 2** [Service Requests Manager] ウィンドウで、[Service Request] を選択してから、[Edit] をクリックします。
- ステップ 3** [MPLS Service Request Editor] ウィンドウで、[Link Attribute] リンクから [Edited] を選択します。
[MPLS Link Attribute Editor - Interface] ウィンドウが表示されます。
- ステップ 4** 次のリンク属性特有の UNI の情報の編集
- [Secondary VLAN ID] : プライベート VLAN の VLAN ID を入力します。Catalyst 4000 スイッチでのみサポートされています。
 - [Multicast IP Address] : [ステップ 5](#) を参照してください。
 - [Multicast VLAN ID] : マルチキャスト VLAN の [VLAN ID] を入力します。
- ステップ 5** [Edit] をクリックします。
[Multicast IP Addresses] ダイアログボックスが表示されます。
- ステップ 6** 次のリンク属性特有の UNI の情報の編集

- [Multicast IP Address] : マルチキャストグループに参加するための IP アドレスを入力します。これにより、ユーザはビデオ オン デマンドなどにアクセスできるようになります。
- [Counter] : マルチキャスト IP アドレスから開始する連続する数の IP アドレスを決定する番号を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 サービス要求を作成するための標準的な手順を実行し、[Save] をクリックします。



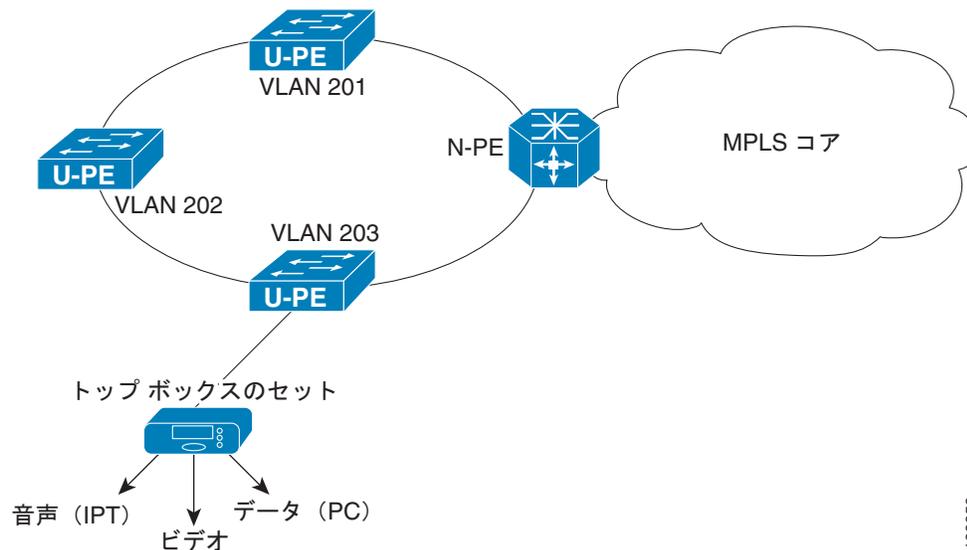
(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「[MPLS サービス要求での VRF および VPN 属性の定義](#)」(P.5-91) を参照してください。

[MPLS Service Requests] ウィンドウが再表示され、サービス要求が [Requested] 状態になり、展開可能になっていることが示されます。

個人用サービス

個人カスタマーのグループでは、異なる UNI インターフェイス上でトラフィックを分離する同じ UNI スイッチ上の同じ VLAN を共有できます。図 5-30 に示すように、N-PE では、同じ UNI スイッチからの個人用サービスすべてに対して VRF SVI が定義されます。

図 5-30 個人用サービス



138953

共有 VLAN を経由する個人用サービスのポリシーの作成

特殊なポリシーは共有 VLAN をイネーブルにして作成する必要があります。これを行うには、次の手順を実行します。

- ステップ 1** [Operate] > [Service Requests] > [Service Request Manager] を選択します。
[MPLS Policy Editor - Policy Type] ウィンドウが表示されます。
- ステップ 2** [Policy Name] フィールドに、ポリシー名を入力します。
- ステップ 3** [Policy Owner] で [Global Policy] オプション ボタンをクリックします。
- ステップ 4** [Policy Type] の下で、[Regular: PE-CE] を受け入れます。
- ステップ 5** [CE Present] でチェックボックスをオフにして、[Next] をクリックします。
[MPLS Policy Editor - Interface] ウィンドウが表示されます。
- ステップ 6** [Use SVI:] チェックボックスをオンにして、ウィンドウが更新されるまで待ちます。
- ステップ 7** [ETTH Support:] チェックボックスをオンにして、ウィンドウが更新されるまで待ちます。
- ステップ 8** [Standard UNI Port:] チェックボックスをオンにして、ウィンドウが更新されるまで待ちます。
- ステップ 9** [Shared VLAN:] チェックボックスをオンにして、ウィンドウが更新されるまで待ちます。この時点で、一部のフィールドはグレー表示されます。



(注) このポリシーによって [ETTH Support] と [Shared VLAN] がイネーブルになるため、これらの属性はリンク レベルでは使用できなくなります。

- ステップ 10** [Private VLAN/Protected Port:] チェックボックスをオンにして、ウィンドウが更新するまで待ち、[Next] をクリックします。
- ステップ 11** [IP Address Scheme] ウィンドウで、[Next] をクリックして続行できます。
- ステップ 12** [Routing Information] ウィンドウで、[Next] をクリックして続行できます。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

- ステップ 13** [VRF and VPN Member] ウィンドウで [Next] をクリックしてテンプレートを関連付けて続行するか、[Finish] をクリックしてこのポリシーの作成を完了できます。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

共有 VLAN を経由する個人用サービスのサービス要求を作成

サービス要求を作成するには、次の手順を実行します。

- ステップ 1** [Service Design] > [Policies] > [Policy Manager] > [MPLS Policy Editor - Policy Type] を選択します。
- ステップ 2** 共有 VLAN 個人用サービスに設定したポリシーを選択し、[OK] をクリックします。[MPLS Service Request Editor] ウィンドウが表示されます。
- ステップ 3** [MPLS Service Request Editor] ウィンドウで [Add Link] をクリックし、ウィンドウが更新されるのを待ちます。
- ステップ 4** アクティブなフィールド [Select U-PE] をクリックします。

■ 複数のデバイスのプロビジョニング

- ステップ 5** PE デバイスを選択し、[Select] をクリックします。
- ステップ 6** アクティブなインターフェイス選択機能からインターフェイスを選択し、ウィンドウが更新するまで待ちます。
- ステップ 7** [Link Attributes] 列で、アクティブな [Add] フィールドをクリックします。
[Interface Attributes] ウィンドウが表示されます。



(注) この機能用に作成されたポリシーによって [ETTH Support] と [Shared VLAN] がイネーブルになるため、これらの属性はリンク レベルでは使用できなくなります。

- ステップ 8** 有効な [VLAN ID] の値を入力して、[Next] をクリックします。[IP Address Scheme] ウィンドウが表示されます。
- ステップ 9** 各必須フィールドに有効な値を入力し、[Next] をクリックします。
- ステップ 10** [Routing Information] ウィンドウで該当する項目を選択し、[Next] をクリックします。



(注) プロトコル タイプについては、「サービスのルーティング プロトコルの指定」(P.5-51) を参照してください。

- ステップ 11** [VRF and VPN] ウィンドウの [Maximum Route Threshold] (必須フィールド) でデフォルト値を受け入れるか新しい値を入力します。



(注) 以前に定義された VRF オブジェクトから VRF および VPN の属性を設定する場合は、[Use VRF Object] チェックボックスをオンにします。この機能の詳細については、「独立 VRF 管理」(P.5-15) を参照してください。この項では、MPLS VPN サービス ポリシーとサービス要求で独立 VRF オブジェクトを使用する方法について説明します。



(注) MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」(P.5-91) を参照してください。

- ステップ 12** [VPN Selection] (必須) の下で、[Add] をクリックします。
- ステップ 13** CERC のウィンドウから目的の PE VPN メンバーシップを選択し、[Done] をクリックします。
- ステップ 14** [VRF and VPN] ウィンドウに戻り、[Finish] をクリックします。



(注) サービス要求がベースとして使用するポリシーで、テンプレートの関連付けがイネーブルになっている場合、GUI に [Next] ボタンが表示されます。テンプレートおよびデータ ファイルをサービス要求に定義されたデバイスに追加するには、[Next] ボタンをクリックします。テンプレートをサービス要求に関連付ける手順については、第 9 章「テンプレートおよびデータ ファイルの管理」を参照してください。

サービス ポリシーの属性の設定が完了したら、[MPLS Service Request Editor] ウィンドウが表示されます。

- ステップ 15** [Save] をクリックします。

[MPLS Service Requests] ウィンドウが再表示され、サービス要求が [Requested] 状態になり、展開可能になっていることが示されます。

複数の自律システムのスパニング

この項では、Prime Provisioning プロビジョニング プロセスを使用し、複数の自律システムのスパニングを設定する方法について説明します。

概要

MPLS VPN 機能の相互自律システムにより、MPLS VPN はサービス プロバイダーと自律システムにまたがることができます。自律システムとは、共通のシステム管理グループによって管理され、単一の明確に定義されたルーティング プロトコルを使用する、単一のネットワークまたはネットワークのグループのことです。

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

MPLS VPN 機能の相互自律システムは、自律システムとサービス プロバイダーのシームレスな統合を行います。異なるサービス プロバイダーの異なる自律システムは、VPN-IPv4 アドレスの形式で IPv4 ネットワーク層到達可能性情報 (NLRI) を交換することによって通信できます。自律システムのボーダー エッジ ルータはその情報を交換するために外部ボーダー ゲートウェイ プロトコル (eBGP) を使用します。その後、Interior Gateway Protocol (IGP) によって、各 VPN および各自律システム全体に、VPN-IPv4 プレフィックスのネットワーク層情報が配布されます。ルーティング情報では、次のプロトコルが使用されます。

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

相互自律システム サポートのある MPLS VPN により、サービス プロバイダーはカスタマーに Web ホスティング、アプリケーションのホスト、対話型の学習、e- コマース、およびテレフォニー サービスなど、スケーラブルなレイヤ 3 VPN サービスを提供することができます。VPN サービス プロバイダーは、1 つまたは複数の物理ネットワークでリソースを共有するセキュアな IP ベースのネットワークを提供します。

eBGP の主な機能は、自律システムのルー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。詳細については、「[自律システム間のルーティング](#)」(P.5-162) を参照してください。

MPLS VPN でサポートされている相互自律システム設定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、Interior Gateway Protocol (IGP) またはルーティング情報は交換されません。

- **BGP 連合**: 単一の自律システムを複数のサブ自律システムに分割してから、指定された単一の連合として分類した MPLS VPN。ネットワークでは、連合は単一の自律システムとして認識されず。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。

利点

相互自律システムの MPLS VPN 機能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

MPLS VPN 向け相互自律システム機能によって、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。相互自律システム機能によって、複数の自律システムでサービス プロバイダーのカスタマー サイト間に継続的 (かつシームレスな) 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

MPLS VPN 向け相互自律システム機能によって、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。

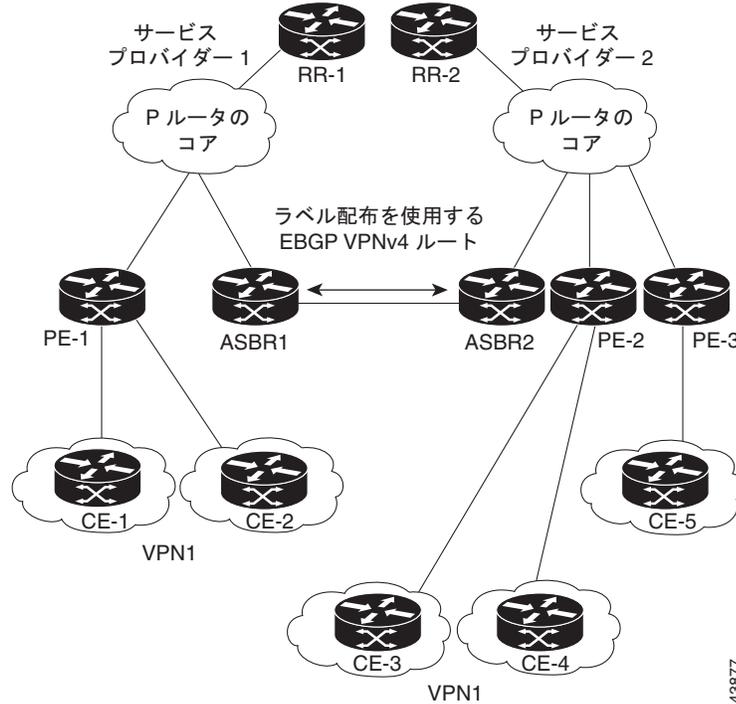
- IBGP メッシングを最適化するための連合が可能

相互自律システム機能は、自律システムの iBGP メッシュをより高度に編成して、管理できるようにします。自律システムを複数の異なるサブ自律システムに分割して、それらを単一の連合に分類できます (ただし、VPN バックボーン全体は単一の自律システムと見なされます)。連合を形成するサブ自律システム間でのラベル付き VPN-IPv4 ネットワーク層到達可能性情報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。

自律システム間のルーティング

図 5-31 に、2 つの異なる自律システムから構成された 1 つの MPLS VPN を示します。各自律システムは異なる管理制御下で運用され、異なる IGP が実行されています。サービス プロバイダーは、eBGP ボーダー エッジ ルータ (ASBR1 および ASBR2) を経由してルーティング情報を交換します。

図 5-31 2つの自律システム間のEBGP接続



この設定では、次のプロセスによって情報が送信されます。

1. プロバイダーエッジルータ (PE-1) では、ルートを配布する前に、そのルートに対してラベルが割り当てられます。PE ルータは、ボーダーゲートウェイプロトコル (BGP) のマルチプロトコル拡張を使用して、ラベルマッピング情報を送信します。PE ルータは、VPN-IPv4 アドレスとしてルートを配布します。アドレスラベルおよびVPN識別子は、NLRIの一部として符号化されます。
2. 2つのルートリフレクタ (RR-1 と RR-2) には、自律システム内のVPN-IPv4 内部ルートが反映されます。自律システムのボーダーエッジルータ (ASBR1 と ASBR2) は、VPN-IPv4 外部ルートをアドバタイズします。
3. EBGP ボーダーエッジルータ (ASBR1) によって、次の自律システム (ASBR2) にルートが再配布されます。ASBR1 は、EBGP のネクストホップ属性の値として自身のアドレスを指定し、新しいラベルを割り当てます。ASBR1 アドレスでは、次が保証されます。
 - ネクストホップルータが、サービスプロバイダー (P) バックボーンネットワーク内で常に到達可能であること。
 - 配布元ルータによって割り当てられたラベルが適切に解釈されること (ルータに関連付けられるラベルは、対応するネクストホップルータによって割り当てられる必要があります)。
4. eBGP ボーダーエッジルータ (ASBR2) では、設定に応じて、次のいずれかの方法でルートが再配布されます。
 - iBGP ネイバーが **neighbor next-hop-self** コマンドを使用して設定されている場合、ASBR2 は、eBGP ピアから受信したアップデートのネクストホップアドレスを変更して転送します。
 - iBGP ネイバーが **neighbor next-hop-self** コマンドを使用して設定されていない場合、ネクストホップアドレスは変更されません。ASBR2 は、eBGP ピアのホストルートを IGP 経路で伝播する必要があります。

図 5-33 に、自律システム間における VPN のルートおよびラベル情報の交換について示します。唯一の違いは、ASBR2 が **redistribute connected** コマンドを使用して設定されていることです。これにより、ホストルートがすべての PE に伝播されます。ASBR2 はネクストホップアドレスを変更するように設定されていないため、**redistribute connected** コマンドが必要となります。

図 5-33 2 つの自律システム間のすべての PE に伝播されるホストルート

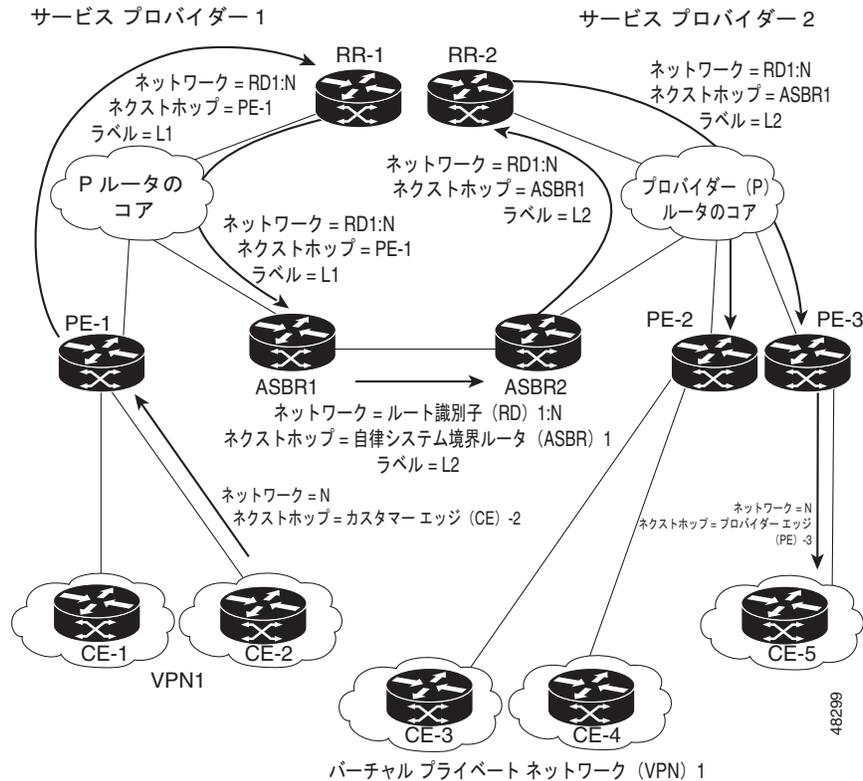


図 5-34 には、プロバイダー間ネットワークにおいて、次のパケット転送方法を使用して自律システム間でパケットが転送されるようすが示されています。

パケットは、MPLS によって宛先に転送されます。パケットでは、各 PE ルータおよび eBGP ボーダーエッジルータの LFIB に格納されているルーティング情報が使用されます。サービス プロバイダー VPN バックボーンはラベルを転送するために動的ラベルスイッチングを使用します。

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

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

- 最初のラベル (IGP ルートラベル) によって、パケットが正しい PE ルータまたは EBGP ボーダーエッジルータに転送されます (たとえば、ASBR2 の IGP ラベルは、ASBR2 ボーダーエッジルータを指します)。
- 2 番目のラベル (VPN ルートラベル) によって、パケットが適切な PE ルータまたは EBGP ボーダーエッジルータに転送されます。

図 5-34 2つの自律システム間のパケット転送

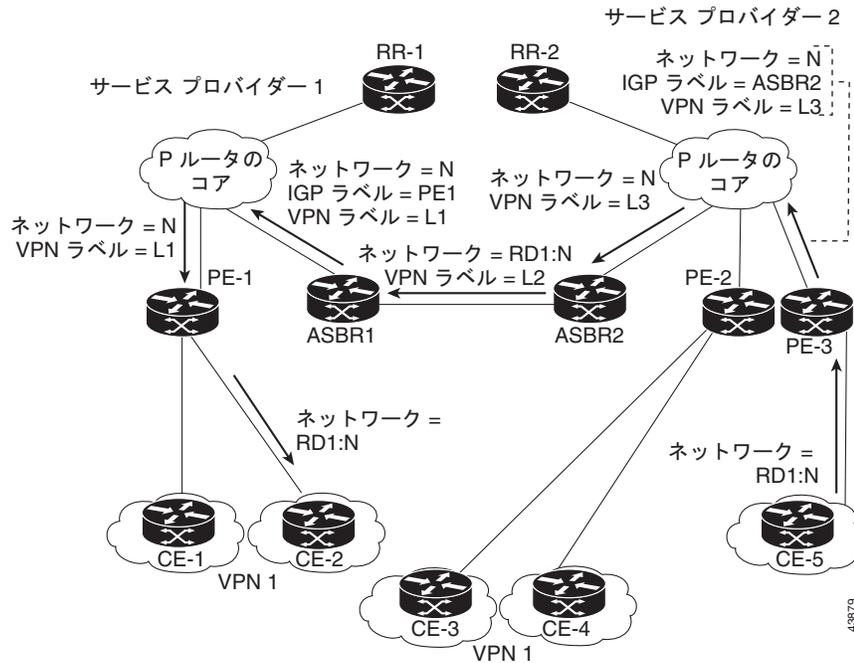
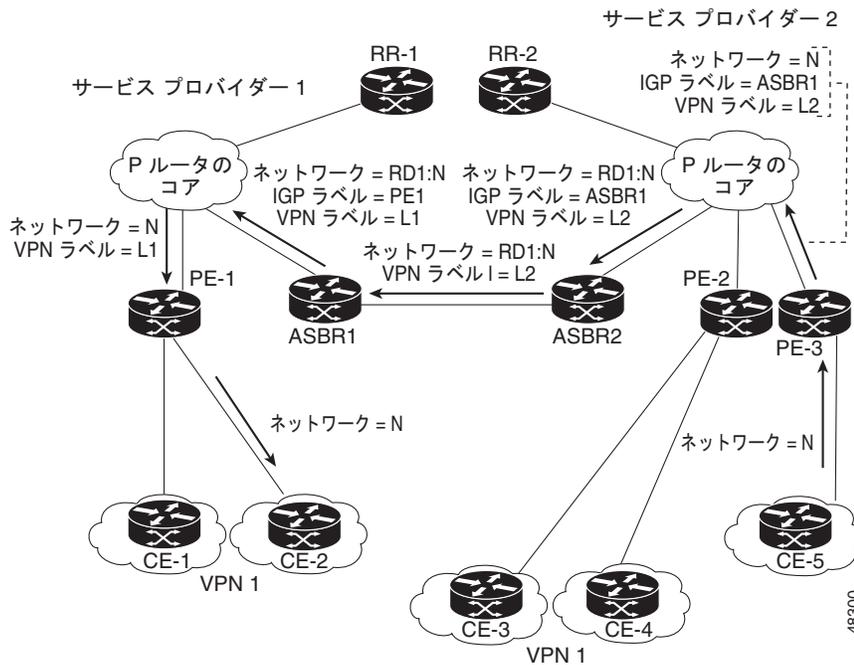


図 5-35 に、同じパケット転送方法を示します。ただし、今回は、eBGP ルータ (ASBR1) で新しいラベルが再割り当てされずにパケットが転送されます。

図 5-35 新しいラベルの再割り当てを行わないパケット転送



連合内のサブ自律システム間のルーティング

VPN は、異なる自律システムで実行するサービス プロバイダーまたは連合を形成するように一緒にグループ化された複数のサブ自律システム間に拡張できます。

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。

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。Confederation EBGP (CEBGP; 連合 EBGP) 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。

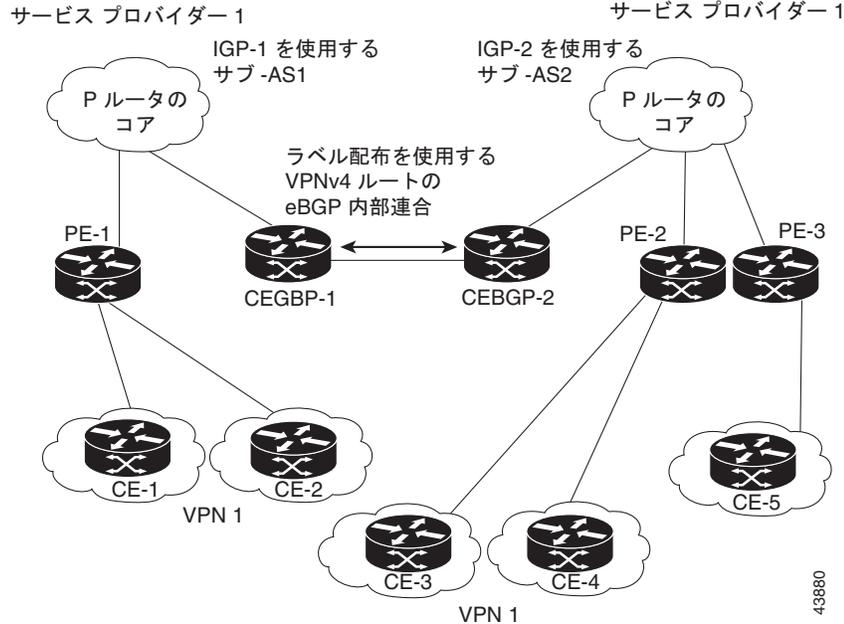
次の 2 つの方法で、異なるサブ自律システムに連合を設定できます。

- next-hop-self アドレスが CeGRP 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できます (双方向)。サブ自律システム ボーダーのサブ自律システム (iBGP ピア) では、next-hop-self アドレスは転送されません。各サブ自律システムは、単一の IGP ドメインとして実行されます。ただし、CEGRP 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せん。
- next-hop-self アドレスが CeGRP 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できます。各サブ自律システムは、単一の IGP ドメインとして実行されますが、ドメイン内の PE ルータ間で next-hop-self アドレスの転送もします。CEGRP 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 5-36 に、一般的な MPLS VPN 連合設定を示します。この連合設定の特徴は次のとおりです。

- 2 つの CEGRP ボーダー エッジルータは、2 つのサブ自律システム間でラベル付きの VPN-IPv4 アドレスを交換します。
- 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、CEGRP-1 と CEBGP-2 のアドレスが認識されます。

図 5-36 連合内の 2 つの AS 間の EGBP 接続



この連合設定の特徴は次のとおりです。

- CEGRP ボーダー エッジ ルータは、サブ自律システム間のネイバー ピアとして機能します。サブ自律システムは、EGRP を使用してルート情報を交換します。
- 各 CEGRP 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、ルートのラベルを割り当てます。CEGRP 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 CEGRP 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 アドレスプレフィックスに独自のラベルを割り当てます。CEGRP ボーダー エッジ ルータは、ラベル付きの VPN-IPv4 アドレスを交換します。

ラベルには、(EGRP 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、CeGRP 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 CeGRP ボーダー エッジ ルータが両方の連合で認識されます。

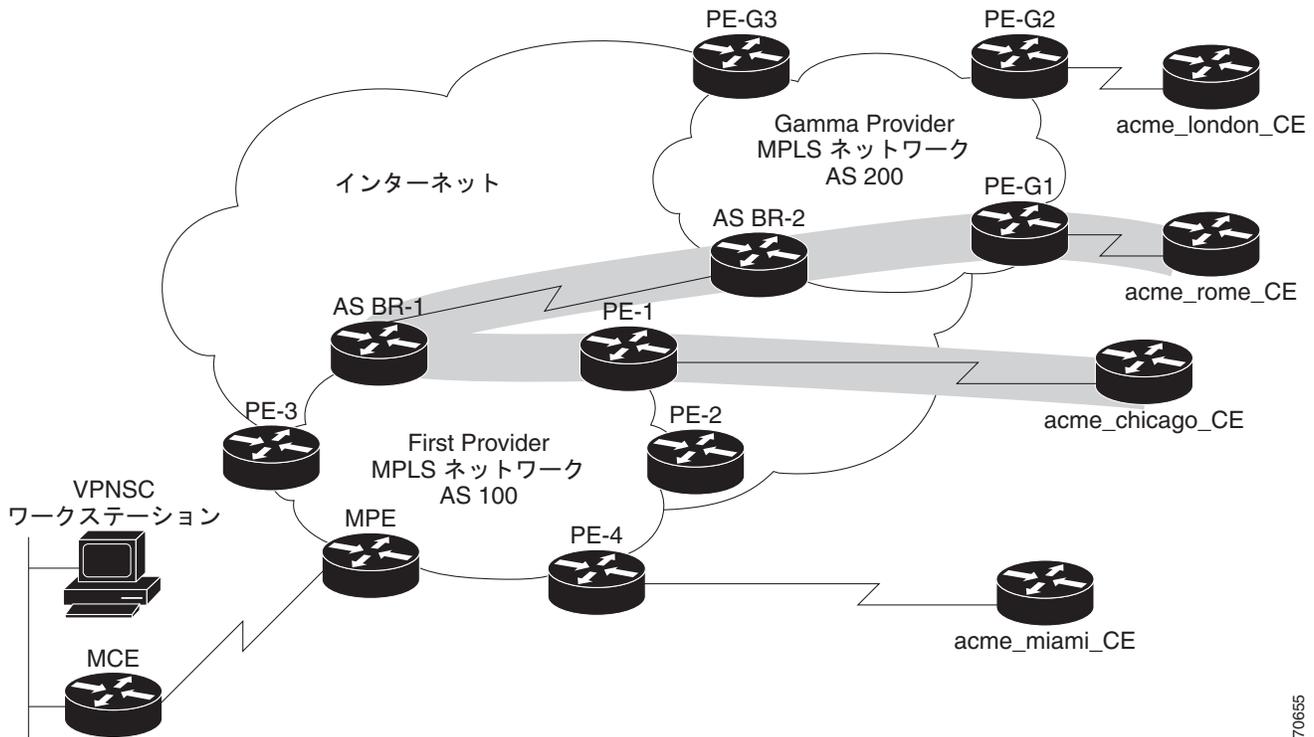
Prime Provisioning を使用した複数の自律システムのスパニング

「VPN ルーティング情報の交換」(P.5-164) に説明するように、自律システムは、接続を確立するために VPN ルーティング情報 (ルートとラベル) を交換します。自律システム間の接続を制御するために、PE ルータおよび外部 BGP Autonomous System Boundary Router (ASBR; 自律システム境界ルータ) がラベル転送情報ベース (LFIB) を保持します。LFIB では、VPN 情報の交換中に PE ルータおよび eGRP ボーダー エッジ ルータが受信するラベルとルートが管理されます。

ASBR は、iBGP ネイバーに VPN-IPv4 ネットワーク層到達可能性情報を送信する場合に、ネクストホップ (next-hop-self) を変更するように設定されています。したがって、ASBR では、iBGP ネイバーに NLRI を転送する場合に新しいラベルを割り当てる必要があります。

図 5-37 に、この項で使用する Prime Provisioning ネットワークの例を示します。

図 5-37 2 つの自律システムを持つ VPN ネットワークの例



AS 100 の Acme_Chicago から AS 200 の Acme_Rome に到達するためには、Prime Provisioning が次の 2 つのリンクのみをプロビジョニングする必要があります。

- Acme_Chicago と PE-1 間のリンク
- Acme_Rome と PE-G1 間のリンク

図 5-37 に示すように、Prime Provisioning は、PE-1 から ASBR-1 に、ASBR-1 から ASBR-2 に、さらに ASBR-2 から PE-G1 に VPN トラフィックをルーティングして、最終的にトラフィックはその宛先である Acme-Rome にルーティングされます。

ASBR-1 および ASBR-2 は Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) を実行する必要があります。その後、Interior Multiprotocol BGP (IMP-BGP; 内部マルチプロトコル BGP) によって、AS 100 の PE-1 と ASBR-1 間のルートおよび AS 200 の PE-2 と ASBR-2 間のルートが処理されます。Exterior Multiprotocol BGP (EMP-BGP; 外部マルチプロトコル BGP) では、ASBR-1 と ASBR-2 間のルートを処理します。

ヒント

サービスプロバイダーは、直接接続の Autonomous System Boundary Router (ASBR; 自律システム境界ルータ) 間の VPN-IPv4 EGRP セッションを設定する必要があります。これは、サービスプロバイダーが管理する必要があるワンタイム設定手順です。Prime Provisioning は、複数の自律システムに拡張された ASBR デバイス間のリンクはプロビジョニングしません。

VPN-IPv4 アドレス (IPNv4 アドレスとも呼ばれる) は、IPv4 アドレスと 8 バイトのルート識別子 (RD) の組み合わせです。RD と IPv4 アドレスを組み合わせることで、IPv4 ルートは MPLS VPN ネットワーク全体でグローバルに一意のルートになります。BGP では、同じネットワークとサブネットマスクを持つ IPv4 アドレスでもルート識別子が異なる場合は、IPv4 アドレスは異なると見なします。

相互自律システム ソリューションをサポートするためのテンプレートの使用

この項では、Prime Provisioning が Inter-Autonomous Systems (Inter-AS; 相互自律システム) およびプロバイダー間 VPN を Prime Provisioning テンプレートを介してどのようにサポートしているかを説明します。



(注) Prime Provisioning は、L2TPV3 ネットワークの Inter-AS 10B Hybrid モデルだけを現在サポートしています。Inter-AS 10B Hybrid モデルがこの項に記載されているソリューションです。

Inter-AS 10B Hybrid モデル

最新リリースの Prime Provisioning では、2 つのペアのテンプレート スクリプトが Inter-AS 10B Hybrid VPN のプロビジョニングおよびデコミッション用に提供されています。

- Autonomous System Border Router (ASBR; 自律システム ボーダー ルータ) 上の VPN-independent Inter-AS 10B Hybrid CLI のプロビジョニングおよびデコミッション
- ASBR 上の VPN-specific Inter-AS 10B Hybrid CLI のプロビジョニングおよびデコミッション

2 番目のテンプレート スクリプトのペアを使用すると、プロバイダーは ASBR 上に新しい Inter-AS VPN が追加された場合のプロビジョニングおよびデコミッション用に新しいペアのデータファイルを作成できます。Inter-AS 設定を変更する目的でスクリプトを作成または変更するためにデフォルト Inter-AS スクリプトを変更できます。

VPN-independent Inter-AS 10B Hybrid デフォルト テンプレートでは、次のコマンドがサポートされています。

- ASBR 上の L2TPV3 トンネルの Resolve In VRF (RIV) の VRF のプロビジョニング
- L2TPV3 トンネル設定
- ASBR-facing インターフェイス プロビジョニング
- BGP 設定
 - peer-group による BGP 設定
 - EBGP 設定
 - BGP address-family ipv4 設定
 - BGP address-family ipv4 tunnel 設定
 - BGP address-family vpnv4 設定
- L2TPV3 トンネル インターフェイスを通じたデフォルト ルート設定

VPN-specific Inter-AS 10B Hybrid デフォルト テンプレートでは、次のコマンドがサポートされています。

- カスタマー VPN の VRF プロビジョニング
- フル メッシュおよびハブ アンド スポーク VPN タイプ用の推奨/標準ルート ターゲット (RT) サポート。スポーク RT はオプションです。
- RT-rewrite 設定 :
 - 拡張コミュニティ (extcommunity-list) プロビジョニング
 - ルート マップ プロビジョニング

Inter-AS RT-Rewrite

Prime Provisioning は、ASBR 上の Inter-AS RT-rewrite 設定をサポートしています。RT-rewrite コマンドのプロビジョニングおよびデコミッション用の Velocity Template Language (VTL) テンプレート スクリプトは、次の項で説明する Inter-AS 10B Hybrid テンプレートの一部として提供されています。それぞれの使用例に対して独自のテンプレートを作成するために、VTL スクリプトを編集できます。

Inter-AS テンプレートの作成



(注)

Prime Provisioning でのテンプレートの作成および使用の詳細については、次を参照してください。
第 9 章「テンプレートおよびデータ ファイルの管理」

デフォルト Inter-AS テンプレートは、Prime Provisioning の Examples templates ディレクトリにあります。テンプレートは [Service Design] ウィンドウで作成します。このウィンドウにアクセスするには、次のように選択します。

[Service Design] > [Templates] > [Examples]

Inter-AS 10B Hybrid 用のテンプレートは次のとおりです。

- Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_
- Remove_PE_as_ASBR_non_VPN_Specific_Template_TMPL_
- Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_
- Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_

それぞれの使用例に基づいて、デフォルトのプロビジョニングおよびデコミッション スクリプトを使用してテンプレートを作成および変更できます。Inter-AS 設定のほとんどはワンタイム設定のため、テンプレートはデバイス コンソールからダウンロードされるだけでサービス要求には付加されません。

Prime Provisioning テンプレート機能では、テンプレート データ ファイルの展開に成功したかどうか、または展開に失敗したコマンドがあったかどうかを判断する基本的な展開チェックをサポートしています。また、ユーザ インターフェイスにおけるデータファイル作成中に正しい値の入力を容易にする、変数のデータタイプを選択できます。

Inter-AS CLI を含むテンプレート データ ファイルを正常に作成した後で、テンプレート データ ファイルを ASBR またはルート リフレクタに Prime Provisioning の [Device Console] ウィンドウを使用してダウンロードできます。このウィンドウにアクセスするには、次のように選択します。

[Service Inventory] > [Device Console]

[Service Design] で作成したテンプレートは、デバイスまたはデバイスグループで展開するために選択できます。



(注)

Prime Provisioning のテンプレート機能は、モデルベースではありません。このため、[Device Console] を使用してテンプレートをダウンロードした場合、テンプレート展開履歴またはスタックは保存されず、またテンプレートのロールバックおよびテンプレート CLI 監査はサポートされていません。PE ルータに特定の IBGP コマンドをダウンロードする必要がある場合は、サービス要求でテンプレートを選択してから PE ルータにダウンロードすることもできます。

サンプル コンフィグレット

この項では、Prime Provisioning での MPLS VPN プロビジョニングのサンプル コンフィグレットを紹介し、次の事項について説明します。

- 「概要」 (P.5-172)
- 「L3 MPLS VPN への L2 アクセス」 (P.5-174)
- 「CE-PE L3 MPLS VPN (フルメッシュの BGP)」 (P.5-176)
- 「CE-PE L3 MPLS VPN (BGP with SOO)」 (P.5-177)
- 「CE-PE L3 MPLS VPN」 (P.5-179)
- 「N-PE L3 MPLS VPN (IPv4、IOS XR、OSPF)」 (P.5-180)
- 「N-PE L3 MPLS VPN (IPv6、IOS XR、EIGRP)」 (P.5-184)
- 「PE L3 MPLS VPN (デュアル スタック、スタティック (IPv4)、BGP (IPv6)、IOS)」 (P.5-187)
- 「CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS)」 (P.5-189)
- 「CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS XR)」 (P.5-191)
- 「PE L3 MPLS VPN (マルチキャスト、IPv4 および IPv6 対応の VPN、IOS-XR)」 (P.5-199)
- 「PE L3 MPLS VPN (Static、IOS、IPv6)」 (P.5-204)
- 「PE L3 MPLS VPN (BGP、IOS)」 (P.5-205)
- 「PE L3 MPLS VPN (BGP、IOS、IPv6)」 (P.5-206)
- 「PE L3 MPLS VPN (BGP、IOS XR)」 (P.5-207)
- 「PE L3 MPLS VPN (BGP、RD フォーマット、IOS XR)」 (P.5-212)
- 「PE L3 MPLS VPN (BGP、Maximum Prefix/Restart、IOS XR)」 (P.5-214)
- 「PE L3 MPLS VPN (BGP、Default Information Originate、IOS XR)」 (P.5-219)
- 「PE L3 MPLS VPN (OSPF、IOS)」 (P.5-223)
- 「PE L3 MPLS VPN (OSPF、IOS XR)」 (P.5-224)
- 「L3 MPLS VPN (OSPF、Default Information Originate、IOS XR)」 (P.5-229)
- 「PE L3 MPLS VPN (EIGRP、Authentication Keychain Name、IOS XR)」 (P.5-234)
- 「PE L3 MPLS VPN (独立 VRF、IOS XR)」 (P.5-240)
- 「PE L3 MPLS VPN (IPv4 および IPv6 の独立 RT、IOS XR)」 (P.5-246)
- 「PE L3 MPLS VPN (Bundle-Ether Interface、IOS XR)」 (P.5-249)
- 「PE L3 MPLS VPN (Outgoing Interface + Next Hop IP Address、Static Route Configuration、IOS XR、および IOS)」 (P.5-251)

概要

この項で説明するコンフィグレットは、特定のサービスおよび機能向けに Prime Provisioning によって生成された CLI を示しています。各コンフィグレット例では、次の情報を提供します。

- サービス。
- 機能。

- デバイス設定（ネットワーク ロール、ハードウェア プラットフォーム、デバイスの関係、およびその他の関連情報）。
- 設定内の各デバイス用のサンプル コンフィグレット。
- コメント



(注) Prime Provisioning によって生成されるコンフィグレットは、プロビジョニングする必要のある要素と現在デバイス上に存在する要素の差分にすぎません。つまり、関連する CLI がすでにデバイス上に存在する場合、その CLI は関連コンフィグレットには示されません。



(注) この付録にあるすべての例は MPLS コアを前提としています。

コンフィグレットの表示方法については、「サービス要求コンフィグレットの表示」(P.8-5) を参照してください。

L3 MPLS VPN への L2 アクセス

設定

- サービス : L2VPN/メトロ イーサネット。
- 機能 : L3 MPLS VPN へのアクセス。
- デバイス設定 :
 - CE は、IOS 12.1(22)EA1 が動作する Cisco 3550。
インターフェイス : F0/13 <-> F0/4。
 - U-PE は、IOS 12.1(22)EA1 が動作する Cisco 3550。
インターフェイス : F0/14。
 - N-PE は IOS 12.2(18)SXF を備えた Cisco 7609。
インターフェイス : F2/8
 - VLAN = 3101。

コンフィグレット

CE	U-PE	N-PE
<pre>! vlan 3101 exit ! interface FastEthernet0/13 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3101 ! interface Vlan3101 description By VPNSC: Job Id# = 13 ip address 10.19.19.10 255.255.255.252 no shutdown</pre>	<pre>! vlan 3101 exit ! interface FastEthernet0/14 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3101 ! interface FastEthernet0/4 no keepalive no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 3101 switchport nonegotiate cdp enable no shutdown mac access-group ISC-FastEthernet0/4 in ! mac access-list extended ISC-FastEthernet0/4 deny any host 0100.0ccc.cccc deny any host 0100.0ccc.cccd deny any host 0100.0ccd.cdd0 deny any host 0180.c200.0000 permit any any</pre>	<pre>! ip vrf V5:VPN_sample rd 100:1502 route-target import 100:1602 route-target import 100:1603 route-target export 100:1602 maximum routes 100 80 ! interface FastEthernet2/8 no shutdown ! interface FastEthernet2/8.3101 description FastEthernet2/8.3101 dot1q vlan id=3101. By VPNSC: Job Id# = 13 encapsulation dot1Q 3101 ip vrf forwarding V5:VPN_sample ip address 10.19.19.9 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V5:VPN_sample redistribute connected redistribute static exit-address-family</pre>

コメント

- VPN リンクの Dot1q カプセル化を使用した IP 番号付きシナリオです。
- VRF は N-PE デバイスで作成されます。(s は、VRF がハブ アンド スポーク トポロジのスポークとして VPN に参加することを示します)。
- N-PE で、接続オプションと静的オプションのユーザ設定再配布を使用して、VRF が iBGP ルーティング インスタンスに追加されています。
- VRF は、U-PE 対向インターフェイスに関連付けられた転送を使用して NPE に作成されます。

CE-PE L3 MPLS VPN (フルメッシュの BGP)

設定

- サービス : L3 MPLS VPN
- 機能 : フルメッシュの CE-PE BGP。
- デバイス設定 :
 - PE は IOS 12.2(18)SXF を備えた Cisco 7609。
インターフェイス : F2/5
 - CE は、IOS 12.2(22)EA1 が動作する Cisco 3550。
インターフェイス : F0/13
 - ルーティングプロトコル = BGP

コンフィグレット

CE	PE
<pre> ! vlan 62 exit ! interface FastEthernet0/13 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 62 ! interface Vlan62 description By VPNSC: Job Id# = 29 ip address 10.19.19.42 255.255.255.252 no shutdown ! router bgp 10 neighbor 10.19.19.41 remote-as 100 </pre>	<pre> ! ip vrf V9:mpls_vpn1 rd 100:1506 route-target import 99:3204 route-target export 99:3204 maximum routes 100 80 ! interface FastEthernet2/5.62 description FastEthernet2/5.62 dot1q vlan id=62. By VPNSC: Job Id# = 29 encapsulation dot1q 62 ip vrf forwarding V9:mpls_vpn1 ip address 10.19.19.41 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V9:mpls_vpn1 neighbor 10.19.19.42 remote-as 100 neighbor 10.19.19.42 activate neighbor 10.19.19.42 allowas-in 2 redistribute connected redistribute static exit-address-family </pre>

コメント

- フルメッシュの設定は、VPN ポリシーに選択されている CERC によって作成されます。その結果、ルートターゲットのインポートとルートターゲットのエクスポートは同じです。
- BGP は CE-PE アクセスリンク上のルーティングプロトコルです。
- VPN リンクの dot1q カプセル化を使用した IP 番号付きシナリオです。
- VRF は PE デバイス上で作成されます。
- VRF は、CE 対向インターフェイスに関連付けられた転送を使用して PE に作成されます。

CE-PE L3 MPLS VPN (BGP with SOO)

設定

- サービス : L3 MPLS VPN
- 機能 : CE-PE。
- デバイス設定 :
 - PE は IOS 12.2(18)SXF を備えた Cisco 7609。
インターフェイス : FE2/3
 - Prime Provisioning に作成された CE。
インターフェイス : FE1/0/14
 - ルーティング プロトコル = BGP
 - VPN = ハブ。

コンフィグレット

CE	PE
<pre> ! vlan 3100 exit ! interface FastEthernet1/0/14 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3100 no shutdown ! interface Vlan3100 description By VPNSC: Job Id# = 12 ip address 10.19.19.6 255.255.255.252 no shutdown ! router ospf 3500 network 10.19.19.4 0.0.0.3 area 12345 </pre>	<pre> ! ip vrf V4:VPN_sample-s rd 100:1501 route-target import 100:1602 route-target export 100:1603 maximum routes 100 80 ! interface FastEthernet2/3.3100 description FastEthernet2/3.3100 dot1q vlan id=3100. By VPNSC: Job Id# = 12 encapsulation dot1Q 3100 ip vrf forwarding V4:VPN_sample-s ip address 10.19.19.5 255.255.255.252 no shutdown ! router ospf 2500 vrf V4:VPN_sample-s redistribute bgp 100 subnets network 10.19.19.4 0.0.0.3 area 12345 ! router bgp 100 address-family ipv4 vrf V4:VPN_sample-s redistribute connected redistribute ospf 2500 vrf V4:VPN_sample-s match internal external 1 external 2 redistribute static exit-address-family </pre>

コメント

- VPN リンクの dot1q カプセル化を使用した IP 番号付きシナリオです。
- VRF は PE デバイス上で作成されます (VPN はスポークとして参加しています)。
- PE で、接続オプションと静的オプションのユーザ設定再配布を使用して、VRF が iBGP ルーティング インスタンスに追加されています。
- VRF は、CE 対向インターフェイスに関連付けられた転送を使用して PE に作成されます。

- この例は、IOS デバイス用です。Site-of-Origin (SOO) は、IOS XR デバイスにもサポートされています。IOS XR デバイスの場合、結果のコンフィグレットは異なります。IOS XR デバイスの場合、SOO 用に生成されたコンフィグレットの形式は **site-of-origin 64512:500** です。

CE-PE L3 MPLS VPN

設定

- サービス : L3 MPLS VPN
- 機能 : CE-PE。
- デバイス設定 :
 - PE は、IOS 12.2(18) SXD7 を備えた Cisco 7603 です。
インターフェイス : FE2/25
 - CE は IOS 12.2(25)EY2 が動作する Cisco 3750ME-I5-M
インターフェイス : FE1/0/6
 - VPN = スポーク。

コンフィグレット

CE	PE
<pre>! vlan 890 exit ! interface FastEthernet1/0/6 no ip address switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 890 no shutdown ! interface Vlan890 description By VPNSC: Job Id# = 336 : SR Id# = 336 ip address 10.10.75.2 255.255.255.252 no shutdown ! router bgp 120 neighbor 10.10.75.1 remote-as 100 no auto-summary</pre>	<pre>! ip vrf V60:TestVPN-s rd 100:8069 route-target import 100:1891 route-target export 100:1892 ! interface FastEthernet2/25.890 description FastEthernet2/25.890 dot1q vlan id=890. By VPNSC: Job Id# = 336 : SR Id# = 336 encapsulation dot1Q 890 ip vrf forwarding V60:TestVPN-s ip address 10.10.75.1 255.255.255.252 no shutdown ! router bgp 100 no auto-summary address-family ipv4 vrf V60:TestVPN-s neighbor 10.10.75.2 remote-as 120 neighbor 10.10.75.2 activate neighbor 10.10.75.2 route-map SetSOO_V60:TestVPN-s_100:100 in exit-address-family ! route-map SetSOO_V60:TestVPN-s_100:100 permit 10 set extcommunity soo 100:100</pre>

コメント

- VPN リンクの dot1q カプセル化を使用した IP 番号付きシナリオです。
- VRF は PE デバイス上で作成されます。
- CE BGP AS ID が 120 に設定されているポリシーの結果として、neighbor 10.10.75.2 remote-as 120 が作成されます。
- VRF は、CE 対向インターフェイスに関連付けられた転送を使用して PE に作成されます。
- PE 上で、BGP は CE ネイバーのルートマップを定義します。
- 関連するルート マップはコミュニティ値 (Prime Provisioning に定義されている SOO プール値) である SOO に拡張コミュニティ属性を設定します。
- この例は、IOS デバイス用です。Site-of-Origin (SOO) は、IOS XR デバイスにもサポートされています。IOS XR デバイスの場合、結果のコンフィグレットは異なります。IOS XR デバイスの場合、SOO 用に生成されたコンフィグレットの形式は **site-of-origin 64512:500** です。

N-PE L3 MPLS VPN (IPv4、IOS XR、OSPF)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS XR を持つ IPv4。
- デバイス設定 :
 - N-PE は IOS XR が動作する Cisco 12000 ルータ。
 - ルーティング プロトコル = OSPF

コンフィグレット

N-PE

(次の拡張コード例を参照)

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <Delete>
    <Configuration Source="CurrentConfig">
      <InterfaceConfigurationTable>
        <InterfaceConfiguration>
          <Naming>
            <Name>GigabitEthernet0/1/1/1.856</Name>
            <Active>act</Active>
          </Naming>
          <Shutdown>true</Shutdown>
        </InterfaceConfiguration>
      </InterfaceConfigurationTable>
    </Configuration>
  </Delete>
  <Set>
    <Configuration Source="CurrentConfig">
      <VRFTable>
        <VRF>
          <Naming>
            <Name>ICICI_VPN_1</Name>
          </Naming>
          <AFI_SAFITable>
            <AFI_SAFI>
              <Naming>
                <AFI>IPv4</AFI>
                <SAFI>Unicast</SAFI>
              </Naming>
            </AFI_SAFI>
          </AFI_SAFITable>
          <BGP>
            <ImportRouteTargets>
              <RouteTargetTable>
                <RouteTarget>
                  <Naming>
                    <Type>AS</Type>
                    <AS>100</AS>
                    <ASIndex>1</ASIndex>
                  </Naming>
                  <True>true</True>
                </RouteTarget>
              </RouteTargetTable>
            </ImportRouteTargets>
            <ExportRouteTargets>
              <RouteTargetTable>
```

```

        <RouteTarget>
          <Naming>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>1</ASIndex>
          </Naming>
          <True>>true</True>
        </RouteTarget>
      </RouteTargetTable>
    </ExportRouteTargets>
  </BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <Name>GigabitEthernet0/1/1/1.856</Name>
      <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/1/1/1.856 dot1q vlan id=856. By VPNSC: Job Id# =
116</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
      <VLANIdentifier>
        <VlanType>VLANTypeDot1q</VlanType>
        <FirstTag>856</FirstTag>
      </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>ICICI_VPN_1</VRF>
    <IPV4Network>
      <Addresses>
        <Primary>
          <IPAddress>10.10.56.1</IPAddress>
          <Mask>255.255.255.252</Mask>
        </Primary>
      </Addresses>
    </IPV4Network>
  </InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>100</AS>
      </Naming>
    </FourByteAS>
    <VRFTable>
      <VRF>
        <Naming>
          <Name>ICICI_VPN_1</Name>
        </Naming>
        <VRFGlobal>
          <Exists>>true</Exists>
          <RouteDistinguisher>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>8064</ASIndex>
          </RouteDistinguisher>
          <VRFGlobalAFTable>
            <VRFGlobalAF>

```

```

    <Naming>
      <AF>IPv4Unicast</AF>
    </Naming>
    <Enabled>>true</Enabled>
    <Redistribution>
      <ConnectedRoutes/>
      <OSPFRouteTable>
        <OSPFRoutes>
          <Naming>
            <OSPFInstanceName>100</OSPFInstanceName>
          </Naming>
          <RedistType>21</RedistType>
          <DefaultMetric>20000</DefaultMetric>
        </OSPFRoutes>
      </OSPFRouteTable>
      <StaticRoutes/>
    </Redistribution>
  </VRFGlobalAF>
</VRFGlobalAFTable>
</VRFGlobal>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
<OSPF>
  <ProcessTable>
    <Process>
      <Naming>
        <InstanceName>100</InstanceName>
      </Naming>
      <Start>true</Start>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>ICICI_VPN_1</VRFName>
          </Naming>
          <VRFStart>true</VRFStart>
          <Redistribution>
            <RedistributeTable>
              <Redistribute>
                <Naming>
                  <ProtocolType>rip</ProtocolType>
                  <InstanceName>rip</InstanceName>
                </Naming>
                <Classful>>false</Classful>
              </Redistribute>
              <Redistribute>
                <Naming>
                  <ProtocolType>static</ProtocolType>
                  <InstanceName>static</InstanceName>
                </Naming>
                <Classful>>false</Classful>
              </Redistribute>
            </RedistributeTable>
          </Redistribution>
        </VRF>
      </VRFTable>
    </Process>
  </ProcessTable>
  <AreaTable>
    <Area>
      <Naming>
        <IntegerID>100</IntegerID>
      </Naming>
      <NameScopeTable>
        <NameScope>
          <Naming>

```

```
        <Interface>GigabitEthernet0/1/1/1.856</Interface>
      </Naming>
      <Running>true</Running>
    </NameScope>
  </NameScopeTable>
  <Running>true</Running>
</Area>
</AreaTable>
<DefaultInformation>
  <AlwaysAdvertise>true</AlwaysAdvertise>
</DefaultInformation>
</VRF>
</VRFTable>
</Process>
</ProcessTable>
</OSPF>
</Configuration>
</Set>
<Commit/>
</Request>
```

コメント

- IOS XR では、デバイス設定は XML 形式で指定します。
- XML スキーマに対して、IOS XR のバージョンが異なると別の XML コンフィグレットが生成されます。ただし、XML スキーマでの変更を除いて設定はほぼ同一です。
- 考慮すべきさまざまなケースがあります。たとえば、サービス要求がデコミッションまたは変更される場合、XML 設定も少し変化します。

N-PE L3 MPLS VPN (IPv6、IOS XR、EIGRP)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS XR 3.5.x. を実行する N-PE。
- デバイス設定 :
 - N-PE は IOS XR 3.5.x が動作する Cisco 12000 ルータ
 - ルーティング プロトコル = EIGRP。

コンフィグレット

N-PE

(次の拡張コード例を参照)

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
interface GigabitEthernet0/1/1/1.840

ipv6 address fec0:140:9834::/64

exit

</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <EIGRP>
      <ProcessTable>
        <Process>
          <Naming>
            <ASNumber>100</ASNumber>
          </Naming>
          <VRFTable>
            <VRF>
              <Naming>
                <VRFName>V10:ICICI_VPN</VRFName>
              </Naming>
              <VRF_AFTable>
                <VRF_AF>
                  <Naming>
                    <VRF_AFType>IPv4</VRF_AFType>
                  </Naming>
                  <AutoSummary/>
                </VRF_AF>
              </VRF_AFTable>
            </VRF>
          </VRFTable>
        </Process>
      </ProcessTable>
    </EIGRP>
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/1/1.840</Name>
          <Active>act</Active>
        </Naming>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
</Request>
```

```

        </Naming>
        <Shutdown>true</Shutdown>
    </InterfaceConfiguration>
</InterfaceConfigurationTable>
</Configuration>
</Delete>
<Set>
    <Configuration Source="CurrentConfig">
        <InterfaceConfigurationTable>
            <InterfaceConfiguration>
                <Naming>
                    <Name>GigabitEthernet0/1/1/1.840</Name>
                    <Active>act</Active>
                </Naming>
                <Description>GigabitEthernet0/1/1/1.840 dot1q vlan id=840. By VPNSC: Job Id# =
50</Description>
                <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
                <VLANSubConfiguration>
                    <VLANIdentifier>
                        <VlanType>VLANTypeDot1q</VlanType>
                        <FirstTag>840</FirstTag>
                    </VLANIdentifier>
                </VLANSubConfiguration>
                <VRF>V10:ICICI_VPN</VRF>
            </InterfaceConfiguration>
        </InterfaceConfigurationTable>
    </BGP>
    <AS>
        <Naming>
            <AS>0</AS>
        </Naming>
        <FourByteAS>
            <Naming>
                <AS>100</AS>
            </Naming>
            <VRFTable>
                <VRF>
                    <Naming>
                        <Name>V10:ICICI_VPN</Name>
                    </Naming>
                    <VRFGlobal>
                        <Exists>true</Exists>
                        <VRFGlobalAFTable>
                            <VRFGlobalAF>
                                <Naming>
                                    <AF>IPv6Unicast</AF>
                                </Naming>
                                <Enabled>true</Enabled>
                                <Redistribution>
                                    <EIGRPRouteTable>
                                        <EIGRPRoutes>
                                            <Naming>
                                                <EIGRPInstanceName>120</EIGRPInstanceName>
                                            </Naming>
                                        </EIGRPRoutes>
                                    </EIGRPRouteTable>
                                </Redistribution>
                            </VRFGlobalAF>
                        </VRFGlobalAFTable>
                    </VRFGlobal>
                </VRF>
            </VRFTable>
        </FourByteAS>
    </AS>

```

```

</BGP>
<EIGRP>
  <ProcessTable>
    <Process>
      <Naming>
        <ASNumber>100</ASNumber>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>V10:ICICI_VPN</VRFName>
          </Naming>
          <Enabled>true</Enabled>
          <VRF_AFTable>
            <VRF_AF>
              <Naming>
                <VRF_AFType>IPv4</VRF_AFType>
              </Naming>
              <Enabled>true</Enabled>
              <RedistributeTable>
                <Redistribute>
                  <Naming>
                    <Protocol>BGP</Protocol>
                    <SecondASNumber>100</SecondASNumber>
                  </Naming>
                  <PolicySpecified>>false</PolicySpecified>
                </Redistribute>
              </RedistributeTable>
            </VRF_AF>
            <DefaultMetric>
              <BW>2000</BW>
              <Delay>2001</Delay>
              <Reliability>200</Reliability>
              <Load>201</Load>
              <MTU>20000</MTU>
            </DefaultMetric>
            <InterfaceTable>
              <Interface>
                <Naming>
                  <InterfaceName>GigabitEthernet0/1/1/1.840</InterfaceName>
                </Naming>
                <Enabled>true</Enabled>
              </Interface>
            </InterfaceTable>
            <AutonomousSystem>120</AutonomousSystem>
          </VRF_AF>
        </VRF_AFTable>
      </VRF>
    </VRFTable>
  </Process>
</ProcessTable>
</EIGRP>
</Configuration>
</Set>
<Commit/>
</Request><Comments

```

- IOS XR では、デバイス設定は XML 形式で指定します。
- XML スキーマに対して、IOS XR のバージョンが異なると別の XML コンフィグレットが生成されます。ただし、XML スキーマでの変更を除いて設定はほぼ同一です。
- 考慮すべきさまざまなケースがあります。たとえば、サービス要求がデコミッションまたは変更される場合、XML 設定も少し変化します。

PE L3 MPLS VPN (デュアルスタック、スタティック (IPv4)、BGP (IPv6)、IOS)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS デバイス上の、VPN ルーティング プロトコルがスタティックおよび BGP (デュアルスタック) に設定された MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS バージョン 12.2(33) SRD2 を実行しています。
インターフェイス : GigabitEthernet2/3.345
 - ルーティング プロトコル = スタティック (IPv4)、BGP (IPv6)。

コンフィグレット

PE

(次の拡張コード例を参照)

```

!
vrf definition UP-Tony-1
rd 1:45
address-family ipv4
route-target import 64512:73647
route-target import 64512:73648
route-target export 64512:73647
mdt default 225.4.4.1
mdt data 225.4.4.2 0.0.0.0 threshold 2343
mdt mtu 2345
address-family ipv6
route-target import 64512:73647
route-target import 64512:73648
route-target export 64512:73647
!
interface GigabitEthernet2/3.345
description GigabitEthernet2/3.345 dot1q vlan id=345. By VPNSC: Job Id# = 42
encapsulation dot1q 345
vrf forwarding UP-Tony-1
ip address 44.5.5.5 255.255.255.0
ipv6 address 53:33::3/60
ip pim sparse-dense-mode
mpls label protocol ldp
mpls ip
no shutdown
!
ip multicast vrf UP-Tony-1 route-limit 12343
!
ip multicast-routing vrf UP-Tony-1
!
ip pim vrf UP-Tony-1 autorp listener
!
ip pim vrf UP-Tony-1 rp-address 4.3.3.4 list132 override
!
router bgp 64512
address-family ipv4 vrf UP-Tony-1
default-information originate
redistribute connected

```

```
redistribute static
exit-address-family
address-family ipv6 vrf UP-Tony-1
neighbor 535::2 remote-as 35
neighbor 535::2 activate
neighbor 535::2 as-override
neighbor 535::2 allowas-in 1
neighbor 535::2 send-community both
neighbor 535::2 advertisement-interval 34
neighbor 535::2 maximum-prefix 455 23 restart 2345
redistribute connected
redistribute static
exit-address-family
!
ip route vrf UP-Tony-1 34.5.3.3 255.255.255.255 GigabitEthernet2/3.345 4.5.3.2 234
!
ip route vrf UP-Tony-1 44.3.4.4 255.255.255.255 GigabitEthernet2/3.345 4.5.3.2 23
```

コメント

- なし

CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS)

設定

- サービス : L3 MPLS VPN
- 機能 : CE-PE。Q-in-Q (2 つめの VLAN ID) が PE に設定されています。
- デバイス設定 :
 - N-PE は、IOS 12.2(33)SRC が動作し、ES20 ラインカードを搭載した Cisco 7606-S インターフェイス : GE2/0/15。
 - CE は Cisco 2811。
インターフェイス : FE0/0
 - VPN = スポーク。

コンフィグレット

CE	N-PE
<pre>! interface FastEthernet0/0.158 description FastEthernet0/0.158 dot1q vlan id=158. By VPNSC: Job Id# = 239 encapsulation dot1Q 158 ip address 10.1.1.98 255.255.255.252 no shutdown ! ip route 0.0.0.0 0.0.0.0 FastEthernet0/0.158</pre>	<pre>! ip vrf V15:MPLS-1 rd 100:6812 route-target import 100:7000 route-target import 100:7001 route-target export 100:7000 ! interface GigabitEthernet2/0/15.158 description GigabitEthernet2/0/15.158 dot1q vlan id=158. By VPNSC: Job Id# = 239 encapsulation dot1Q 158 second-dot1q 1502 ip vrf forwarding V15:MPLS-1 ip address 10.1.1.97 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V15:MPLS-1 redistribute connected redistribute static exit-address-family</pre>

コメント

- カプセル化は dot1q とし、SVI をディセーブルにする必要があります。
- 結果の CLI コンフィギュレーション コマンドは次のとおりです。


```
encapsulation dot1Q <VID-1> second-dot1q <VID-2>
```

 - *VID-1* は Prime Provisioning VLAN ID リソース プールまたは手動で割り当てることができません。
 - *VID-2* を手動で追加する必要があります。2 つめの VLAN ID に対する自動選択 ID のサポートはありません。
- コマンドをサポートする Platforms/IOS のバージョンが含まれますが、これに限定されるわけではありません。
 - ES-20、SIP400 + 2、および 5-port GE-V2 SPA を備えた Cisco 7600/SRBx。

- ES-20、SIP400 + 2、5-port GE-V2 SPA、および 10GE-V2 SPA を備えた Cisco 7600/SRCx。
- IOS 12.4 メインラインが動作する Cisco 7200 NPE-G1
- IOS 12.4(4)XD を備えた Cisco 7200 NPE-G2。
- Q-in-Q は IOS XR デバイスでもサポートされています。
- 2 つめの VLAN ID である *Second_PE_Vlan_ID* のテンプレート型変数があります。
- サポートされるネットワーク設定は次のとおりです。
 - PE のみ。
 - 管理対象および管理対象外 CE の PE-CE。



(注) CE が管理対象か管理対象外かに関係なく、Q-in-Q/2 つめの VLAN ID は PE にのみ設定されます。

Prime Provisioning での Q-in-Q サポートの詳細については、「[MPLS VPN PE-CE サービス要求の作成](#)」(P.5-86) の項の 2 つめの VLAN ID 属性のカバレッジを参照してください。

CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : CE-PE。Q-in-Q (2 つめの VLAN ID) が PE に設定されています。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.8.1 または 3.9.0 を備えた Cisco GSR 12008 です。
 - インターフェイス : TenGigE0/0/0/0。

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```
vrf V3:Vpn-Apr-30
  address-family ipv4 unicast
    import route-target
      64512:9688
      64512:9689
    !
    export route-target
      64512:9688
    !
  !
  address-family ipv6 unicast
    import route-target
      64512:9688
      64512:9689
    !
    export route-target
      64512:9688
    !
  !
interface TenGigE0/0/0/0.1825
  description TenGigE0/0/0/0.1825 dot1q vlan id=1825. By VPNSC: Job Id# = 29
  vrf V3:Vpn-Apr-30
  ipv4 address 6.8.14.15 255.255.255.0
  ipv6 address 18::219/64
  dot1q vlan 1825 869
!
router bgp 64512
  vrf V3:Vpn-Apr-30
  rd 64512:9864
  address-family ipv4 unicast
    redistribute static
  !
  address-family ipv6 unicast
    redistribute static
  !
```

```

!
!
end

```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```

vrf V3:Vpn-Apr-30
  address-family ipv4 unicast
    import route-target
      64512:9688
      64512:9689
    !
    export route-target
      64512:9688
    !
  !
  address-family ipv6 unicast
    import route-target
      64512:9688
      64512:9689
    !
    export route-target
      64512:9688
  !
!
!
interface GigabitEthernet0/3/0/1.488
  description GigabitEthernet0/3/0/1.488 dot1q vlan id=488. By VPNSC: Job Id# = 30
  vrf V3:Vpn-Apr-30
  ipv4 address 25.14.12.4 255.255.255.0
  ipv6 address 98::16/64
  dot1q vlan 488 758
!
router bgp 64512
  address-family vpv4 unicast
  !
  address-family vpv6 unicast
  !
  vrf V3:Vpn-Apr-30
    rd 64512:9864
    address-family ipv4 unicast
      redistribute static
    !
    address-family ipv6 unicast
      redistribute static
  !
!
!
end

```

XML コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V3:Vpn-Apr-30
address-family ipv6 unicast
import route-target 64512:9688
import route-target 64512:9689
export route-target 64512:9688
exit

```

```

interface TenGigE0/0/0/0.1825
ipv6 address 18::219/64
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>TenGigE0/0/0/0.1825</Name>
          <Active>act</Active>
        </Naming>
        <Shutdown>>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>V3:Vpn-Apr-30</Name>
        </Naming>
        <Create>>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
              <Topology>default</Topology>
            </Naming>
            <Create>>true</Create>
          <BGP>
            <ImportRouteTargets>
              <RouteTargetTable>
                <RouteTarget>
                  <Naming>
                    <Type>AS</Type>
                    <AS>64512</AS>
                    <ASIndex>9688</ASIndex>
                  </Naming>
                  <True>>true</True>
                </RouteTarget>
                <RouteTarget>
                  <Naming>
                    <Type>AS</Type>
                    <AS>64512</AS>
                    <ASIndex>9689</ASIndex>
                  </Naming>
                  <True>>true</True>
                </RouteTarget>
              </RouteTargetTable>
            </ImportRouteTargets>
            <ExportRouteTargets>
              <RouteTargetTable>
                <RouteTarget>
                  <Naming>
                    <Type>AS</Type>
                    <AS>64512</AS>
                    <ASIndex>9688</ASIndex>
                  </Naming>
                  <True>>true</True>
                </RouteTarget>
              </RouteTargetTable>
            </ExportRouteTargets>
          </BGP>
        </AFI_SAFI>
      </VRF>
    </VRFTable>
  </Configuration>
</Set>

```

```

        </RouteTargetTable>
    </ExportRouteTargets>
</BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
    <InterfaceConfiguration>
        <Naming>
            <Name>TenGigE0/0/0/0.1825</Name>
            <Active>act</Active>
        </Naming>
        <Description>TenGigE0/0/0/0.1825 dot1q vlan id=1825. By VPNSC: Job Id# =
29</Description>
        <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
        <VLANSubConfiguration>
            <VLANIdentifier>
                <VlanType>VLANTypeDot1q</VlanType>
                <FirstTag>1825</FirstTag>
                <SecondTag>869</SecondTag>
            </VLANIdentifier>
        </VLANSubConfiguration>
        <VRF>V3:Vpn-Apr-30</VRF>
        <IPV4Network>
            <Addresses>
                <Primary>
                    <IPAddress>6.8.14.15</IPAddress>
                    <Mask>255.255.255.0</Mask>
                </Primary>
            </Addresses>
        </IPV4Network>
    </InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
    <AS>
        <Naming>
            <AS>0</AS>
        </Naming>
        <FourByteAS>
            <Naming>
                <AS>64512</AS>
            </Naming>
        <VRFTable>
            <VRF>
                <Naming>
                    <Name>V3:Vpn-Apr-30</Name>
                </Naming>
                <VRFGlobal>
                    <Exists>true</Exists>
                    <RouteDistinguisher>
                        <Type>AS</Type>
                        <AS>64512</AS>
                        <ASIndex>9864</ASIndex>
                    </RouteDistinguisher>
                    <VRFGlobalAFTable>
                        <VRFGlobalAF>
                            <Naming>
                                <AF>IPv4Unicast</AF>
                            </Naming>
                            <Enabled>true</Enabled>
                            <StaticRoutes/>
                        </VRFGlobalAF>
                    </VRFGlobalAFTable>
                </VRF>
            </VRFTable>
        </AS>
    </BGP>

```

```

        <VRFGlobalAFTable>
        <VRFGlobalAF>
        <Naming>
        <AF>IPv6Unicast</AF>
        </Naming>
        <Enabled>>true</Enabled>
        <StaticRoutes/>
        </VRFGlobalAF>
    </VRFGlobalAFTable>
</VRFGlobal>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>

```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V3:Vpn-Apr-30
address-family ipv6 unicast
import route-target 64512:9688
import route-target 64512:9689
export route-target 64512:9688
exit
interface GigabitEthernet0/3/0/1.488
ipv6 address 98::16/64
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <InterfaceName>GigabitEthernet0/3/0/1.488</InterfaceName>
          <Active>act</Active>
        </Naming>
        <Shutdown>>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <VRFName>V3:Vpn-Apr-30</VRFName>
        </Naming>
        <Create>true</Create>
        <AFTable>
          <AF>
            <Naming>
              <AFName>IPv4</AFName>
              <SAFName>Unicast</SAFName>
              <TopologyName>default</TopologyName>
            </Naming>

```

```

<Create>>true</Create>
<BGP>
  <ImportRouteTargets>
    <RouteTargetTable>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>9688</ASIndex>
        </Naming>
        <Enable>>true</Enable>
      </RouteTarget>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>9689</ASIndex>
        </Naming>
        <Enable>>true</Enable>
      </RouteTarget>
    </RouteTargetTable>
  </ImportRouteTargets>
  <ExportRouteTargets>
    <RouteTargetTable>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>9688</ASIndex>
        </Naming>
        <Enable>>true</Enable>
      </RouteTarget>
    </RouteTargetTable>
  </ExportRouteTargets>
</BGP>
</AF>
</AFTable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <InterfaceName>GigabitEthernet0/3/0/1.488</InterfaceName>
      <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/3/0/1.488 dot1q vlan id=488. By VPNSC: Job Id# =
30</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
      <VLANIdentifier>
        <VlanType>VLANTypeDot1q</VlanType>
        <FirstTag>488</FirstTag>
        <SecondTag>758</SecondTag>
      </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>V3:Vpn-Apr-30</VRF>
    <IPV4Network>
      <Addresses>
        <Primary>
          <Address>25.14.12.4</Address>
          <Netmask>255.255.255.0</Netmask>

```

```

        </Primary>
    </Addresses>
</IPv4Network>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>64512</AS>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>V3:Vpn-Apr-30</VRFName>
          </Naming>
          <VRFGlobal>
            <Exists>true</Exists>
            <RouteDistinguisher>
              <Type>AS</Type>
              <AS_XX>0</AS_XX>
              <AS>64512</AS>
              <ASIndex>9864</ASIndex>
            </RouteDistinguisher>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AFName>IPv4Unicast</AFName>
                </Naming>
                <Enable>true</Enable>
                <StaticRoutes/>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AFName>IPv6Unicast</AFName>
                </Naming>
                <Enable>true</Enable>
                <StaticRoutes/>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
          </VRFGlobal>
        </VRF>
      </VRFTable>
    </DefaultVRF>
    <Global>
      <GlobalAFTable>
        <GlobalAF>
          <Naming>
            <AFName>VPNv4Unicast</AFName>
          </Naming>
          <Enable>true</Enable>
        </GlobalAF>
        <GlobalAF>
          <Naming>
            <AFName>VPNv6Unicast</AFName>
          </Naming>
          <Enable>true</Enable>
        </GlobalAF>
      </GlobalAFTable>
    </Global>
  </AS>
</BGP>

```

```
        </Global>
      </DefaultVRF>
    </FourByteAS>
  </AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>
```

コメント

- なし。

PE L3 MPLS VPN (マルチキャスト、IPv4 および IPv6 対応の VPN、IOS-XR)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS XR でマルチキャスト IPv4 および IPv6 がイネーブルになっている MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : GigabitEthernet0/1/0/1。
 - ルーティング プロトコル = なし

コンフィグレット

PE

次のコード例は、MPLS サービス要求の CLI および XML コンフィグレットを示します。

CLI コンフィグレット

```
vrf V18:VPN_Verve1
address-family ipv4 unicast
  import route-target
    100:19916
    100:19917
  !
  export route-target
    100:19916
  !
!
address-family ipv6 unicast
  import route-target
    100:19916
    100:19917
  !
  export route-target
    100:19916
  !
!
!
interface GigabitEthernet0/1/0/1.2589
  description GigabitEthernet0/1/0/1.2589 dot1q vlan id=2589. By VPNSC: Job Id# = 54
  vrf V18:VPN_Verve1
  ipv4 address 115.106.116.122 255.255.255.0
  ipv6 address 1125::254/24
  dot1q vlan 2589
!
router bgp 100
  vrf V18:VPN_Verve1
  rd 100:19891
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
!
```

```

!
multicast-routing
vrf V18:VPN_VerVel address-family ipv4
  interface GigabitEthernet0/1/0/1.2589
    enable
  !
  mdt mtu 8003
  mdt data 224.10.0.5/32 threshold 8002
  mdt default ipv4 224.10.0.4
  !
vrf V18:VPN_VerVel address-family ipv6
  interface GigabitEthernet0/1/0/1.2589
    enable
  !
  mdt mtu 8003
  mdt default ipv4 224.10.0.4
  !
!
!
router pim vrf V18:VPN_VerVel address-family ipv4
  rp-address 115.101.110.122 list1
  !
router pim vrf V18:VPN_VerVel address-family ipv6
  rp-address 1114::122 list2
  !
end

```

XML コンフィグレット

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V18:VPN_VerVel
address-family ipv6 unicast
import route-target 100:19916
import route-target 100:19917
export route-target 100:19916
exit
interface GigabitEthernet0/1/0/1.2589
ipv6 address 1125::254/24
multicast-routing
vrf V18:VPN_VerVel
mdt default 224.10.0.4
mdt data 224.10.0.5/32 threshold 8002
mdt mtu 8003
interface GigabitEthernet0/1/0/1.2589
enable
vrf V18:VPN_VerVel address-family ipv6
mdt default 224.10.0.4
mdt mtu 8003
interface GigabitEthernet0/1/0/1.2589
enable
router pim vrf V18:VPN_VerVel address-family ipv4 rp-address 115.101.110.122 list1
router pim vrf V18:VPN_VerVel address-family ipv6 rp-address 1114::122 list2
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/0/1.2589</Name>

```

```

        <Active>act</Active>
      </Naming>
      <Shutdown>>true</Shutdown>
    </InterfaceConfiguration>
  </InterfaceConfigurationTable>
</Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>V18:VPN_VerVel</Name>
        </Naming>
        <Create>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
              <Topology>default</Topology>
            </Naming>
            <Create>true</Create>
            <BGP>
              <ImportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19916</ASIndex>
                    </Naming>
                    <True>true</True>
                  </RouteTarget>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19917</ASIndex>
                    </Naming>
                    <True>true</True>
                  </RouteTarget>
                </RouteTargetTable>
              </ImportRouteTargets>
              <ExportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19916</ASIndex>
                    </Naming>
                    <True>true</True>
                  </RouteTarget>
                </RouteTargetTable>
              </ExportRouteTargets>
            </BGP>
          </AFI_SAFI>
        </AFI_SAFITable>
      </VRF>
    </VRFTable>
  </InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>

```

```

    <Name>GigabitEthernet0/1/0/1.2589</Name>
    <Active>act</Active>
  </Naming>
  <Description>GigabitEthernet0/1/0/1.2589 dot1q vlan id=2589. By VPNSC: Job Id# =
54</Description>
  <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
  <VLANSubConfiguration>
    <VLANIdentifier>
      <VlanType>VLANTypeDot1q</VlanType>
      <FirstTag>2589</FirstTag>
    </VLANIdentifier>
  </VLANSubConfiguration>
  <VRF>V18:VPN_Ver1</VRF>
  <IPV4Network>
    <Addresses>
      <Primary>
        <IPAddress>115.106.116.122</IPAddress>
        <Mask>255.255.255.0</Mask>
      </Primary>
    </Addresses>
  </IPV4Network>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>100</AS>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <Name>V18:VPN_Ver1</Name>
          </Naming>
          <VRFGlobal>
            <Exists>true</Exists>
            <RouteDistinguisher>
              <Type>AS</Type>
              <AS>100</AS>
              <ASIndex>19891</ASIndex>
            </RouteDistinguisher>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AF>IPv4Unicast</AF>
                </Naming>
                <Enabled>true</Enabled>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AF>IPv6Unicast</AF>
                </Naming>
                <Enabled>true</Enabled>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
          </VRFGlobal>
        </VRF>
      </VRFTable>
    </FourByteAS>
  </AS>

```

```
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>
```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用します。
- このサービス要求には、コンフィグレットに示されているように、マルチキャスト IPv4 および IPv6 対応の VPN およびスタティック RP があります。

PE L3 MPLS VPN (Static、IOS、IPv6)

-
- 設定**
- サービス : L3 MPLS VPN
 - 機能 : IPv6 アドレッシングを使用した IOS デバイス上の、VPN ルーティング プロトコルがスタティックに設定された MPLS サービス要求
 - デバイス設定 :
 - PE は、IOS 12.2(33) SRD2 を実行しています。
インターフェイス : GigabitEthernet2/3.455
 - ルーティング プロトコル = STATIC

コンフィグレット

PE

```
vrf definition test-vpn-1
rd 123:4
address-family ipv6
route-target import 64512:73647
route-target import 64512:73648
route-target export 64512:73647
!
interface GigabitEthernet2/3.455
description GigabitEthernet2/3.455 dot1q vlan id=455. By VPNSC: Job Id# = 87
encapsulation dot1Q 455
vrf forwarding test-vpn-1
ipv6 address 455::2/60
no shutdown
!
router bgp 64512
address-family ipv6 vrf test-vpn-1
default-information originate
redistribute connected
redistribute static
exit-address-family
!
ipv6 route vrf test-vpn-1 54::4/128 GigabitEthernet2/3.455 24::5 45
```

-
- コメント**
- なし。

PE L3 MPLS VPN (BGP、IOS)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS 上の VPN ルーティング プロトコルが BGP に設定された MPLS サービス要求。
- デバイス設定 :
 - PE は IOS バージョン 12.2(17r) S2 を備えた iscind-7600-2 です。
インターフェイス : FastEthernet2/14。
 - ルーティング プロトコル = BGP

コンフィグレット

PE

```

!
ip vrf V21:VPN
rd 100:19894
route-target import 100:19906
route-target import 100:19907
route-target export 100:19906
!
interface FastEthernet2/14.2691
description FastEthernet2/14.2691 dot1q vlan id=2691. By VPNSC: Job Id# = 59
encapsulation dot1q 2691
ip vrf forwarding V21:VPN
ip address 115.123.102.122 255.255.255.0
no shutdown
!
router bgp 100
address-family ipv4 vrf V21:VPN
neighbor 115.102.123.102 remote-as 100
neighbor 115.102.123.102 activate
neighbor 115.102.123.102 allowas-in 5
neighbor 115.102.123.102 send-community both
neighbor 115.102.123.102 advertisement-interval 122
neighbor 115.102.123.102 maximum-prefix 122 12 restart 122
neighbor 5.2.2.5 route-map TESTING_IN in
neighbor 5.2.2.5 route-map TESTING_OUT out
exit-address-family

```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用します。
- このサービス要求では、[Neighbor Send Community] 属性 (**send-community** コンフィギュレーション コマンドを生成) が [Both] に設定されています。

PE L3 MPLS VPN (BGP、IOS、IPv6)

-
- 設定**
- サービス : L3 MPLS VPN
 - 機能 : IPv6 アドレッシングを使用した IOS デバイス上の、VPN ルーティング プロトコルが BGP に設定された MPLS サービス要求。
 - デバイス設定 :
 - PE は、IOS バージョン 12.2(33) SRD2 を実行しています。
インターフェイス : GigabitEthernet2/3.1234
 - ルーティング プロトコル = BGP

コンフィグレット

PE

```

!
vrf definition VPN-test
rd 12:44
address-family ipv6
route-target import 64512:73647
route-target import 64512:73648
route-target export 64512:73647
!
interface GigabitEthernet2/3.1234
description GigabitEthernet2/3.1234 dot1q vlan id=1234. By VPNSC: Job Id# = 86
encapsulation dot1Q 1234
vrf forwarding VPN-test
ipv6 address 23::5/60
no shutdown
!
router bgp 64512
address-family ipv6 vrf VPN-test
neighbor 345::2 remote-as 44
neighbor 345::2 activate
neighbor 345::2 as-override
neighbor 345::2 allowas-in 4
neighbor 345::2 send-community both
neighbor 345::2 advertisement-interval 123
neighbor 345::2 maximum-prefix 4567 23 restart 234
redistribute connected
redistribute static
exit-address-family

```

-
- コメント**
- なし

PE L3 MPLS VPN (BGP、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS XR 上の VPN ルーティング プロトコルが BGP と設定された MPLS サービス要求
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : GigabitEthernet0/1/0/1。
 - ルーティング プロトコル = BGP

コンフィグレット

PE

次のコード例は、MPLS サービス要求の CLI および XML コンフィグレットを示します。

CLI コンフィグレット

```
vrf V25:Cisco3
address-family ipv4 unicast
import route-target
100:19926
100:19927
!
export route-target
100:19926
!
!
!
interface GigabitEthernet0/1/0/1.2841
description GigabitEthernet0/1/0/1.2841 dot1q vlan id=2841. By VPNSC: Job Id# = 86
vrf V25:Cisco3
ipv4 address 125.101.122.125 255.255.255.0
dot1q vlan 2841
!
router bgp 100
vrf V25:Cisco3
rd 100:19898
address-family ipv4 unicast
!
neighbor 112.120.102.112
remote-as 100
advertisement-interval 122
address-family ipv4 unicast
route-policy verve in
allowas-in 3
route-policy verve out
site-of-origin 64512:700
!
!
!
end
```

XML コンフィグレット

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V25:Cisco3
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/0/1.2841</Name>
          <Active>act</Active>
        </Naming>
        <Shutdown>>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>V25:Cisco3</Name>
        </Naming>
        <Create>>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
              <Topology>default</Topology>
            </Naming>
            <Create>>true</Create>
            <BGP>
              <ImportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19926</ASIndex>
                    </Naming>
                    <True>>true</True>
                  </RouteTarget>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19927</ASIndex>
                    </Naming>
                    <True>>true</True>
                  </RouteTarget>
                </RouteTargetTable>
              </ImportRouteTargets>
              <ExportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>

```

```

        <Type>AS</Type>
        <AS>100</AS>
        <ASIndex>19926</ASIndex>
    </Naming>
    <True>true</True>
</RouteTarget>
</RouteTargetTable>
</ExportRouteTargets>
</BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
<InterfaceConfiguration>
    <Naming>
        <Name>GigabitEthernet0/1/0/1.2841</Name>
        <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/1/0/1.2841 dot1q vlan id=2841. By VPNSC: Job Id# =
86</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
        <VLANIdentifier>
            <VlanType>VLANTypeDot1q</VlanType>
            <FirstTag>2841</FirstTag>
        </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>V25:Cisco3</VRF>
    <IPv4Network>
        <Addresses>
            <Primary>
                <IPAddress>125.101.122.125</IPAddress>
                <Mask>255.255.255.0</Mask>
            </Primary>
        </Addresses>
    </IPv4Network>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
    <AS>
        <Naming>
            <AS>0</AS>
        </Naming>
        <FourByteAS>
            <Naming>
                <AS>100</AS>
            </Naming>
            <VRFTable>
                <VRF>
                    <Naming>
                        <Name>V25:Cisco3</Name>
                    </Naming>
                    <VRFGlobal>
                        <Exists>true</Exists>
                        <RouteDistinguisher>
                            <Type>AS</Type>
                            <AS>100</AS>
                            <ASIndex>19898</ASIndex>
                        </RouteDistinguisher>
                        <VRFGlobalAFTable>
                            <VRFGlobalAF>
                                <Naming>
                                    <AF>IPv4Unicast</AF>

```

```

        </Naming>
        <Enabled>>true</Enabled>
    </VRFGlobalAF>
</VRFGlobalAFTable>
</VRFGlobal>
<VRFNeighborTable>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>112.120.102.112</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <Activate>true</Activate>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>112.120.102.112</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <AllowASIn>3</AllowASIn>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>112.120.102.112</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <RoutePolicyIn>verve</RoutePolicyIn>
        <RoutePolicyIn>verve</RoutePolicyIn>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>112.120.102.112</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>

```

```

        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <RoutePolicyOut>verve</RoutePolicyOut>
        <RoutePolicyOut>verve</RoutePolicyOut>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>112.120.102.112</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <Activate>true</Activate>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
    <AdvertisementInterval>122</AdvertisementInterval>
  </VRFNeighbor>
</VRFNeighborTable>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>

```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用しています。
- このサービス要求では、[Neighbor Send Community] 属性 (**send-community** コンフィギュレーション コマンドを生成) が [None] に設定されています。
- このサービス要求では、ルート ポリシーの名前が [Route Map/Policy In (Out)] 属性を使用して提供されました。



(注) ルート ポリシーはすでにデバイスに存在しています。

コンフィグレットに示すように、展開はその名前のみを使用しました。

- ルート マップ名が提示されなかった場合は、Prime Provisioning はデフォルトとして **IscDefaultPassAll** を追加します。このデフォルトは、IOS XR デバイスの場合にのみ追加されません。IOS デバイスについてはデフォルトが追加されません。

PE L3 MPLS VPN (BGP、RD フォーマット、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : IOS XR に RD IP アドレス形式と BGP プロトコルを持つ MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1 の Cisco IOX デバイスです。
インターフェイス : GigabitEthernet。
 - ルーティング プロトコル = BGP

コンフィグレット

PE

次のコード例は、MPLS サービス要求の CLI および XML コンフィグレットを示します。

MPLS サービス要求の CLI コンフィグレット

```
vrf V29:vpn_techm_cisco
address-family ipv6 unicast
import route-target
 100:15038
 100:15039
!
export route-target
 100:15038
!
!
!

Router bgp 100
vrf V29:vpn_techm_cisco
rd 13.13.13.1:14540
address-family ipv6 unicast
!
!
```

MPLS サービス要求の XML コンフィグレット

```
<VRF>
  <Naming>
    <Name>V1:vpn1</Name>
  </Naming>
  <VRFGlobal>
    <Exists>true</Exists>
    <RouteDistinguisher>
      <Type> IPV4Address </Type>
      <Addr>13.13.13.1</Addr>
      <AddrIndex>14540</AddrIndex>
    </RouteDistinguisher>
    <VRFGlobalAFTable>
      <VRFGlobalAF>
        <Naming>
```

```
        <AF>IPv4Unicast</AF>
      </Naming>
      <Enabled>>true</Enabled>
    <StaticRoutes/>
  </VRFGlobalAF>
</VRFGlobalAFTable>
</VRFGlobal>
</VRF>
```

コメント

- なし。

PE L3 MPLS VPN (BGP、Maximum Prefix/Restart、IOS XR)

-
- 設定**
- サービス : L3 MPLS VPN
 - 機能 : BGP ルーティング プロトコルを使用し、最大プレフィックス数と再開値を指定する MPLS サービス要求。
 - デバイス設定 :
 - PE は、IOS XR バージョン 3.8.1 または 3.9.0 が動作する IOS XR デバイス。
インターフェイス : 各種。
 - ルーティング プロトコル = BGP

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```
router bgp 64512
vrf V22:27Cerc1
address-family ipv4 unicast
!
address-family ipv6 unicast
!
neighbor 1.2.5.4
address-family ipv4 unicast
maximum-prefix 101 91 restart 81
!
!
neighbor 11::69
address-family ipv6 unicast
maximum-prefix 124 46 restart 6711
!
!
!
end
```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。これは再開コンフィグレットを示す例です。

```
router bgp 64512
vrf V23:27Cerc2
address-family ipv4 unicast
!
address-family ipv6 unicast
!
neighbor 8.5.2.33
address-family ipv4 unicast
maximum-prefix 160 80 restart 300
!
```

```

!
neighbor 25::9
address-family ipv6 unicast
  maximum-prefix 200 26 restart 214
!
!
!
!
end

```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。これは警告のみのコンフィグレットを示す例です。

```

router bgp 64512
vrf V23:27Cerc2
address-family ipv4 unicast
!
address-family ipv6 unicast
!
neighbor 8.5.2.33
address-family ipv4 unicast
  maximum-prefix 160 80 warning-only
!
!
neighbor 25::9
address-family ipv6 unicast
  maximum-prefix 200 26 warning-only
!
!
!
!
end

```

XML コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <Set>
    <Configuration Source="CurrentConfig">
      <BGP>
        <AS>
          <Naming>
            <AS>0</AS>
          </Naming>
          <FourByteAS>
            <Naming>
              <AS>64512</AS>
            </Naming>
          <VRFTable>
            <VRF>
              <Naming>
                <Name>V22:27Cerc1</Name>
              </Naming>
              <VRFGlobal>
                <Exists>true</Exists>
                <VRFGlobalAFTable>
                  <VRFGlobalAF>
                    <Naming>
                      <AF>IPv4Unicast</AF>
                    </Naming>
                    <Enabled>true</Enabled>

```

```

    </VRFGlobalAF>
  </VRFGlobalAFTable>
<VRFGlobalAFTable>
  <VRFGlobalAF>
    <Naming>
      <AF>IPv6Unicast</AF>
    </Naming>
    <Enabled>>true</Enabled>
  </VRFGlobalAF>
</VRFGlobalAFTable>
</VRFGlobal>
<VRFNeighborTable>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>1.2.5.4</IPv4Address>
      </IPAddress>
    </Naming>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <MaximumPrefixes>
          <Value>101</Value>
          <WarningPercentage>91</WarningPercentage>
          <RestartTime>81</RestartTime>
          <WarningOnly>>false</WarningOnly>
        </MaximumPrefixes>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
<VRFNeighbor>
  <Naming>
    <IPAddress>
      <IPv6Address>11::69</IPv6Address>
    </IPAddress>
  </Naming>
  <VRFNeighborAFTable>
    <VRFNeighborAF>
      <Naming>
        <AF>IPv6Unicast</AF>
      </Naming>
      <MaximumPrefixes>
        <Value>124</Value>
        <WarningPercentage>46</WarningPercentage>
        <RestartTime>6711</RestartTime>
        <WarningOnly>>false</WarningOnly>
      </MaximumPrefixes>
    </VRFNeighborAF>
  </VRFNeighborAFTable>
</VRFNeighbor>
</VRFNeighborTable>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>

```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <Set>
    <Configuration Source="CurrentConfig">
      <BGP>
        <AS>
          <Naming>
            <AS>0</AS>
          </Naming>
          <FourByteAS>
            <Naming>
              <AS>64512</AS>
            </Naming>
          <VRFTable>
            <VRF>
              <Naming>
                <VRFName>V23:27Cerc2</VRFName>
              </Naming>
              <VRFGlobal>
                <Exists>true</Exists>
                <VRFGlobalAFTable>
                  <VRFGlobalAF>
                    <Naming>
                      <AFName>IPv4Unicast</AFName>
                    </Naming>
                    <Enable>true</Enable>
                  </VRFGlobalAF>
                </VRFGlobalAFTable>
                <VRFGlobalAFTable>
                  <VRFGlobalAF>
                    <Naming>
                      <AFName>IPv6Unicast</AFName>
                    </Naming>
                    <Enable>true</Enable>
                  </VRFGlobalAF>
                </VRFGlobalAFTable>
              </VRFGlobal>
              <VRFNeighborTable>
                <VRFNeighbor>
                  <Naming>
                    <NeighborAddress>
                      <IPv4Address>8.5.2.33</IPv4Address>
                    </NeighborAddress>
                  </Naming>
                  <VRFNeighborAFTable>
                    <VRFNeighborAF>
                      <Naming>
                        <AFName>IPv4Unicast</AFName>
                      </Naming>
                      <MaximumPrefixes>
                        <PrefixLimit>160</PrefixLimit>
                        <WarningPercentage>80</WarningPercentage>
                        <RestartTime>300</RestartTime>
                        <WarningOnly>>false</WarningOnly>
                      </MaximumPrefixes>
                    </VRFNeighborAF>
                  </VRFNeighborAFTable>
                </VRFNeighbor>
              </VRFNeighborTable>
            </VRF>
          </VRFTable>
        </AS>
      </BGP>
    </Configuration>
  </Set>
</Request>
```

```

        </NeighborAddress>
    </Naming>
    <VRFNeighborAFTable>
        <VRFNeighborAF>
            <Naming>
                <AFName>IPv6Unicast</AFName>
            </Naming>
            <MaximumPrefixes>
                <PrefixLimit>200</PrefixLimit>
                <WarningPercentage>26</WarningPercentage>
                <RestartTime>214</RestartTime>
                <WarningOnly>>false</WarningOnly>
            </MaximumPrefixes>
        </VRFNeighborAF>
    </VRFNeighborAFTable>
</VRFNeighbor>
</VRFNeighborTable>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>

```

コメント

- ユーザが警告のみの値と再開値の両方を指定した場合、Prime Provisioning は、すべての IOS および IOS XR バージョンの再開値を評価し、優先順位を与えます。
- 個々の値に対して（いずれかが指定されている場合は、warning-only や restart など）、Prime Provisioning はそれに基づいて設定します。

PE L3 MPLS VPN (BGP、Default Information Originate、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : BGP ルーティング プロトコルを使用し、[Default Information Originate] 属性によって BGP スピーカ (ローカル ルータ) がデフォルト ルートをネイバーに送信するようにするための設定を指定する MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.8.1 または 3.9.0 が動作する IOS XR デバイス。
インターフェイス : 各種。
 - ルーティング プロトコル = BGP

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```
vrf V1:mpls
  rd 100:345
  address-family ipv4 unicast
    redistribute static
  !
  address-family ipv6 unicast
  !
  neighbor 1.1.1.1
    remote-as 100
    address-family ipv4 unicast
      default-originate route-policy dinesh
    !
  !
  neighbor 1.1.1.2
    remote-as 100
    address-family ipv4 unicast
      default-originate
    !
  !
  neighbor 2002::23
    remote-as 100
    address-family ipv6 unicast
      default-originate disable
    !
  !
  !
```

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```
vrf V1:mpls
  rd 100:345
```

```

address-family ipv4 unicast
  redistribute static
!
address-family ipv6 unicast
!
neighbor 1.1.1.1
  remote-as 100
  address-family ipv4 unicast
    default-originate route-policy dinesh
!
!
neighbor 1.1.1.2
  remote-as 100
  address-family ipv4 unicast
    default-originate
!
!

neighbor 2002::23
  remote-as 100
  address-family ipv6 unicast
    default-originate inheritance-disable
!
!
!

```

XML コンフィグレットの例

次に、IOS XR 3.8.1 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```

<BGP MajorVersion="30" MinorVersion="2">
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>100</AS>
      </Naming>
      <BGPRunning>true</BGPRunning>
      <VRFTTable>
        <VRF>
          <Naming>
            <Name>V1:mpls</Name>
          </Naming>
          <VRFGlobal>
            <Exists>true</Exists>
            <RouteDistinguisher>
              <Type>AS</Type>
              <AS>100</AS>
              <ASIndex>345</ASIndex>
            </RouteDistinguisher>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AF>IPv4Unicast</AF>
                </Naming>
                <Enabled>true</Enabled>
                <StaticRoutes/>
              </VRFGlobalAF>
            </VRFGlobalAF>
          </VRF>
        </VRFTTable>
      </FourByteAS>
    </AS>
  </AS>
</BGP>

```

```

        <Enabled>true</Enabled>
    </VRFGlobalAF>
</VRFGlobalAFTable>
</VRFGlobal>
<VRFNeighborTable>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv4Address>1.1.1.1</IPv4Address>
      </IPAddress>
    </Naming>
    <RemoteAS>
      <AS_XX>0</AS_XX>
      <AS_YY>100</AS_YY>
    </RemoteAS>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <Activate>true</Activate>
        <DefaultOriginate>
          <Enable>true</Enable>
          <RoutePolicy>dinesh</RoutePolicy>
        </DefaultOriginate>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv6Address>2002::23</IPv6Address>
      </IPAddress>
    </Naming>
    <RemoteAS>
      <AS_XX>0</AS_XX>
      <AS_YY>100</AS_YY>
    </RemoteAS>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>
          <AF>IPv6Unicast</AF>
        </Naming>
        <Activate>true</Activate>
        <DefaultOriginate>
          <Enable>true</Enable>
        </DefaultOriginate>
      </VRFNeighborAF>
    </VRFNeighborAFTable>
  </VRFNeighbor>
  <VRFNeighbor>
    <Naming>
      <IPAddress>
        <IPv6Address>2002::23</IPv6Address>
      </IPAddress>
    </Naming>
    <RemoteAS>
      <AS_XX>0</AS_XX>
      <AS_YY>100</AS_YY>
    </RemoteAS>
    <VRFNeighborAFTable>
      <VRFNeighborAF>
        <Naming>

```

```
        <AF>IPv6Unicast</AF>
      </Naming>
      <Activate>>true</Activate>
      <DefaultOriginate>
        <Enable>>false</Enable>
      </DefaultOriginate>
    </VRFNeighborAF>
  </VRFNeighborAFTable>
</VRFNeighbor>
</VRFNeighborTable>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
```

コメント

- なし。

PE L3 MPLS VPN (OSPF、IOS)

設定

- サービス : L3 MPLS VPN
- 機能 : VPN ルーティング プロトコルが OSPF に設定された IOS 上の MPLS サービス要求
- デバイス設定 :
 - PE は IOS バージョン 12.2(17r) S2 を備えた iscind-7600-2 です。
 - ルーティング プロトコル = OSPF

コンフィグレット

PE

```
!  
no interface FastEthernet2/14.2685  
!  
interface FastEthernet2/14.2677  
description FastEthernet2/14.2677 dot1q vlan id=2677. By VPNSC: Job Id# = 60  
encapsulation dot1q 2677  
ip vrf forwarding Tester1  
ip address 112.126.102.106 255.255.255.0  
no shutdown  
!  
router ospf 1266 vrf Tester1  
redistribute bgp 100 subnets  
network 112.126.102.0 0.0.0.255 area 23693  
!  
router bgp 100  
address-family ipv4 vrf Tester1  
redistribute ospf 1266 vrf Tester1 metric 1263 route-map verve match internal external 1  
external 2
```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用しています。
- OSPF 一致条件は「Both」に設定されています。このため、**internal**、**external1**、および **external2** コンフィギュレーション コマンドがコンフィグレットで生成されます。
- このコマンドの IOS XR バリエーションには **external type 1** または **external type 2** コマンドのサポートは存在しませんが、IOS ではそのサポートが存在します。

PE L3 MPLS VPN (OSPF、IOS XR)

-
- 設定**
- サービス : L3 MPLS VPN
 - 機能 : VPN ルーティング プロトコルが OSPF に設定された IOS XR 上の MPLS サービス要求
 - デバイス設定 :
 - PE は、IOS XR バージョン 3.6.1[00] の mlpe7 です。
インターフェイス : GigabitEthernet0/1/0/1。
 - ルーティング プロトコル = OSPF

コンフィグレット

PE

次のコード例は、MPLS サービス要求の CLI および XML コンフィグレットを示します。

MPLS サービス要求の CLI コンフィグレット

```
vrf V28:Cisco5
address-family ipv4 unicast
import route-target
100:19930
100:19931
!
export route-target
100:19930
!
!
!
interface GigabitEthernet0/1/1/4.2693
description GigabitEthernet0/1/1/4.2693 dot1q vlan id=2693. By VPNSC: Job Id# = 90
vrf V28:Cisco5
ipv4 address 123.33.102.112 255.255.255.0
dot1q vlan 2693
!
router ospf 1238
vrf V28:Cisco5
redistribute bgp 100
area 29871
interface GigabitEthernet0/1/1/4.2693
!
!
!
!
router bgp 100
vrf V28:Cisco5
rd 100:19901
address-family ipv4 unicast
redistribute ospf 1238 match internal external metric 2581 route-policy verve
!
!
!
end
```

MPLS サービス要求の XML コンフィグレット

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V28:Cisco5
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/1/4.2693</Name>
          <Active>act</Active>
        </Naming>
        <Shutdown>>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>V28:Cisco5</Name>
        </Naming>
        <Create>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
            </Naming>
            <Create>true</Create>
            <BGP>
              <ImportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19930</ASIndex>
                    </Naming>
                    <True>true</True>
                  </RouteTarget>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>100</AS>
                      <ASIndex>19931</ASIndex>
                    </Naming>
                    <True>true</True>
                  </RouteTarget>
                </RouteTargetTable>
              </ImportRouteTargets>
              <ExportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>

```

```

        <AS>100</AS>
        <ASIndex>19930</ASIndex>
    </Naming>
    <True>>true</True>
</RouteTarget>
</RouteTargetTable>
</ExportRouteTargets>
</BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
<InterfaceConfiguration>
    <Naming>
        <Name>GigabitEthernet0/1/1/4.2693</Name>
        <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/1/1/4.2693 dot1q vlan id=2693. By VPNSC: Job Id# =
90</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
        <VLANIdentifier>
            <VlanType>VLANTypeDot1q</VlanType>
            <FirstTag>2693</FirstTag>
        </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>V28:Cisco5</VRF>
    <IPV4Network>
        <Addresses>
            <Primary>
                <IPAddress>123.33.102.112</IPAddress>
                <Mask>255.255.255.0</Mask>
            </Primary>
        </Addresses>
    </IPV4Network>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
<AS>
    <Naming>
        <AS>0</AS>
    </Naming>
    <FourByteAS>
        <Naming>
            <AS>100</AS>
        </Naming>
    </VRFTable>
    <VRF>
        <Naming>
            <Name>V28:Cisco5</Name>
        </Naming>
    <VRFGlobal>
        <Exists>>true</Exists>
        <RouteDistinguisher>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>19901</ASIndex>
        </RouteDistinguisher>
    <VRFGlobalAFTable>
        <VRFGlobalAF>
            <Naming>
                <AF>IPv4Unicast</AF>
            </Naming>

```

```

        <Enabled>true</Enabled>
        <OSPFRouteTable>
          <OSPFRoutes>
            <Naming>
              <OSPFInstanceName>1238</OSPFInstanceName>
            </Naming>
            <RoutePolicy/>
            <RedistType>21</RedistType>
            <DefaultMetric>2581</DefaultMetric>
          </OSPFRoutes>
        </OSPFRouteTable>
      </VRFGlobalAF>
    </VRFGlobalAFTable>
  </VRFGlobal>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
<OSPF>
  <ProcessTable>
    <Process>
      <Naming>
        <InstanceName>1238</InstanceName>
      </Naming>
      <Start>true</Start>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>V28:Cisco5</VRFName>
          </Naming>
          <VRFStart>true</VRFStart>
          <Redistribution>
            <RedistributeTable>
              <Redistribute>
                <Naming>
                  <ProtocolType>bgp</ProtocolType>
                  <InstanceName>bgp</InstanceName>
                  <BGP_AS_XX>0</BGP_AS_XX>
                  <BGP_AS_YY>100</BGP_AS_YY>
                </Naming>
                <Classful>>false</Classful>
              </Redistribute>
            </RedistributeTable>
          </Redistribution>
          <AreaTable>
            <Area>
              <Naming>
                <IntegerID>29871</IntegerID>
              </Naming>
              <NameScopeTable>
                <NameScope>
                  <Naming>
                    <Interface>GigabitEthernet0/1/1/4.2693</Interface>
                  </Naming>
                  <Running>true</Running>
                </NameScope>
              </NameScopeTable>
              <Running>true</Running>
            </Area>
          </AreaTable>
        </VRF>
      </VRFTable>
    </Process>
  </ProcessTable>

```

```
        </ProcessTable>
    </OSPF>
</Configuration>
</Set>
<Commit/>
</Request>
```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用します。
- OSPF 一致条件は「Both」に設定されています。このため、**internal** および **external** コンフィギュレーション コマンドがコンフィグレットで生成されます。
- このコマンドの IOS XR バリエーションには **external type 1** または **external type 2** のサポートは存在しませんが、IOS ではそのサポートが存在します。

L3 MPLS VPN (OSPF、Default Information Originate、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : OSPF ルーティング プロトコルを使用し、[Default Information Originate] を設定して、デフォルトの外部ルートを OSPF ルーティング ドメインに生成する MPLS サービス要求。
- デバイス設定 :
 - PE は IOS XR バージョン 3.9.0 が動作する IOS XR デバイス
インターフェイス : 各種。
 - ルーティング プロトコル = OSPF

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの CLI コンフィグレットの例を示します。

```
vrf V35:apr26-vpn9
address-family ipv4 unicast
import route-target
64512:2776
64512:2777
!
export route-target
64512:2776
!
!
address-family ipv6 unicast
import route-target
64512:2776
64512:2777
!
export route-target
64512:2776
!
!
!
interface GigabitEthernet0/15/1/1.947
description GigabitEthernet0/15/1/1.947 dot1q vlan id=947. By VPNSC: Job Id# = 191
vrf V35:apr26-vpn9
ipv4 address 26.27.28.21 255.255.255.0
ipv6 address 2165::541/32
dot1q vlan 947
!
router ospf 1611
vrf V35:apr26-vpn9
default-information originate always metric 652 metric-type 2 route-policy dinesh
area 218
interface GigabitEthernet0/15/1/1.947
!
```

```

!
!
!
router bgp 64512
 vrf V35:apr26-vpn9
  rd 64512:2190
  address-family ipv4 unicast
    redistribute connected
    redistribute static
    redistribute ospf 1611 match internal metric 325
  !
  address-family ipv6 unicast
    redistribute static
  !
!
!
end

```

XML コンフィグレットの例

次に、IOS XR 3.9.0 が動作する IOS XR デバイスの XML コンフィグレットの例を示します。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V35:apr26-vpn9
address-family ipv6 unicast
import route-target 64512:2776
import route-target 64512:2777
export route-target 64512:2776
exit
interface GigabitEthernet0/15/1/1.947
ipv6 address 2165::541/32
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <InterfaceName>GigabitEthernet0/15/1/1.947</InterfaceName>
          <Active>act</Active>
        </Naming>
        <Shutdown>>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <VRFName>V35:apr26-vpn9</VRFName>
        </Naming>
        <Create>>true</Create>
        <AFTable>
          <AF>
            <Naming>
              <AFName>IPv4</AFName>
              <SAFName>Unicast</SAFName>
              <TopologyName>default</TopologyName>
            </Naming>

```

```

<Create>true</Create>
<BGP>
  <ImportRouteTargets>
    <RouteTargetTable>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>2776</ASIndex>
        </Naming>
        <Enable>true</Enable>
      </RouteTarget>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>2777</ASIndex>
        </Naming>
        <Enable>true</Enable>
      </RouteTarget>
    </RouteTargetTable>
  </ImportRouteTargets>
  <ExportRouteTargets>
    <RouteTargetTable>
      <RouteTarget>
        <Naming>
          <Type>AS</Type>
          <AS_XX>0</AS_XX>
          <AS>64512</AS>
          <ASIndex>2776</ASIndex>
        </Naming>
        <Enable>true</Enable>
      </RouteTarget>
    </RouteTargetTable>
  </ExportRouteTargets>
</BGP>
</AF>
</AFTable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <InterfaceName>GigabitEthernet0/15/1/1.947</InterfaceName>
      <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/15/1/1.947 dot1q vlan id=947. By VPNSC: Job Id# =
191</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
      <VLANIdentifier>
        <VlanType>VLANTypeDot1q</VlanType>
        <FirstTag>947</FirstTag>
      </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>V35:apr26-vpn9</VRF>
    <IPv4Network>
      <Addresses>
        <Primary>
          <Address>26.27.28.21</Address>
          <Netmask>255.255.255.0</Netmask>
        </Primary>

```

```

        </Addresses>
    </IPV4Network>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>64512</AS>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>V35:apr26-vpn9</VRFName>
          </Naming>
          <VRFGlobal>
            <Exists>true</Exists>
            <RouteDistinguisher>
              <Type>AS</Type>
              <AS_XX>0</AS_XX>
              <AS>64512</AS>
              <ASIndex>2190</ASIndex>
            </RouteDistinguisher>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AFName>IPv4Unicast</AFName>
                </Naming>
                <Enable>true</Enable>
                <ConnectedRoutes/>
                <OSPFRouteTable>
                  <OSPFRoute>
                    <Naming>
                      <InstanceName>1611</InstanceName>
                    </Naming>
                    <RoutePolicyName/>
                    <RedistType>01</RedistType>
                    <DefaultMetric>325</DefaultMetric>
                  </OSPFRoute>
                </OSPFRouteTable>
                <StaticRoutes/>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
            <VRFGlobalAFTable>
              <VRFGlobalAF>
                <Naming>
                  <AFName>IPv6Unicast</AFName>
                </Naming>
                <Enable>true</Enable>
                <StaticRoutes/>
              </VRFGlobalAF>
            </VRFGlobalAFTable>
          </VRFGlobal>
        </VRF>
      </VRFTable>
    </FourByteAS>
  </AS>
</BGP>
<OSPF>
  <ProcessTable>
    <Process>

```

```
<Naming>
  <ProcessName>1611</ProcessName>
</Naming>
<Start>true</Start>
<VRFTable>
  <VRF>
    <Naming>
      <VRFName>V35:apr26-vpn9</VRFName>
    </Naming>
    <VRFStart>true</VRFStart>
    <DefaultInformation>
      <AlwaysAdvertise>true</AlwaysAdvertise>
      <Metric>652</Metric>
      <MetricType>Type2</MetricType>
      <Policy>dinesh</Policy>
    </DefaultInformation>
    <AreaTable>
      <Area>
        <Naming>
          <AreaID>218</AreaID>
        </Naming>
        <NameScopeTable>
          <NameScope>
            <Naming>
              <InterfaceName>GigabitEthernet0/15/1/1.947</InterfaceName>
            </Naming>
            <Running>true</Running>
          </NameScope>
        </NameScopeTable>
        <Running>true</Running>
      </Area>
    </AreaTable>
  </VRF>
</VRFTable>
</Process>
</ProcessTable>
</OSPF>
</Configuration>
</Set>
<Commit/>
</Request>
```

コメント

- なし。

PE L3 MPLS VPN (EIGRP、Authentication Keychain Name、IOS XR)

-
- 設定**
- サービス : L3 MPLS VPN
 - 機能 : EIGRP ルーティング プロトコルを使用し、キーチェーン名を指定して、インターフェイス上の EIGRP プロトコルトラフィックを認証する MPLS サービス要求。
 - デバイス設定 :
 - PE は、IOS XR バージョン 3.8.1 または 3.9.0 が動作する IOS XR デバイス。
インターフェイス : 各種。
 - ルーティング プロトコル = EIGRP。

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS XR デバイスの CLI コンフィグレット例を示します。

```
vrf V67:apr26-vpn2
address-family ipv4 unicast
import route-target
64512:2764
64512:2765
!
export route-target
64512:2764
!
!
address-family ipv6 unicast
import route-target
64512:2764
64512:2765
!
export route-target
64512:2764
!
!
!
interface TenGigE0/0/0/3.841
description TenGigE0/0/0/3.841 dot1q vlan id=841. By VPNSC: Job Id# = 188
vrf V67:apr26-vpn2
ipv4 address 31.32.33.23 255.255.255.0
ipv6 address 500::200/32
dot1q vlan 841
!
router bgp 64512
vrf V67:apr26-vpn2
rd 64512:2222
address-family ipv4 unicast
redistribute eigrp 1324
!
```

```

address-family ipv6 unicast
  redistribute eigrp 1321
!
!
!
router eigrp 100
vrf V67:apr26-vpn2
  address-family ipv4
    default-metric 1509 1842 196 187 1657
    autonomous-system 1324
    interface TenGigE0/0/0/3.841
      authentication keychain keychain-ipv4
    !
  !
  address-family ipv6
    default-metric 1624 1428 186 127 1095
    autonomous-system 1321
    interface TenGigE0/0/0/3.841
      authentication keychain keychain-ipv6
    !
  !
!
end

```

XML コンフィグレットの例

次に、IOS XR デバイスの XML コンフィグレット例を示します。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V67:apr26-vpn2
address-family ipv6 unicast
import route-target 64512:2764
import route-target 64512:2765
export route-target 64512:2764
exit
interface TenGigE0/0/0/3.841
ipv6 address 500::200/32
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <EIGRP>
      <ProcessTable>
        <Process>
          <Naming>
            <ASNumber>100</ASNumber>
          </Naming>
          <VRFTTable>
            <VRF>
              <Naming>
                <VRFName>V67:apr26-vpn2</VRFName>
              </Naming>
              <VRF_AFTable>
                <VRF_AF>
                  <Naming>
                    <VRF_AFTType>IPv4</VRF_AFTType>
                  </Naming>
                  <AutoSummary/>
                </VRF_AF>
              </VRF_AF>
            </VRF>
          </VRFTTable>
        </Process>
      </ProcessTable>
    </EIGRP>
  </Configuration>
</Delete>

```

```

        <Naming>
          <VRF_AFTType>IPv6</VRF_AFTType>
        </Naming>
        <AutoSummary/>
      </VRF_AF>
    </VRF_AFTTable>
  </VRF>
</VRFTable>
</Process>
</ProcessTable>
</EIGRP>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <Name>TenGigE0/0/0/3.841</Name>
      <Active>act</Active>
    </Naming>
    <Shutdown>>true</Shutdown>
  </InterfaceConfiguration>
</InterfaceConfigurationTable>
</Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>V67:apr26-vpn2</Name>
        </Naming>
        <Create>>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
              <Topology>default</Topology>
            </Naming>
            <Create>>true</Create>
            <BGP>
              <ImportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>64512</AS>
                      <ASIndex>2764</ASIndex>
                    </Naming>
                    <True>>true</True>
                  </RouteTarget>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>
                      <AS>64512</AS>
                      <ASIndex>2765</ASIndex>
                    </Naming>
                    <True>>true</True>
                  </RouteTarget>
                </RouteTargetTable>
              </ImportRouteTargets>
              <ExportRouteTargets>
                <RouteTargetTable>
                  <RouteTarget>
                    <Naming>
                      <Type>AS</Type>

```

```

        <AS>64512</AS>
        <ASIndex>2764</ASIndex>
    </Naming>
    <True>>true</True>
</RouteTarget>
</RouteTargetTable>
</ExportRouteTargets>
</BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <Name>TenGigE0/0/0/3.841</Name>
      <Active>act</Active>
    </Naming>
    <Description>TenGigE0/0/0/3.841 dot1q vlan id=841. By VPNSC: Job Id# =
188</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
      <VLANIdentifier>
        <VlanType>VLANTypeDot1q</VlanType>
        <FirstTag>841</FirstTag>
      </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>V67:apr26-vpn2</VRF>
    <IPV4Network>
      <Addresses>
        <Primary>
          <IPAddress>31.32.33.23</IPAddress>
          <Mask>255.255.255.0</Mask>
        </Primary>
      </Addresses>
    </IPV4Network>
  </InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>64512</AS>
      </Naming>
    </VRFTable>
    <VRF>
      <Naming>
        <Name>V67:apr26-vpn2</Name>
      </Naming>
      <VRFGlobal>
        <Exists>>true</Exists>
        <RouteDistinguisher>
          <Type>AS</Type>
          <AS>64512</AS>
          <ASIndex>2222</ASIndex>
        </RouteDistinguisher>
        <VRFGlobalAFTable>
          <VRFGlobalAF>
            <Naming>
              <AF>IPv4Unicast</AF>
            </Naming>
          </VRFGlobalAF>
        </VRFGlobalAFTable>
      </VRFGlobal>
    </VRF>
  </AS>

```

```

        <Enabled>true</Enabled>
        <EIGRPRouteTable>
          <EIGRPRoutes>
            <Naming>
              <EIGRPInstanceName>1324</EIGRPInstanceName>
            </Naming>
          </EIGRPRoutes>
        </EIGRPRouteTable>
      </VRFGlobalAF>
    </VRFGlobalAFTable>
  <VRFGlobalAFTable>
    <VRFGlobalAF>
      <Naming>
        <AF>IPv6Unicast</AF>
      </Naming>
      <Enabled>true</Enabled>
      <EIGRPRouteTable>
        <EIGRPRoutes>
          <Naming>
            <EIGRPInstanceName>1321</EIGRPInstanceName>
          </Naming>
        </EIGRPRoutes>
      </EIGRPRouteTable>
    </VRFGlobalAF>
  </VRFGlobalAFTable>
</VRFGlobal>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
<EIGRP>
  <ProcessTable>
    <Process>
      <Naming>
        <ASNumber>100</ASNumber>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>V67:apr26-vpn2</VRFName>
          </Naming>
          <Enabled>true</Enabled>
          <VRF_AFTable>
            <VRF_AF>
              <Naming>
                <VRF_AFType>IPv4</VRF_AFType>
              </Naming>
              <Enabled>true</Enabled>
              <RedistributeTable>
                <Redistribute>
                  <Naming>
                    <Protocol>BGP</Protocol>
                    <SecondASNumber>64512</SecondASNumber>
                  </Naming>
                  <PolicySpecified>>false</PolicySpecified>
                </Redistribute>
              </RedistributeTable>
            </VRF_AF>
          </VRF_AFTable>
          <DefaultMetric>
            <BW>1509</BW>
            <Delay>1842</Delay>
            <Reliability>196</Reliability>
            <Load>187</Load>
            <MTU>1657</MTU>
          </DefaultMetric>
        </VRF>
      </VRFTable>
    </Process>
  </ProcessTable>

```

```

</DefaultMetric>
<InterfaceTable>
  <Interface>
    <Naming>
      <InterfaceName>TenGigE0/0/0/3.841</InterfaceName>
    </Naming>
    <Enabled>true</Enabled>
    <Authentication>
      <Keychain>keychain-ipv4</Keychain>
    </Authentication>
  </Interface>
</InterfaceTable>
<AutonomousSystem>1324</AutonomousSystem>
</VRF_AF>
<VRF_AF>
  <Naming>
    <VRF_AFTYPE>IPv6</VRF_AFTYPE>
  </Naming>
  <Enabled>true</Enabled>
  <RedistributeTable>
    <Redistribute>
      <Naming>
        <Protocol>BGP</Protocol>
        <SecondASNumber>64512</SecondASNumber>
      </Naming>
      <PolicySpecified>>false</PolicySpecified>
    </Redistribute>
  </RedistributeTable>
  <DefaultMetric>
    <BW>1624</BW>
    <Delay>1428</Delay>
    <Reliability>186</Reliability>
    <Load>127</Load>
    <MTU>1095</MTU>
  </DefaultMetric>
  <InterfaceTable>
    <Interface>
      <Naming>
        <InterfaceName>TenGigE0/0/0/3.841</InterfaceName>
      </Naming>
      <Enabled>true</Enabled>
      <Authentication>
        <Keychain>keychain-ipv6</Keychain>
      </Authentication>
    </Interface>
  </InterfaceTable>
  <AutonomousSystem>1321</AutonomousSystem>
</VRF_AF>
</VRF_AFTable>
</VRF>
</VRFTable>
</Process>
</ProcessTable>
</EIGRP>
</Configuration>
</Set>
<Commit/>
</Request>

```

コメント

- なし。

PE L3 MPLS VPN (独立 VRF、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : 独立 VRF を IOS XR で使用する MPLS サービス要求
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : GigabitEthernet0/1/0/1。
 - ルーティング プロトコル = なし

コンフィグレット

PE および VRF

次のコード例は、MPLS サービス要求と VRF オブジェクトの CLI および XML コンフィグレットを示します。

MPLS サービス要求の CLI コンフィグレット

```
interface GigabitEthernet0/1/0/0.3233
  description GigabitEthernet0/1/0/0.3233 dot1q vlan id=3233. By VPNSC: Job Id# = 64
  vrf VRF112
  ipv4 address 126.112.102.102 255.255.255.0
  ipv6 address 1365::126/28
  dot1q vlan 3233
!
router bgp 100
  vrf VRF112
    address-family ipv4 unicast
    !
    address-family ipv6 unicast
    !
    !
  !
!
multicast-routing
  vrf VRF112 address-family ipv4
    interface GigabitEthernet0/1/0/0.3233
      enable
    !
  !
  vrf VRF112 address-family ipv6
    interface GigabitEthernet0/1/0/0.3233
      enable
    !
  !
!
end
```

MPLS サービス要求の XML コンフィグレット

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
interface GigabitEthernet0/1/0/0.3233
ipv6 address 1365::126/28
multicast-routing
vrf VRF112
interface GigabitEthernet0/1/0/0.3233
enable
vrf VRF112 address-family ipv6
interface GigabitEthernet0/1/0/0.3233
enable
</Configuration>
</CLI>
<Delete>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/0/0.3233</Name>
          <Active>act</Active>
        </Naming>
        <Shutdown>true</Shutdown>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
  </Configuration>
</Delete>
<Set>
  <Configuration Source="CurrentConfig">
    <InterfaceConfigurationTable>
      <InterfaceConfiguration>
        <Naming>
          <Name>GigabitEthernet0/1/0/0.3233</Name>
          <Active>act</Active>
        </Naming>
        <Description>GigabitEthernet0/1/0/0.3233 dot1q vlan id=3233. By VPNSC: Job Id# =
64</Description>
        <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
        <VLANSubConfiguration>
          <VLANIdentifier>
            <VlanType>VLANTypeDot1q</VlanType>
            <FirstTag>3233</FirstTag>
          </VLANIdentifier>
        </VLANSubConfiguration>
        <VRF>VRF112</VRF>
        <IPV4Network>
          <Addresses>
            <Primary>
              <IPAddress>126.112.102.102</IPAddress>
              <Mask>255.255.255.0</Mask>
            </Primary>
          </Addresses>
        </IPV4Network>
      </InterfaceConfiguration>
    </InterfaceConfigurationTable>
    <BGP>
      <AS>
        <Naming>
          <AS>0</AS>
        </Naming>

```

```

<FourByteAS>
  <Naming>
    <AS>100</AS>
  </Naming>
  <VRFTable>
    <VRF>
      <Naming>
        <Name>VRF112</Name>
      </Naming>
      <VRFGlobal>
        <Exists>true</Exists>
        <VRFGlobalAFTable>
          <VRFGlobalAF>
            <Naming>
              <AF>IPv4Unicast</AF>
            </Naming>
            <Enabled>true</Enabled>
          </VRFGlobalAF>
        </VRFGlobalAFTable>
        <VRFGlobalAFTable>
          <VRFGlobalAF>
            <Naming>
              <AF>IPv6Unicast</AF>
            </Naming>
            <Enabled>true</Enabled>
          </VRFGlobalAF>
        </VRFGlobalAFTable>
      </VRFGlobal>
    </VRF>
  </VRFTable>
</FourByteAS>
</AS>
</BGP>
</Configuration>
</Set>
<Commit/>
</Request>

```

VRF サービス要求の CLI コンフィグレット

```

vrf VRF112
  address-family ipv4 unicast
    import route-target
      100:19890
      100:19891
    !
    export route-target
      100:19890
    !
  !
  address-family ipv6 unicast
    import route-target
      100:19890
      100:19891
    !
    export route-target
      100:19890
    !
  !
!
router bgp 100
  vrf VRF112
    rd 112.101.112.101:1263

```

```

!
!
multicast-routing
vrf VRF112 address-family ipv4
  mdt mtu 8025
  mdt data 224.10.0.9/32 threshold 8024
  mdt default ipv4 224.10.0.8
!
vrf VRF112 address-family ipv6
  mdt mtu 8025
  mdt default ipv4 224.10.0.8
!
!
router pim vrf VRF112 address-family ipv4
  rp-address 112.101.122.102 list1
!
router pim vrf VRF112 address-family ipv6
  rp-address 1253::214 list2
!
end

```

VRF サービス要求の XML コンフィグレット

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf VRF112
address-family ipv6 unicast
import route-target 100:19890
import route-target 100:19891
export route-target 100:19890
exit
multicast-routing
vrf VRF112
mdt default 224.10.0.8
mdt data 224.10.0.9/32 threshold 8024
mdt mtu 8025
vrf VRF112 address-family ipv6
mdt default 224.10.0.8
mdt mtu 8025
router pim vrf VRF112 address-family ipv4 rp-address 112.101.122.102 list1
router pim vrf VRF112 address-family ipv6 rp-address 1253::214 list2
</Configuration>
</CLI>
<Set>
  <Configuration Source="CurrentConfig">
    <VRFTable>
      <VRF>
        <Naming>
          <Name>VRF112</Name>
        </Naming>
        <Create>true</Create>
        <AFI_SAFITable>
          <AFI_SAFI>
            <Naming>
              <AFI>IPv4</AFI>
              <SAFI>Unicast</SAFI>
              <Topology>default</Topology>
            </Naming>
            <Create>true</Create>
          </AFI_SAFI>
        </AFI_SAFITable>
      </VRF>
    </VRFTable>
  </Configuration>
</Set>

```

```

    <ImportRouteTargets>
      <RouteTargetTable>
        <RouteTarget>
          <Naming>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>19890</ASIndex>
          </Naming>
          <True>>true</True>
        </RouteTarget>
        <RouteTarget>
          <Naming>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>19891</ASIndex>
          </Naming>
          <True>>true</True>
        </RouteTarget>
      </RouteTargetTable>
    </ImportRouteTargets>
    <ExportRouteTargets>
      <RouteTargetTable>
        <RouteTarget>
          <Naming>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>19890</ASIndex>
          </Naming>
          <True>>true</True>
        </RouteTarget>
      </RouteTargetTable>
    </ExportRouteTargets>
  </BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>100</AS>
      </Naming>
      <VRFTable>
        <VRF>
          <Naming>
            <Name>VRF112</Name>
          </Naming>
          <VRFGlobal>
            <Exists>>true</Exists>
            <RouteDistinguisher>
              <Type>IPv4Address</Type>
              <Addr>112.101.112.101</Addr>
              <AddrIndex>1263</AddrIndex>
            </RouteDistinguisher>
          </VRFGlobal>
        </VRF>
      </VRFTable>
    </FourByteAS>
  </AS>
</BGP>

```

```
</Configuration>  
</Set>  
<Commit/>  
</Request>
```

コメント

- このサービス要求は、MPLS VPN PE_NO_CE ポリシーを使用します。
- このサービス要求には、コンフィグレットに示されているように、マルチキャスト IPv4 および IPv6 対応の VPN およびスタティック RP があります。

PE L3 MPLS VPN (IPv4 および IPv6 の独立 RT、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : IPv4 および IPv6 について独立 RT を使用する MPLS サービス要求
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : 各種。
 - ルーティング プロトコル = なし

コンフィグレット

PE

次のコード例は、注に示すように、指定した独立 RT 構成の CLI および XML コンフィグレット例を示します。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次の例は、指定した独立 RT 構成の CLI コンフィグレットを示します。

例 1 : [CERC Type] が [IPv4] に設定された CE-PE。

```
address-family ipv4 unicast
  import route-target
    7777:12345
  export route-target
    7777:12345
address-family ipv6 unicast
```



(注)

CERC が IPv6 とタグ付けされていた場合、RT は **ipv6 address-family** の下で構成されます。

例 2 : [CERC Type] が [IPv4+IPv6] に設定された PE-CE。

```
address-family ipv4 unicast
  import route-target
    7777:12345
  export route-target
    7777:12345
address-family ipv6 unicast
  import route-target
    7777:123456
  export route-target
    7777:123456
```



(注)

追加の IPv4 または IPv6 CERC が選択され、タグ付けされている場合、該当する **address-family CLI** の下の、上記のフォーマット内にそれらは増分的に追加されます。

例 3 : より多くの VPN の追加

より多くの VPN を設定に追加すると、以下に示すように、1 つの VPN 名が文字列 **-etc** を付加されてコンフィグレットに表示されます。

```
vrf V872:vpn2-etc
```

```

address-family ipv4 unicast
import route-target
64512:1005
!
export route-target
64512:1005
!
!

```

XML コンフィグレットの例

次の例は、[CERC Type] が [IPv4+IPv6] に設定された PE-CE の XML コンフィグレットです。キー XML タグは太字で示されています。

```

<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V6:Verve_VPN32
address-family ipv6 unicast
import route-target <?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
<Configuration>
vrf V6:Verve_VPN32
address-family ipv6 unicast
import route-target 64512:25428
import route-target 64512:25429
export route-target 64512:25428
exit
interface GigabitEthernet0/3/0/2.3039
ipv6 address 10::12/24
ipv6 address 10::15/32
ipv6 address 15::20/28
</Configuration>
</CLI>
  <Set>
    <Configuration Source="CurrentConfig">
      <VRFTable>
        <VRF>
          <Naming>
            <Name>V6:Verve_VPN32</Name>
          </Naming>
          <Create>true</Create>
          <AFI_SAFITable>
            <AFI_SAFI>
              <Naming>
                <AFI>IPv4</AFI>
                <SAFI>Unicast</SAFI>
                <Topology>default</Topology>
              </Naming>
              <Create>true</Create>
              <BGP>
                <ImportRouteTargets>
                  <RouteTargetTable>
                    <RouteTarget>
                      <Naming>
                        <Type>AS</Type>
                        <AS>64512</AS>
                        <ASIndex>254288</ASIndex>
                      </Naming>
                      <True>true</True>
                    </RouteTarget>
                  </RouteTargetTable>
                </ImportRouteTargets>
              </BGP>
            </AFI_SAFI>
          </AFI_SAFITable>
        </VRF>
      </VRFTable>
    </Configuration Source="CurrentConfig">
  </Set>
</CLI>
</Request MajorVersion="1" MinorVersion="0">
</Request MajorVersion="1" MinorVersion="0">

```

```
        <Naming>
          <Type>AS</Type>
          <AS>64512</AS>
          <ASIndex>254299</ASIndex>
        </Naming>
        <True>true</True>
      </RouteTarget>
    </RouteTargetTable>
  </ImportRouteTargets>
<ExportRouteTargets>
  <RouteTargetTable>
    <RouteTarget>
      <Naming>
        <Type>AS</Type>
        <AS>64512</AS>
        <ASIndex>254288</ASIndex>
      </Naming>
      <True>true</True>
    </RouteTarget>
  </RouteTargetTable>
</ExportRouteTargets>
</BGP>
</AFI_SAFI>
</AFI_SAFITable>
</VRF>
</VRFTable>
</Configuration>
</Set>
</Request>
```

コメント

- なし。

PE L3 MPLS VPN (Bundle-Ether Interface、IOS XR)

設定

- サービス : L3 MPLS VPN
- 機能 : バンドルイーサネット インターフェイスを使用した MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : Bundle-Ether147
 - ルーティング プロトコル = なし

コンフィグレット

PE

次のコード例は、注に示すように、バンドルイーサネット インターフェイスの CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に示すのは、バンドルイーサネット インターフェイス機能の CLI コンフィグレット例です。コンフィグレットは PE デバイスに展開されます。

```
interface Bundle-Ether147
  description Bun
!
interface Bundle-Ether147.369
  description subbun
  vrf ISC521
  ipv4 address 66.174.25.3 255.255.255.254
  ipv6 address 2001:4888:10:100::3/64
  dot1q vlan 269
!
```

XML コンフィグレットの例

次に示すのは、バンドルイーサネット インターフェイス機能の XML コンフィグレット例です。コンフィグレットは PE デバイスに展開されます。

```
<InterfaceConfiguration>
  <Naming>
    <Active>act</Active>
    <Name>Bundle-Ether147</Name>
  </Naming>
  <InterfaceVirtual>true</InterfaceVirtual>
  <Description>Bun</Description>
</InterfaceConfiguration>

<InterfaceConfiguration>
  <Naming>
    <Active>act</Active>
    <Name>Bundle-Ether147.369</Name>
  </Naming>
  <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
  <Description>subbun</Description>
  <VRF MajorVersion="3" MinorVersion="3">ISC521</VRF>
  <IPV4Network MajorVersion="5" MinorVersion="0">
```

```
<Addresses>
  <Primary>
    <IPAddress>66.174.25.3</IPAddress>
    <Mask>255.255.255.254</Mask>
  </Primary>
</Addresses>
</IPV4Network>
<VLANSubConfiguration MajorVersion="2" MinorVersion="1">
  <VLANIdentifier>
    <VlanType>VLANTypeDot1q</VlanType>
    <FirstTag>269</FirstTag>
  </VLANIdentifier>
</VLANSubConfiguration>
</InterfaceConfiguration>
```

コメント

- なし。

PE L3 MPLS VPN (Outgoing Interface + Next Hop IP Address、Static Route Configuration、IOS XR、および IOS)

設定

- サービス : L3 MPLS VPN
- 機能 : スタティック ルーティング プロトコルを使用し、発信インターフェイスとネクスト ホップの IP アドレスを指定する MPLS サービス要求。
- デバイス設定 :
 - PE は、IOS XR バージョン 3.7.1[00] の iscind-12010-1 (GSR) です。
インターフェイス : 各種。
 - ルーティング プロトコル = Static。

コンフィグレット

PE

次のコード例は、CLI および XML コンフィグレットを示しています。すべてのコンフィグレットが PE デバイスに展開されます。

CLI コンフィグレットの例

次に、IOS デバイスの CLI コンフィグレット例を示します。

```
router bgp 64512
address-family ipv4 vrf V14:July7_VPN
redistribute static
exit-address-family
!
ip route vrf V14:July7_VPN 15.18.16.17 255.255.255.255 GigabitEthernet0/3/0/0 10.12.16.19
78
```

次に、IOS XR デバイスの CLI コンフィグレット例を示します。

```
router static
vrf V7:techm_vpn
address-family ipv4 unicast
12.23.34.34/32 GigabitEthernet0/3/0/2 10.14.54.18 45
!
address-family ipv6 unicast
15:16:17:13:14:15:17:18/128 GigabitEthernet0/3/0/2 18:12:13:14:16:13:16:14
!
```

XML コンフィグレットの例

次に、IPv4 アドレス ファミリの XML コンフィグレット例を示します。

```
<VRF>
  <Naming>
    <VRFFName>V1:VPN_June22</VRFFName>
  </Naming>
  <AddressFamily>
    <VRFIPv4>
      <VRFUnicast>
        <VRFPrefixTable>
          <VRFPrefix>
            <Naming>
              <Prefix>
```

```

        <IPV4Address>10.77.66.58</IPV4Address>
      </Prefix>
    <Length>32</Length>
  </Naming>
</VRFRouteTable>
<VRFNextHopInfoTable>
  <VRFNextHopInfo>
    <Naming>
      <Interface>GigabitEthernet0/3/0/0</Interface>
    <Address>
      <IPV4Address>10.12.16.19</IPV4Address>
    </Address>
    </Naming>
    <Metric>48</Metric>
  </VRFNextHopInfo>
</VRFNextHopInfoTable>
</VRFRouteTable>
</VRFPrefix>
</VRFPrefixTable>
</VRFUnicast>
</VRFIPV4>
</AddressFamily>
</VRF>

```

次に、IPv6 アドレス ファミリの XML コンフィグレット例を示します。

```

<VRF>
  <Naming>
    <VRFName>V39:techm_vpn</VRFName>
  </Naming>
  <AddressFamily>
    <VRFIPV6>
      <VRFUnicast>
        <VRFPrefixTable>
          <VRFPrefix>
            <Naming>
              <Prefix>
                <IPV6Address>10::19</IPV6Address>
              </Prefix>
              <Length>128</Length>
            </Naming>
          <VRFRouteTable>
            <VRFNextHopInfoTable>
              <VRFNextHopInfo>
                <Naming>
                  <Interface>GigabitEthernet0/3/0/0</Interface>
                <Address>
                  <IPV6Address>45::10</IPV6Address>
                </Address>
                </Naming>
                <Metric>75</Metric>
              </VRFNextHopInfo>
            </VRFNextHopInfoTable>
          </VRFRouteTable>
        </VRFPrefix>
      </VRFPrefixTable>
    </VRFUnicast>
  </VRFIPV6>
</AddressFamily>
</VRF>

```

コメント

- なし。

MPLS VPN のトラブルシューティング

この項では、MPLS VPN のトラブルシューティングに関する情報を示します。

一般的なトラブルシューティングのガイドライン

プロビジョニングに失敗した場合の一般的なトラブルシューティングについては、次の手順を実行します。

-
- ステップ 1** 失敗したサービス要求を特定し、[Details] に移動します。
- a. これを行うには、[Service Request Editor] に移動し、[Details] をクリックします。
最も注目すべき項目はステータス メッセージです。これは何が起きたかを正確に示しています。
 - b. ステータス メッセージに監査が失敗したと表示される場合は、[Audit] ボタンをクリックして監査の正確にどの部分が失敗したのかを見つけます。
- ステップ 2** トラブルシューティング手順のステップ 1 で、何が起こったのかを明確に把握できない場合は、タスクマネージャのログを使用して問題を特定します。
- a. これを行うには、[Monitoring] > [Task Manager] > [Logs] > [Task Name] を選択します。
 - b. このログに多くの情報があります。問題を特定するために、フィルタを使用できます。ログレベルまたはコンポーネントでフィルタリングする場合は、通常、関連する情報の量を減らして、問題を特定するために把握する必要のある情報に焦点を当てることができます。
- ステップ 3** いくつかの一般的な質問および問題の詳細については、この付録の「よくあるご質問」(P.5-254) の項を参照してください。
-

開発エンジニアリング用のログの収集

「一般的なトラブルシューティングのガイドライン」(P.5-253) で説明されているトラブルシューティングの手順を実行します。問題のトラブルシューティングまたは特定に失敗した場合のために、この項では開発エンジニアがトラブルシューティングするためにログを収集する方法について説明します。



ヒント

ログは、MPLS VPN とレイヤ 2 VPN の両方に適用されます。

DCPL には、**Provisioning.Service.mpls.saveDebugData** と呼ばれるプロパティがあります。このプロパティが **True** に設定されている場合、サービス要求を展開するたびに、一時ディレクトリが **PRIMEP_HOME/tmp/mppls** に作成されます。

ディレクトリには、タイムスタンプとともに、プレフィックスとして付加されているサービス要求のジョブ ID が含まれています。このディレクトリには、アップロードされたコンフィギュレーションファイル、XML 形式のサービス パラメータ、およびプロビジョニングと監査の結果が含まれます。

デフォルトは **true** に設定されています。

確認するには、次の手順を実行します。

-
- ステップ 1** [Administration] > [Control Center] を選択して、プロパティを見つけます。
[Control Center Hosts] ページが表示されます。

- ステップ 2** 対象のホストのチェックボックスをオンにします。
[Hosts] ページのメニュー ボタンがイネーブルになります。
- ステップ 3** [Config] をクリックします。
[Host Configuration] ウィンドウが表示されます。
- ステップ 4** [Provisioning] > [mpls] と移動します。
- ステップ 5** デバッグのために、[saveDebugData] をクリックして一時ディレクトリにデータを保存します。
-

よくあるご質問

MPLS VPN のプロビジョニングに関する FAQ のリストを次に示します。

MPLS のプロビジョニング ワークフローとは何ですか。

次に示すタスクは、MPLS プロビジョニング ワークフローを示します。この項では、オペレータがタスク マネージャなどの発信者を使用してサービス要求を展開することを前提としています。

1. プロビジョニング ドライバ (ProvDrv) が、展開するサービス要求を取得します。
2. サービス要求で、プロビジョニング ドライバは、どのデバイスが関係するかを推測します。
3. 最新のルータ コンフィギュレーションを取得して、プロビジョニング ドライバが **Generic Transport Library (GTL) /Device Configuration Service (DCS)** に最新のルータ コンフィギュレーションをアップロードするように伝達できるようにする必要があります。結果は、サービス モジュールで使用されます。
4. プロビジョニング ドライバはサービスとデバイス タイプに基づいて、どのサービス モジュールが関連するのかを判別します。
5. **Provisioning Driver** は、サービス目的をリポジトリに問い合わせます。プロビジョニング ドライバは、アップロードされた設定とともにサービス モジュールにサービス目的を送信します。
6. 設定とサービス目的に基づいて、サービス モジュールがコンフィグレットを生成し、プロビジョニング ドライバに適切なコンフィグレットを返します。
7. プロビジョニング ドライバは **GTL/DCS** に信号を送信し、コンフィグレットをターゲット ルータにダウンロードします。
8. **Provisioning Driver** は、ダウンロード結果を含む更新結果をリポジトリに送信します。その後リポジトリは、その状態を更新します。

上記の手順で説明した用語の定義。

- **デバイス設定サービス (DCS)** : コンフィギュレーション ファイルのアップロードとダウンロードを担当します。
- **汎用転送ライブラリ (GTL)** : ターゲット デバイスにコンフィグレットをダウンロードして、コンフィギュレーション ファイルをターゲット デバイスからアップロード、し、ターゲット デバイスでコマンドを実行して、ターゲット デバイスをリロードするための API を提供します。

このライブラリは、トランスポート プロバイダー (DCS) と **Provisioning Driver**、**Auditor**、**Collect Config** 動作、**Exec** コマンドなどのクライアント アプリケーション間にレイヤを提供します。GTL の主な役割は、ターゲットに関する具体的な情報をリポジトリおよびプロパティファイルから収集し、トランスポート プロバイダー (DCS) に渡すことです。

- **ProvDrv (Provisioning Driver)** : ProvDrv は複数のデバイスで 1 つ以上のサービスの展開を担当するタスクです。

ProvDrv はすべてのサービスに共通のタスクを実行します。たとえば、デバイスからのコンフィギュレーション ファイルのジャスト イン タイム アップロード、Data Driven Provisioning (DDP) エンジンの起動、DDP エンジンから収集されたコンフィグレットまたは監査レポートの取得、およびデバイスへのコンフィグレットのダウンロードなどです。

- **リポジトリ** : リポジトリにはさまざまな IP Solution Center データが保存されています。Prime Provisioning のリポジトリは Sybase または Oracle を使用します。
- **サービス モジュール** : サービス タイプに基づいてコンフィグレットを生成します。

即時展開のためにスケジュール設定したのにタスクが実行されなかった場合、どうすればいいですか。

この問題は、Prime Provisioning サーバのいずれかが停止したか、ディセーブルになっているために発生した可能性があります。

すべての Prime Provisioning サーバのステータスを確認するには、次の手順を実行します。

- ステップ 1** [Administration] > [Control Center] > [Hosts] と移動して、[Host Configuration] ダイアログを開きます。
[Hosts] ページが表示されます。
- ステップ 2** 対象のホストのチェックボックスをオンにします。
[Hosts] ページのメニュー ボタンがイネーブルになります。
- ステップ 3** [Servers] を選択します。
図 5-38 に示されているように、[Server Status] ページが表示されます。

図 5-38 Prime Provisioning サーバ状態

#	<input type="checkbox"/>	Name	State	Generation	Start Time	Successful Heartbeats	Missed Heartbeats
1	<input type="checkbox"/>	rnpoller	started	1	Nov 21 07:37:07 AM EST	690	0
2	<input type="checkbox"/>	dbpoller	started	1	Nov 21 07:37:07 AM EST	682	0
3	<input type="checkbox"/>	httpd	started	1	Nov 21 07:37:12 AM EST	685	0
4	<input type="checkbox"/>	rgserver	disabled	11	Nov 21 08:00:25 AM EST	0	0
5	<input type="checkbox"/>	crserver	started	1	Nov 21 07:37:12 AM EST	690	0

Rows per page: 10 Page 1 of 1

Start Stop Restart Logs OK

- ステップ 4** Prime Provisioning サーバで、**wdclient status** コマンドを使用してサーバの詳細な状態を確認します。

サービス要求が [Wait Deployed] 状態になっている場合、どのようにすればよいですか？

これは、アクセス方式として、Cisco Configuration Engine を使用するよう設定されたデバイスに関係しています。デバイスがオフラインで、コンフィグレットがそれ自体のために生成された場合、サービス要求は [Wait Deployed] 状態に移行します。デバイスがオンラインになるとすぐに、コンフィグレットのリストがダウンロードされ、デバイスのステータスが変更されます。

サービス要求が [Failed Audit] 状態になっている場合、どのようにすればよいですか？

少なくとも 1 つのコマンドがデバイスから欠落しています。次の操作を行ってください。

-
- ステップ 1** Prime Provisioning のユーザ インターフェイスから、[Service Request Editor] > [Audit] > [Audit Config] と移動します。
 - ステップ 2** デバイスごとに欠落しているコマンドのリストを確認します。
 - ステップ 3** デフォルト値を持つ属性がある、欠落したコマンドがないか確認します。
-

サービス要求が展開前と同じ状態の場合はどうすればいいですか。

展開後に、サービス要求の状態が以前の展開されていないときの状態 (Request、Invalid、または Pending) のままである場合、プロビジョニング タスクが正常に完了しなかったことを示しています。「一般的なトラブルシューティングのガイドライン」(P.5-253) で説明されている手順に従って、サービス要求が失敗した理由を探します。

次のメモリ不足に関するエラー「OutOfMemoryError?」を受け取った場合、どのようにすればいいですか？

次の操作を行ってください。

-
- ステップ 1** [Administration] > [Control Center] > [Hosts] と選択して、[Host Configuration] ダイアログを開きます。
[Hosts] ページが表示されます。
 - ステップ 2** 対象のホストのチェックボックスをオンにします。
[Hosts] ページのメニュー ボタンがイネーブルになります。
 - ステップ 3** [Config] をクリックします。
[Host Configuration] ウィンドウが表示されます。
 - ステップ 4** [watchdog] > [servers] > [worker] > [java] > [flags] と移動します。
 - ステップ 5** 次の属性を変更します。
[Xmx256M] 属性を [Xmx384M] または [Xmx512M] に変更します。
-

Prime Provisioning が VPN のルート ターゲット インポート/エクスポートを削除しない場合は、どうすればいいですか。

シナリオ: 新しい VPN に関連付けられるように MPLS サービス要求が編集されると、1 つのインターフェイスにのみ関連付けられている場合のみ、古い VPN は削除されます。サービス要求とカスタマーの関係は、VPN を通ります。サービス要求のオプションの [Customer] フィールドには、設定に関する関係はありません。たとえば、*custA* の MPLS サービス要求が *vpnB/cercB* とともに存在するが、*vpnA/cercA* を反映するように変更する必要がある場合、*vpnA/cercA* を使用するようにサービス要求を変更しても、複数のインターフェイスが同じ VRF に関連付けられている場合、*vrfB* から *vpnB* のルート ターゲットは削除されません。

推奨される処理のとおり、同じシナリオを 1 つのインターフェイスだけが *vrfB* を参照して実行している場合は、Prime Provisioning によって *vrfB* が削除されて、ルート ターゲット *A* で *vrfA* が適切に追加されます。

追加の CE ループバック インターフェイスのプロビジョニングを選択すると、サービス要求が [Invalid] に移行するのはなぜですか。

IP アドレスの自動選択のオプションがサービス要求に対して選択されたが、/32 IP アドレス プールが定義されていない可能性があります。このサービス要求に対して定義した IP アドレスと IP アドレス プールに確実に互換性があることを確認します。

サービス要求を保存するときに、「CERC not initialized」というメッセージが表示されるのはなぜですか。

参加するリンクの CERC を選択する必要があります。サービス要求をチェックして、CERC が選択されているかどうかを確認してください。

なぜ VLAN ID プールの作成には、アクセス ドメインが必要なのですか。

VLAN ID プールは、アクセス ドメインに関連付けられています。アクセス ドメインはブリッジドメインをモデル化します。このため、VLAN ID はブリッジ ドメインで一意である必要があります。

PE-POP はアクセス ドメインに関連付けられる必要があります。アクセス ドメインは、複数の PE-POP と関連付けることができます。

ページング テーブルで、1 つのチェックボックスのみがオンになっていても、[Edit] と [Delete] オプションがディセーブルになるのはなぜですか。

前のウィンドウで 1 つ以上のチェックボックスが選択されている可能性があります。

なぜ MPLS VPN または L2VPN ポリシーを編集できないのですか。

サービス要求がポリシーに関連付けられている場合、そのポリシーは編集できません。

CERC を作成できません。これはなぜですか。

ルート ターゲットを手動で指定しない限り、CERC を作成する前にルート ターゲット プールを定義する必要があります。

PE、CE、および PE-CLE デバイスの間でコンフィグレットのダウンロード順序を変更するにはどのようにすればいいですか。

Provisioning.Services.mpls.DownloadWeights.* という名前のプロパティを使用して、PE、CE、PE-CLE、および MVRF CE のデバイス タイプのダウンロード順序を指定できます。

たとえば、CE にダウンロードされる前にコンフィグレットが PE にダウンロードされるようにするには、**Provisioning.Services.mpls.DownloadWeights.weightForPE** プロパティに CE よりも大きい重み値を設定します。

プロパティ **Provisioning.Service.mpls.reapplyIpAddress** は何を行いますか。

デコミッションされたサービス要求の展開時にこのプロパティが True に設定されている場合、このプロパティは CE および PE 上の IP アドレスをルータでそのまま保持し、CE への IPv4 接続を維持します。

少なくとも 1 つの PE-CLE デバイスを介して CE と PE 間のマルチホップ NPC を作成するとき、いくつかの追加 NPC が作成されるのはなぜですか。

オペレータが同じ情報を再入力する必要をなくすために、IP Solution Center によって余分な NPC が作成されます。CE は PE-CLE デバイスに接続できるようになったため、PE-CLE と PE NPC 間のリンクを介した新しい CE と PE 間を接続する新しい NPC が作成されます。

サービス要求のプロビジョニング中に、[Interface selection] リスト ボックスにデバイス上のインターフェイスのリスト全体が表示されないのはなぜですか。

これは、特定のインターフェイス タイプがサービス ポリシーで指定されていることが原因です。これが原因の場合、指定されたインターフェイス タイプのインターフェイスのみが表示されます。

メッセージ「loopback address missing」が表示されてサービス要求が [Invalid] に移行するのはなぜですか。

これは、レイヤ 2 VPN の問題です。

これは、PE 間の疑似回線にピアを確立するために必要なループバック アドレスが Prime Provisioning の PE-POP オブジェクトに定義されていないことが原因です。

MPLS ポリシーの [Allocate New Route Distinguisher] チェックボックスは何のために使用するのですか。

従来の製品の「VPNSC」とは異なる、Prime Provisioning に実装された動作の変更がいくつかありました。VPNSC では、VRF は PE を中心にしていました。このため、その動作は、PE ルータ上の VPN ごとに設定される新しい VRF に対応していました。この動作は VRF を VPN 中心にするために、Prime Provisioning で変更されました。大部分のルーティングで、iBGP ロード バランシングを行う場合を除き、VRF/ルート識別子 (RD) は PE のみを重視します。したがって、すべての PE ルータで単一の VPN に同じ値を使用することが可能です。これは、トラブルシューティング、レポートなどを行うユーザにとって、より便利な機能です。

iBGP ロード バランシングを行う場合のユーザの柔軟性を向上させ、カスタム ソリューションとニーズに対応するために、Prime Provisioning では 2 つのオプションを使用できます。1 つは [VRF and RD Overwrite] であり、もう 1 つは [Allocate New Route Distinguisher] です。[VRF and RD Overwrite] は

文字どおりに機能します。これを使用すると、ユーザはプロビジョニング中のリンクに VRF 名および RD 値を強制できます。これは Prime Provisioning によってプロビジョニングされなかった既存 VRF に参加するのに役立ちます。



(注)

[VRF and RD Overwrite] 属性の下にあるサブ属性（つまり、[VRF Name] および [RD Value] 属性）に値を指定し、MPLS サービス要求を保存すると、これらの両方のフィールドがディセーブルになり、編集できなくなります。[VRF Name] および [RD Value] のデフォルト値を変更すると、現在実行中のサービス要求を変更またはディセーブルにする可能性があるために、この動作は導入されました。したがって、展開済みサービス要求でこれらの値を変更する必要がある場合の回避策は、そのサービス要求をデコミッションおよび削除し、新規サービス要求を作成することです。まだ展開されていない新規サービス要求の場合、サービス要求を強制的に削除してから新規値を使用して新規サービスを作成する必要があります。

2 つめのオプションは [Allocate New Route Distinguisher] です。これは、PE ルータに初めて新しい VRF と RD を設定する場合にのみ有効です。これは、PE ルータごとに個別の VRF の VPNSC の動作を模倣します。次に、既存 VPNSC リポジトリが含まれない場合の新しい RD のルールを示します。

[Allocate New Route Distinguisher] がイネーブルである場合

- その PE に一致する VRF 設定がない場合は、新しい VRF を作成します。
- その PE に一致する VRF コンフィギュレーションがある場合は再使用します。

[Allocate New Route Distinguished] がディセーブルである場合

- PE に関係なく、PE のすべての範囲にわたって最初に一致する VRF 設定を検出し、設定された PE でこの VRF が検出された場合、それを再利用します。PE で検出されない場合は、作成します。
- 注：すでに別の PE ルータで設定されている VRF をサービス要求が取得する可能性があります。

VPNSC の下に設定された既存 VRF では、VPNSC で [Allocate New Route Distinguisher] フラグが常にオンになっていたことが問題でした。このため、フラグを再度適用すると、Prime Provisioning は最初に PE の既存の VRF を検索します。その VRF（この場合、VPNSC でプロビジョニングされたもの）を使用します。VRF が見つからない場合、Prime Provisioning は新しい VRF を作成します。古い VPNSC リンクに新しいリンクを追加するときに、[Allow New Route Distinguisher] フラグがオンにならない場合、Prime Provisioning はネットワーク全体に設定されている、最初に一致する VRF を検索します。PE にこの VRF が存在しない場合、Prime Provisioning はルータにそれを作成します。

使用例

1. レガシー（VPNSC）VRF とのリンクを既存の PE に追加するときに、[Allocate New Route Distinguisher] オプションを選択する必要があります。
2. 新しい PE にリンクを追加するときに、この VPN で前に設定されていない VRF/RD 値が必要な場合は、[Allocate New Route Distinguisher] オプションを選択する必要があります。
3. 新しいリンクを新しい PE に追加するときに、ネットワークの別の場所で使用されている VRF/RD 値を再利用する場合は、[VRF and RD Overwrite] オプションを選択する必要があります。
4. 不正な VRF/RD 値（つまり、以前に VPNSC でプロビジョニングされたものと一致しないもの）を持つリンクをプロビジョニングする場合は、リンクを変更して、再展開する必要があります。変更時に、[VRF and RD Overwrite] オプションを選択し、VPNSC で使用したのと同じ VRF/RD 値を指定する必要があります。
5. 複数の PE 間で iBGP ロード バランシングの展開を計画している場合、[Allocate New Route Distinguisher] オプションを常にイネーブルにする必要があります。これにより、ロード バランシングの要件を満たすための固有の RD 条件が満たされます。

標準 UNI ポートを使用する MPLS サービス要求はどのようにして CDP パケットを許可できますか。

デフォルトで、MPLS サービス要求はレイヤ 2 コントロールプレーンでの BPDU 処理のアクセスを制限する標準 UNI の MAC ACL を作成します。作成される ACL は次のようになります。

```
interface FastEthernet0/15
mac access-group ISC-$name in
mac access-list extended ISC-$name

deny any host 0180.c200.0000 ==> PVST, MSTP, RSTP, and STP
deny any host 0100.0ccc.cccd ==> PVST+
deny any host 0100.0ccc.cccc ==> CDP, VTP, DTP, UDLD, PAgP
deny any host 0100.0ccd.cdd0 ==> CDP,VTP,STP
permit any any
```



(注)

「==>」の後に表示されているテキストは、MAC ACL の一部ではありません。これは、各 MAC アドレスによってブロックされるプロトコルのリストです。

代わりに、MPLS サービス要求が作成されたときに、リンク属性を編集してから次の手順を実行することもできます。

- ステップ 1** [Use Existing ACL Name] をイネーブルにします。
これは、[Port-Based ACL Name] オプションをイネーブルにします
- ステップ 2** 空または存在しない MAC ACL の名前を入力します。

MPLS サービス要求が展開されると、MAC ACL をフィルタリングするデフォルト BPDU を発行しなくなります。代わりに、**access-group** コマンドを空の ACL をポイントする UNI インターフェイスに作成します。例：

```
interface FastEthernet0/15 mac access-group {$PACL_NAME} in
```

MAC ACL は作成されません。

L3 VPN を作成するときに、2 つまたは 3 つのアドレス プールを使用できますか。

IP プール 10.10.10.0/24 を領域に割り当て、PE がその領域に割り当てられていると想定します。ここで、1 人のカスタマーが自身の LAN 範囲内で同じサブネットを使用すると仮定します。これにより、PE-CE リンクに対して別のサブネットを使用しなければなりません。Prime Provisioning はこれをどのように処理するでしょうか。唯一の方法は、自動選択を使用せずに手動で行うことです。Prime Provisioning は異なるカスタマーに異なるアドレス プールの使用をサポートしていません。

その他の関連する問題は次のとおりです。IP アドレスの Prime Provisioning プールで使用されているものと同じ IP アドレスをカスタマーが自分の LAN セグメント内で使用している場合、これにより問題が発生します。このため、PE-CE の IP アドレスに対して複数のサブネットを持ち、最も適切なもの（カスタマーが使用する IP アドレスと競合しないもの）を使用する必要があります。IP アドレス プールを作成すると、リポジトリは範囲を認識し、プールの一部として、重複する IP アドレスを使用することはできなくなります。Prime Provisioning には、同じ PE 内で使用される異なるプールに対するサポートはありません。Prime Provisioning を使用して複数のプールを作成できますが、プロバイダー領域に基づいて 1 つのみを使用できます。Prime Provisioning は、最初のプールが IP アドレスをすべ

て使用すると、次の順番のものを選択します。自動選択するプールを選択するための選択メカニズムはありません。IP アドレスがプールと重複しないかぎり、手動で追加された IP アドレスを使用できません。

サービス要求がデコミッションされた後で、MPLS IP アドレス プールからの IP アドレスは使用可能なプールにいつ戻されますか。

サービス要求がデコミッションされると、サービス要求が [Deployed] 状態になった後、IP アドレスは使用可能なプールに戻ります。Prime Provisioning は、約 24 時間、返された IP アドレスを新しいサービス要求が再利用できないようにします。サービス要求がデコミッションされてから削除されたときも同じ動作が適用されます。

サービス要求がデコミッションされるときに、Prime Provisioning によって一部のルータ BGP/EIGRP コマンドが削除されないのはなぜですか。

Prime Provisioning は、VRF が削除された場合にのみ、ルータ BGP または EIGRP 設定からアドレスファミリー CLI を削除します。EIGRP ルータの場合、Prime Provisioning によって設定されていない他の CLI が存在する可能性があるため、このプロセスは削除されません。これは、特にネットワークステートメントが Prime Provisioning の外で追加されたときに当てはまります。Prime Provisioning は、redistribute コマンドがリンク用に特に作成されていない可能性があるため、EIGRP で他のルーティングプロトコルからの再配布を削除しません。

Prime Provisioning は、VRF が削除される場合に、ルータの OSPF プロセスのみを削除します。これは、PE のみに適用されます。CE の場合、ネットワークステートメントが削除されると、ルータ OSPF が削除されます。Prime Provisioning はルータ BGP とルータ EIGRP のどちらも削除しません。

プラットフォームまたは IOS（または IOS XR）バージョンが Q-in-Q（たとえば WS-X6724-SFP）をサポートしていない場合、どのようになりますか。

サービス要求は [Failed Deploy] 状態になり、ログ ファイルは次のようになります。

IOS の場合：

```
SEVERE Provisioning.ProvDrvDownload failed for device NPE-1: 315 : Error downloading
cmd=[encapsulation dot1q 158 second-dot1q 1510], response=[encapsulation dot1q 158
second-dot1q 1510^
% Invalid input detected at '^' marker.NPE-1(config-subif)#]
```

IOS XR の場合：

```
SEVERE Provisioning.ProvDrvDownload failed for device NPE-1: 315 : Error downloading
cmd=[encapsulation dot1q 158 1510], response=[encapsulation dot1q 158 1510^
% Invalid input detected at '^' marker.NPE-1(config-subif)#]
```

サービス要求を編集し、2 つめの VLAN ID をディセーブルにして、再配布します。

ハードウェア/IOS が Q-in-Q サポートしているのに、Prime Provisioning が Q-in-Q をプロビジョニングしないのはなぜですか。

発生する可能性のあるエラー

- ポートがスイッチポート モードです。解決策：ポート設定を確認して、必要に応じて **no switchport** を実行します。
- SVI フラグがイネーブルです。解決策：SVI をディセーブルにします。

既存のサブインターフェイス（Q-in-Q）と SVI が同じインターフェイスにあるポートが INVALID になるのはなぜですか。

1 つのサブインターフェイスのみで SVI がイネーブルになるようにサービス要求を変更すると、そのサービス要求は [Deployed] 状態になります（IOS デバイスの場合）。同じインターフェイス（つまり、既存のサブインターフェイス）で SVI をイネーブルにして新しいサービス要求を作成すると、そのサービス要求は [Invalid] 状態になります。

同じインターフェイス/ポートの下に、dot1q と Q-in-Q の単一のサービス要求を展開できますか。

はい。

Q-in-Q で展開されたサービス要求から 2 つめの VLAN ID をどのようにして削除できますか。

サービス要求を編集/変更し、2 番めの VLAN ID エントリを削除してから、サービス要求を再展開する必要があります。次のようなコンフィグレットが作成されます。

```
interface GigabitEthernet2/0/15.158
no encapsulation dot1q
encapsulation dot1q 158
ip address 10.1.1.105 255.255.255.252
```

VRF

2 つの VPN ルーティング/転送（VRF）モデルがあります。

従来の VRF モデルでは、オペレータは最初に VPN オブジェクトを作成してから、それを MPLS VPN リンクに関連付けます。必要な VRF 情報は、MPLS VPN リンクをプロビジョニングときに生成され、展開されます。VRF 情報が削除されるのは、VRF に関連付けられた最後のリンクがデコミッションされた場合だけです。

独立 VRF の管理機能を使用して、物理リンクとは独立して、VRF 情報をプロビジョニングすることができます。これにより、MPLS VPN リンクとは関係なく VRF オブジェクトの作成、変更、および削除を実行できます。これには、次の利点があります。

- VRF 情報およびテンプレートは、インターフェイスと関連付けることなく、PE デバイスで直接展開できます。
- VRF 情報は、VRF 向けのリンクなしで存在できます。
- VRF オブジェクトは、リンクに関連付けられている場合でも変更できます。
- Route Target (RT; ルート ターゲット) は、停止せずに追加および削除できます。

物理リンクとは独立した VRF の管理には、次の作業が含まれます。

- VRF オブジェクトの作成、変更、削除。
- VRF サービス要求と呼ばれる、新しいタイプのサービス要求の作成、変更、展開、デコミッション、および削除。
- サービス ポリシーとサービス要求を介した MPLS VPN リンクを持つ、展開済み VRF オブジェクトの使用。
- 従来の MPLS VPN サービス要求の独立 VRF モデルへの移行。

この項では、独立 VRF オブジェクトを作成して管理する方法について説明します。ここでは、次の内容について説明します。

- 「VRF の作成」(P.5-263)
- 「VRF の編集」(P.5-265)

VRF の作成

VRF オブジェクトを作成した後、次に説明されているように、VRF サービス要求を使用してプロビジョニングできます。『Cisco Prime Provisioning 6.3 User Guide』

VRF の作成手順は、次のとおりです。

-
- ステップ 1** [Inventory] > [Logical Inventory] > [VRF] を選択します。
- ステップ 2** [Create] をクリックします。
- [Create VRF] ウィンドウが表示されます。
- ステップ 3** 必要に応じて、VRF のフィールドに入力します。
- a. [Name] (必須) : VRF の名前を入力します。任意の名前を使用できます。この名前は PE デバイスに直接展開されます。
 - b. [Provider] (必須) : この VRF に関連付けられたプロバイダーを選択するには、[Select] を選択します。
 - c. プロバイダーのリストから、適切なプロバイダーを選択し、[Select] をクリックします。
 - d. [Description] (任意) : 選択した場合は、説明を入力します。
 - e. [Route Targets] (必須) : [Select] ボタンをクリックします。
 - f. ルート ターゲットのリストから、適切なルート ターゲットを 1 つだけ選択し、[Select] をクリックします。
 - g. [Import RT List] : VRF にインポートする 1 つ以上のルート ターゲット (RT) を入力します。複数の RT の場合は、カンマで RT を区切ります。RT リストは、たとえば 100:120,100:130,100:140 のようになります。

- h. [Export RT List] : VRF からエクスポートされる 1 つ以上のルート ターゲットを入力します。複数の RT の場合は、カンマで RT を区切ります。
- i. [Import Route Map] : デバイスで定義したルート マップの名前を入力します。Prime Provisioning は、VRF のプロビジョニング中にこの名前を検証し、ルート マップが定義されていない場合、エラーを生成します。
- j. [Export Route Map] : デバイスで定義したルート マップの名前を入力します。Prime Provisioning は、VRF のプロビジョニング中にこの名前を検証し、ルート マップが定義されていない場合、エラーを生成します。
- k. [Maximum Routes] : VRF にインポートできるルートの最大数を示す整数を指定します。IOS デバイスの範囲は 1 ~ 4294967295 であり、IOS XR デバイスの範囲は 32 ~ 2000000 です。デバイス タイプの特定の検証は、サービス要求の作成中に実行されます。
- l. [Threshold] : しきい値を 1 ~ 100 のパーセントで指定します。このパーセンテージを超えると、警告メッセージが表示されます。これは、IOS デバイスでは必須で、IOS XR デバイスでは任意です。デバイス タイプの特定の検証は、サービス要求の作成中に実行されます。
- m. [RD Format] : ドロップダウン リストに 2 つの選択肢があります。ルート識別子に **RD_AS** を選択し、たとえば 100:202 のような自律システム (AS) フォーマットにします。それ以外の場合は、[RD_IPADDR] を選択して、RD を RD_IPADDRESS 形式 (たとえば、10.2.2.3:1021) にします。
- n. [RD] (必須) : ルート識別子 (RD) を手動で指定するか、または [Autopick RD] チェックボックスをオンにして、Prime Provisioning がルート識別子プールから RD を自動的に選択するようにします (ルート識別子プールが設定されている場合)。
- o. [Enable IPv4 Multicast] : マルチキャスト VRF の展開は、IPv4 展開に対してのみサポートされません。マルチキャストがイネーブルの場合は、ルート ターゲットは必須です。IPv4 マルチキャスト VRF の展開をイネーブルにするには、チェックボックスをオンにします。
- p. [Enable IPv6 Multicast] : マルチキャスト VRF の展開は、IPv6 展開に対してのみサポートされません。マルチキャストがイネーブルの場合は、ルート ターゲットは必須です。IPv6 マルチキャスト VRF の展開をイネーブルにするには、チェックボックスをオンにします。
- q. [Enable Auto Pick MDT Addresses] (任意) : このチェックボックスをオンにして、マルチキャストのリソース プールから [Default MDT Address] および [Default MDT Subnet] の値を使用します。
- r. [Default MDT Address] : [Enable Auto Pick MDT Addresses] がオンになっていない場合は、[Default MDT Address] を指定できます。
- s. [Data MDT Subnet] (任意) : [Enable Auto Pick MDT Addresses] がオンになっていない場合は、[Default MDT Subnet] を指定できます。
- t. [Data MDT Size] (任意) : [Enable Multicast] がオンになっている場合は、[Data MDT Size] が必要です。ドロップダウン リストから、データ MDT のサイズを選択します。

MDT とは、*Multicast Distribution Tree* (MDT; マルチキャスト分散ツリー) のことです。ここで定義される MDT は、マルチキャスト ドメインに関連付けられたプロバイダーからのマルチキャスト トラフィックを伝送します。
- u. [Data MDT Threshold] (任意) : [Enable Multicast] がオンになっている場合は、[Data MDT Threshold] が必要です。データ マルチキャスト配信ツリーの帯域幅のしきい値を入力します。有効な範囲は 1 ~ 4294967 であり、キロビット/秒を示します。

データ MDT には、一連のマルチキャスト グループ アドレスおよび帯域幅のしきい値が含まれています。したがって、マルチキャスト トラフィックを送信中にマルチキャスト VRF の背後にある PE がこの帯域幅しきい値を超えると、PE によって、送信元からのマルチキャスト トラフィックに新しいデータ MDT が必ず設定されます。PE は、このデータ MDT についてその他の PE に通知し、その他の PE が対応するグループの受信機を持っている場合、その他の PE はこのデータ MDT に参加します。

- v. [Default PIM Mode] (任意) : デフォルトの Protocol Independent Multicast (PIM) モードの場合、ドロップダウン リストをクリックし、[SPARSE_MODE] または [SPARSE_DENSE_MODE] を選択します。IOS XR デバイスの場合、どちらのモードについてもコンフィグレットは生成されません。
- w. [MDT MTU] (任意) : この MDT 最大伝送単位 (MTU) の場合、IOS デバイスの範囲は 576 ~ 18010 であり、IOS XR デバイスの範囲は 1401 ~ 65535 です。デバイス タイプの特定の検証は、サービス要求の作成中に実行されます。
- x. [Enable PIM SSM] (任意) : PIM Source Specific Multicast (SSM) のためには、このチェックボックスをオンにします。
- y. [SSM List Name] (任意) ドロップダウン リストから [DEFAULT] を選択し、次の CLI を作成します。**ip pim vrf <vrfName> ssm default**。標準 SSM 範囲 232.0.0.0 /8 を使用しているため、IOS XR デバイスに対してコンフィグレットは生成されません。ドロップダウン リストから [RANGE] を選択し、アクセス リスト番号または名前付きアクセス リストを SSM の設定に関連付けます。こうすることにより、次の CLI (**ip pim vrf <vrfName> ssm range {ACL#!named-ACL-name}**) が作成されます。
- z. [Multicast Route Limit] (任意) 1 ~ 2147483647 の有効な値を入力します。IOS XR デバイスの場合、コンフィグレットは生成されません。
- aa. [Enable Auto RP Listener] (任意) : ランデブー ポイント (RP) リスナー機能をイネーブルにするには、このチェックボックスをオンにします。デフォルトでは、この機能は IOS XR デバイスで実行され、この属性に対してコンフィグレットは生成されません。
- ab. [My PIM Static-RPs] : スタティック RP を設定するには、このチェックボックスをオンにします。編集オプションがアクティブになります。[Edit] をクリックし、表示されるウィンドウの該当するフィールドに入力します。次に [OK] をクリックします。

ステップ 4 この VPF の設定が終了したら、[Save] をクリックします。

[VRFs] ウィンドウの左下隅の [Status] 表示に示されているように、VRF が正常に作成されました。

VRF の編集

[VRF] ウィンドウから、1 つ以上の VRF を編集できます。

VRF を編集するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRF] を選択します。
- ステップ 2** 編集するすべての VRF のチェックボックスをオンにしてから、[Edit] をクリックします。
- ステップ 3** ある VRF に対して 1 つのチェックボックスしかオンにしなれば、[Edit VRF] というタイトルのウィンドウが表示され、[Name] フィールドには選択した VRF の名前が表示されます。また、[Provider] フィールドには選択した VRF のプロバイダーの名前が事前に取り込まれます。変更を行った後、[ステップ 8](#) に進みます。
- ステップ 4** 複数のチェックボックスをオンにすると、[Edit Multiple VRFs] というタイトルのウィンドウが表示されます。
- ステップ 5** [VRFs Affecting] セクションに、選択した VRF の名前が表示されます。[Attributes] をクリックすると、選択されたすべての VRF について現在設定されている属性が表示されたウィンドウが表示されます。

- ステップ 6** [Route Attributes] セクションに、追加および削除する [Import Targets] および [Export Targets] を指定します。ルート ターゲット (RT) のこれらのリストは、「VRF の作成」(P.5-263) の [Import RT List] および [Export RT List] の説明に示されているように、カンマで区切る必要があります。編集する残りのフィールドの詳細については、「VRF の作成」(P.5-263) を参照してください。
- ステップ 7** [Multicast Attributes] セクションで、フィールドを編集できます。編集するフィールドの詳細については、「VRF の作成」(P.5-263) を参照してください。
- ステップ 8** [Save] をクリックすると VRF が更新されます。
-

VRF の削除

[VRF] ウィンドウから、特定の VRF を削除できます。



(注) VRF サービス要求に関連付けられていない VRF のみ削除できます。

VRF を削除するには、次の手順を実行します。

- ステップ 1** [Inventory] > [Logical Inventory] > [VRF] を選択します。
- ステップ 2** VRF 名の左にあるチェックボックスをオンにして削除する VRF を選択します。
- ステップ 3** [Delete] ボタンをクリックします。
[Confirm Delete] ウィンドウが表示されます。
- ステップ 4** リストされた VRF を削除することを確認して、[OK] をクリックします。
指定された VRF が削除された状態で、[VRF] ウィンドウが再表示されます。
-