Cisco Prime Provisioning 6.3 ユーザ ガイド

2012 年 10 月 9 日

Text Part Number: OL-27136-01-J

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

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

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

Cisco Prime Provisioning 6.3 ユーザ ガイド

CONTENTS

このマニュアルについて

ここでは、次の項について説明します。

目的

『*Cisco Prime Provisioning 6.3 ユーザ ガイド*』には、すべてのアプリケーションにわたって Prime Provisioning サービスおよびコンポーネントの詳細な説明があります。

（注）

このリリースの Prime Provisioning は、スタンドアロン製品、または Cisco Prime for IP Next Generation Network（IP NGN）スイートの一部として使用できます。スイートの一部としてインストールした場合は、Prime Central ポータルから Prime Provisioning を起動できます。Prime Central の詳細については、Cisco Prime Central 1.1 のマニュアルを参照してください。

対象読者

このマニュアルは、カスタマーのために Prime Provisioning サービスのプロビジョニングを担当するサービス プロバイダーのネットワーク管理者およびオペレータを対象にしています。

ネットワーク管理者とオペレータは、設定しているサービスに必要な次の項目に精通している必要があります。

- インターネットワーキングで使用される基本的な概念と用語。
- ネットワーク トポロジおよびプロトコル
- Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）、Virtual Private LAN Service（VPLS; 仮想専用 LAN サービス）、VPN、マルチプロトコル ラベル スイッチング（MPLS）、用語、およびテクノロジー
- MPLS VPN の用語とテクノロジー。

- また、マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）の概念とトラフィック エンジニアリングに関する一般的な知識も必要です。

マニュアルの構成

このマニュアルは、次の章で構成されています。

- 第 1 章「Prime Provisioning GUI の概要」では、Prime Provisioning のグラフィカル ユーザ インターフェイス（GUI）の概要について説明します。
- 第 2 章「Prime Provisioning を設定する前に」では Cisco Prime Provisioning サービスを設定する方法について説明します。
- 第 3 章「L2VPN とキャリア イーサネット サービスの管理」では、L2VPN とキャリア イーサネット サービスを管理する方法について説明します。
- 第 4 章「RAN バックホール サービスの管理」では、RAN バックホール サービスを管理する方法について説明します。
- 第 5 章「MPLS VPN サービスの管理」では、MPLS VPN サービスを管理する方法について説明します。
- 第 6 章「MPLS トランスポート プロファイル サービスの管理」では、MPLS 転送プロファイル サービスを管理する方法について説明します。
- 第 7 章「MPLS トラフィック エンジニアリング サービスの管理」では、MPLS トラフィック エンジニアリング サービスを管理する方法について説明します。
- 第 8 章「サービス要求の管理」では、サービス要求を管理する方法について説明します。
- 第 9 章「テンプレートおよびデータ ファイルの管理」では、テンプレートおよびデータ ファイルを管理する方法について説明します。
- 第 10 章「モニタリング」では、Prime Provisioning をモニタする方法について説明します。
- 第 11 章「診断の実行」では、Prime Provisioning での診断の実行について説明します。
- 第 12 章「トポロジ ツールの使用」では、Prime Provisioning でトポロジ ツールを使用する方法について説明します。
- 第 13 章「インベントリ マネージャの使用」では、Prime Provisioning でインベントリ マネージャを使用する方法について説明します。
- 付録では、補足情報を提供します。

関連資料

Cisco Prime Provisioning のすべてのマニュアル セットは、次の URL でアクセスできます。

http://www.cisco.com/en/US/products/ps12199/tsd_products_support_series_home.html

または

http://www.cisco.com/go/provisioning

Cisco Prime Provisioning 6.3 マニュアル セットには次のマニュアルが含まれます。

一般的なマニュアル（この順序で読むことを推奨します）

- *『Cisco Prime Provisioning 6.3 Documentation Overview』*

- 『*Cisco Prime Provisioning 6.3 Release Notes*』
- 『*Cisco Prime Provisioning 6.3 Installation Guide*』
- 『*Cisco Prime Provisioning 6.3 Supported Devices*』
- 『*Cisco Prime Provisioning 6.3 User Guide*』
- 『*Cisco Prime Provisioning 6.3 Administration Guide*』
- 『*Open Source Used in Cisco Prime Provisioning 6.3*』

API に関するマニュアル

- 『*Cisco Prime Provisioning 6.3 API Programmer Guide*』
- 『*Cisco Prime Provisioning API 6.3 Programmer Reference*』

（注） どのマニュアルも、将来アップグレードされる*可能性*があります。アップグレードされたマニュアルはすべて、本書で示したのと同じ URL で入手できます。

他の Cisco Prime 製品マニュアル

次の Cisco Prime 製品のマニュアルも参照してください。

- *Cisco Prime Central 1.1*
- *Cisco Prime Network 3.9*
- *Cisco Prime Optical 9.6*
- *Cisco Prime Performance Manager 1.2*

マニュアルの入手方法およびテクニカル サポート

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

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

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

CHAPTER 1

Prime Provisioning GUI の概要

この章では、Cisco Prime Provisioning の使用を開始する方法とこのガイドの構造的な概要を説明します。次の事項について説明します。

システム推奨事項

システム推奨事項と要件は、*『Cisco Prime Provisioning 6.3 Installation Guide』*および*『Cisco Prime Provisioning 6.3 Release Notes』*の第 1 章『System Recommendations』に記載されています。インストールを計画する前に、このリストを十分に確認し、インストールを正常に完了させるために必要なハードウェアおよびソフトウェアがすべて用意できているかどうかを確認することを推奨します。

はじめに

Prime Provisioning 6.3 は Cisco IP Solution Center（ISC）を発展させたものであり、ユーザ インターフェイス、デバイスとテクノロジーの追加と更新、および強力な診断ワークフローの拡張に対する大幅な拡張が組み合わされたオファリングの強力な機能が含まれています。Prime Provisioning の章は、*『Cisco Prime Provisioning 6.3 Release Notes』*に記載されています。

このマニュアルには、個別に販売され、ライセンスを受けている複数のアプリケーション間で共通する多くの機能が示されています。アプリケーションとそれらの各*ユーザ ガイド*では、ポリシーを作成した後、アプリケーションに固有のサービス要求を作成するために必要なセットアップステップと、他の共通機能に関して、このマニュアルを参照します。

グラフィカル ユーザ インターフェイス（GUI）のタブを説明する前に、「構造の概要」（P.1-2）を参照してください。これは、Prime Provisioning の多数のウィンドウに共通の要素を説明しています。

GUI は、次の大まかなセクション（タブ）に分割されています。

- 「Operate」（P.1-8）
- 「Inventory」（P.1-8）
- 「Service Design」（P.1-9）
- 「Traffic Engineering」（P.1-10）
- 「Diagnostics」（P.1-11）
- 「Administration」（P.1-11）

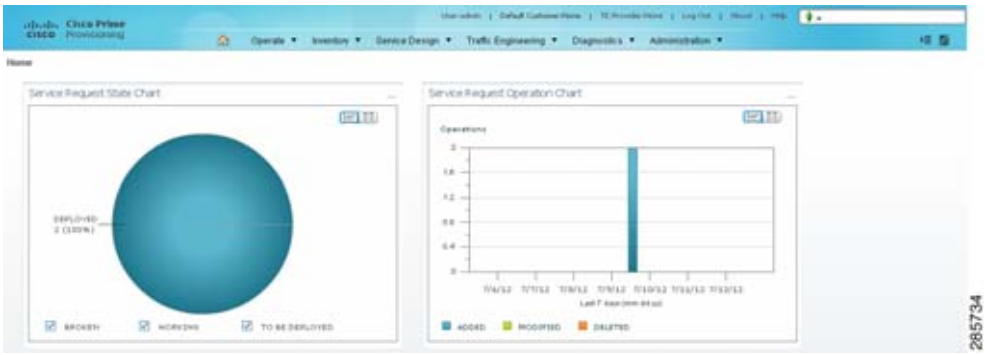
この章の残りの項では、これらのタブから使用可能な機能を説明するこのマニュアルのセクションおよびサブセクションについて説明します。

（注）　このマニュアルとこの製品で使用されている用語は、他の用語とほぼ同じ意味で使用できます。

構造の概要

Prime Provisioning にログインした後、最初に表示されるウィンドウは図 1-1 の「[Home] ウィンドウ」に示されている [Home] ウィンドウです。

図 1-1　[Home] ウィンドウ



（注）　表示されるタブと、タブ内のナビゲートに使用する選択肢は、ユーザの権限によって異なります。『*Cisco Prime Provisioning 6.3 Administration Guide*』を参照してください。

ホーム画面では 2 種類の新しいグラフを使用できるようになりました。この図にはさまざまな状態の SR カウントが示され、過去 7 日間に展開した SR がリストされています。

- [Pie chart]：この円グラフは、さまざまな状態の Prime Provisioning のサービス要求に関する全体像を示します。円グラフ内のいずれかの状態をクリックすると、選択された状態のすべてのサービス要求リストが示されたサービス マネージャの画面にリダイレクトします。
- [Bar chart]：この棒グラフには、Prime Provisioning で追加、変更、または削除された過去 7 日間のサービス要求が示されます。棒グラフをクリックすると、選択された日のすべてのサービス要求リストが示されたサービス マネージャの画面にリダイレクトします。

この概要では、次の項目について説明します。

リンク

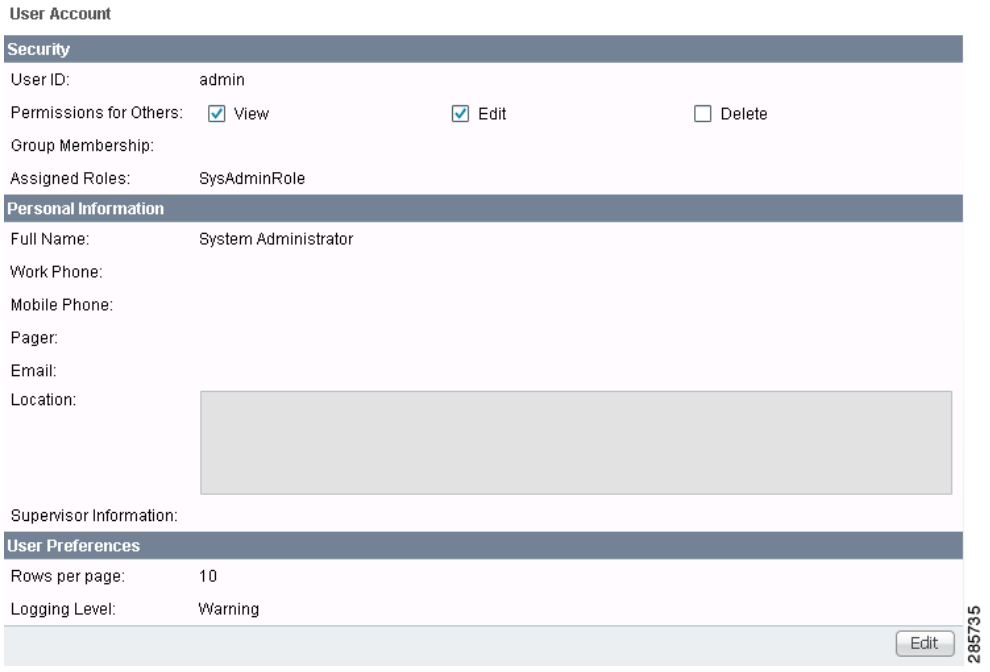
[Home] ウィンドウ（図 1-1）の右上隅に、次のように機能する追加リンクが表示されます。

- 「User」（P.1-3）
- 「Customer」（P.1-4）
- 「TE Provider」（P.1-4）
- 「Logout」（P.1-4）
- 「About」（P.1-4）
- 「Help」（P.1-5）

User

[Home] ページにある [User] は、[User:] の後ろに admin（デフォルト）またはユーザ名が続きます。[User: admin] をクリックすると、次のウィンドウが表示されます。

図 1-2　[User: admin] ウィンドウ



[Edit] ボタンをクリックすると、SysAdmin または UserAdmin 特権なしでパスワードを変更できます。これにより、パスワードの変更など、ユーザ プロファイルを編集することができます。

Customer

[Home] ページの [Customer] は、[Customer:] の後ろに None（デフォルト）またはカスタマー名が続きます。これはカスタマー コンテキストと呼ばれます。カスタマー コンテキストの利点は、指定されたカスタマーに関する情報のみに焦点が当てられることです。このリンクはデフォルトのカスタマーが設定されるとアクティブになります。デフォルトのカスタマーは、カスタマー コンテキストを編集または表示できます。

TE Provider

[Home] ページの [TE Provider] は、[TE Provider:] の後ろに [None]（デフォルト）または TE プロバイダー名が続きます。これは、TE プロバイダー コンテキストといいます。TE プロバイダー コンテキストの利点は、指定されたプロバイダーの情報のみに焦点が当てられることです。プロバイダー コンテキストを設定するには、次の手順を実行します。

ステップ 1　[TE Provider: None] の後に続く名前をクリックすると、次のウィンドウが表示されます。

図 1-3　　TE プロバイダー コンテキスト

ステップ 2　[Select] ボタンをクリックすると、現在作成されているすべてのプロバイダーのリストが表示されます。

ステップ 3　情報を表示するカスタマーのオプション ボタンをクリックして、[Select] をクリックします。

図 1-3 が、選択された TE プロバイダー名で再表示されます。[Save] をクリックするか、TM プロバイダー名を強調表示し、[Clear] をクリックして、情報が必要な TE プロバイダーをリセットします。

選択した TE プロバイダーが、[Home] ウィンドウの [TE Provider:] の後に表示されます。これは、情報が表示される唯一の TE プロバイダーです。

ステップ 4　TE プロバイダー コンテキストをクリアして再選択することでリセットできます。

Logout

[Logout] をクリックすると、製品からログアウトします。

About

[About] をクリックすると、製品名とバージョンが表示されます。

Help

[Help] をクリックすると、Prime Provisioning マニュアルへのポインタが表示されます。
http://www.cisco.com/en/US/products/ps12199/tsd_products_support_series_home.html
この場所から、参照する Prime Provisioning のマニュアルのタイプを選択できます。

共通 GUI コンポーネント

多くのウィンドウで共通の GUI コンポーネントは次のとおりです。

フィルタ

多くのウィンドウの最上部で、ウィンドウで表示される情報をフィルタリングできます。図 1-4 に示されているように、カテゴリのドロップダウン リストをクリックし、**一致する**フィールドに検索条件を入力します。何らかの一致するものを示す場合は * を使用し（* のみを入力するか、他の文字の前、他の文字の中央、他の文字の後ろ、または複数の場所に * を置く）、[Find] をクリックします。場合によっては、**一致する**フィールドの後にフィールドがあります。このフィールドを使用して、[Find] を実行する際にさらに指定内容を選択または入力できます。

[Header Row] チェックボックス

図 1-4 に示されているように、多くのウィンドウにはヘッダー行にカラム名が表示されたチェックボックスがあります。このチェックボックスをオンにすると、ウィンドウ内のすべてのチェックボックスがオンに設定されます。

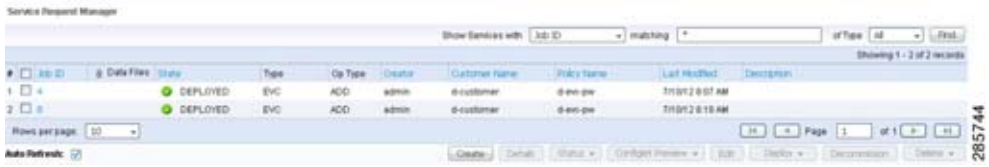
Rows per Page

多くのウィンドウの左下隅には [Rows per page] が表示されていて、このウィンドウ内に表示される行数を変更できます（図 1-4 を参照）。このドロップダウン リストをクリックして、[5]、[10]、[20]、[30]、[40]、[50]、[100]、[500]、[1000]、または [2500] から選択できます。

Go To Page

図 1-4 に示されているように、多くのウィンドウの右下隅に *y* の [Go to page] *フィールド*があります。この *フィールド*に、選択するページを入力して、[Go] ボタンをクリックし、そのページに移動することができます。***y*** は、このトピックの最後のページを示します。矢印を使用して特定のページを選択することもできます。> 矢印をクリックして次のページを選択したり、右向きの最端矢印 >| を使用して最後のページを選択したりすることができます。< 矢印をクリックして前のページを選択したり、左向きの最端矢印 |< を使用して最初のページを選択したりすることができます。

図 1-4　[Filtering]、[Header Row] チェックボックス、[Rows per Page]、および [Changing Pages] の例



Auto Refresh

図 1-5 に示されているように、いくつかのウィンドウの左下隅には、[Auto Refresh] 機能をイネーブルまたはディセーブルにするために使用するチェックボックスがあります。このチェックボックスをオンにすると、ウィンドウとデータが **n** ミリ秒ごとに更新されます。更新サイクルの間隔は、DCPL プロパティ GUI.srRefreshRate で設定できます。デフォルトで、[Auto Refresh] 機能は 30000 ミリ秒に設定されています。

表示色

図 1-5 に示されているように、[Service Request] テーブル、[Task] テーブル、および [Device] テーブルでは、表示されている色によって項目の状態が表されます。

[Service Request] テーブルでは、各状態は次の色で示されます。

- [BROKEN] は明るい黄色
- [CLOSED] は無色
- [DEPLOYED] は明るい緑色
- [FAILED AUDIT] は明るい黄色
- [FAILED DEPLOY] は明るい赤色
- [FUNCTIONAL] は明るい緑色
- [INVALID] は明るい赤色
- [LOST] は明るい黄色
- [PENDING] は明るい緑色
- [IN-PROGRESS] は明るい黄色
- [REQUESTED] はクリーム色
- [WAIT DEPLOYED] はクリーム色

[Task] テーブルでは、各状態は次の色で示されます。

- [ABORTED] は橙色
- [RUNNING] は明るい緑色
- [WAITING_TO_RUN] はクリーム色
- エラーは明るい赤色
- 成功は明るい緑色
- 警告は青緑色

[Devices] テーブルでは、各状態は次の色で示されます。

- デバイスが **success** または **no result** 以外のものを返す場合、明るい赤色
- デバイスが **success** を返す場合、明るい緑色
- デバイスから返されるのが **no result** である場合、暗い青色

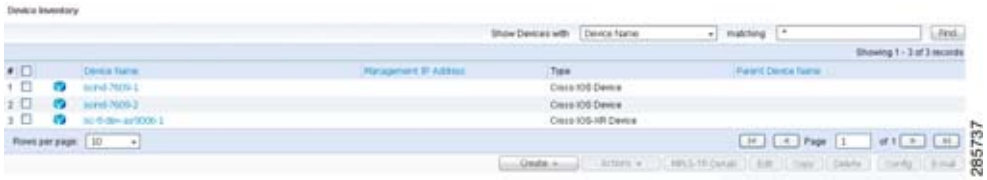
図 1-5　識別子としての色

アイコン

情報の表が含まれる一部のウィンドウでは、図 1-6 に示されるように、デバイスのタイプを示すアイコンが表示されます。

（注）　使用可能なアイコンのリストは、第 12 章「トポロジ ツールの使用」の「トポロジ ツールの起動」（P.12-2）の項にある表 12-1 で入手できます。

図 1-6　デバイス：アイコン

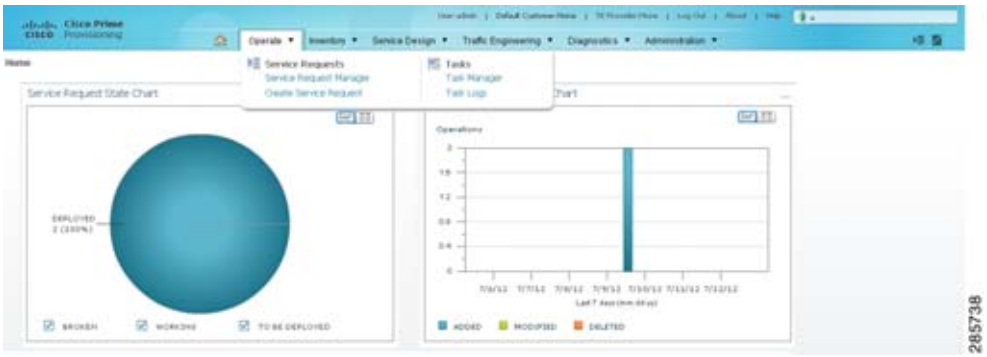


Operate

[Operate] には、サービス要求を作成および管理するためのツールと、Prime Provisioning のさまざまなタスクが含まれています。

ログイン時に表示される [Home] ウィンドウで [Operate] タブをクリックすると、ウィンドウが表示されます（図 1-7 を参照）。

図 1-7　[Operate] の選択肢



選択肢は次のとおりです。

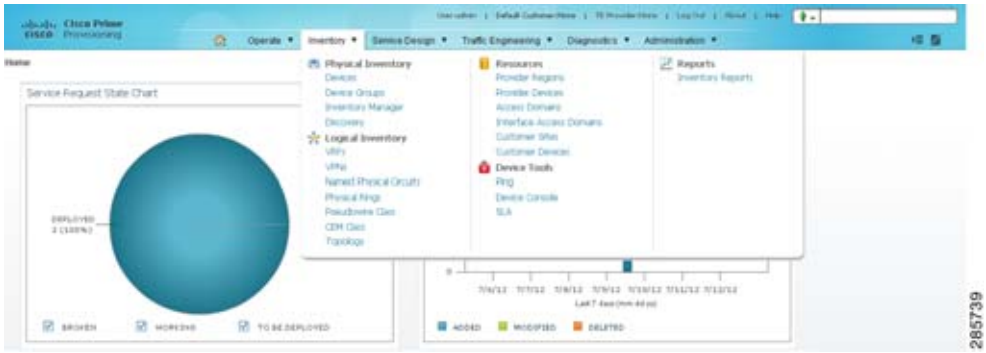
- [Service Requests]：サービス要求（SR）を作成、展開、および管理します。これは、第 8 章「サービス要求の管理」で詳しく説明されています。
- [Tasks]：Prime Provisioning に関連付けられたタスクを作成および管理します。これは、第 10 章「モニタリング」の「タスク マネージャ」（P.10-25）の項で詳しく説明されています。

Inventory

[Inventory] には、物理および論理インベントリ要素、リソース、デバイス ツール、およびレポートを管理するためのツールが含まれています。

ログイン時に表示される [Home] ウィンドウで [Inventory] タブをクリックすると、ウィンドウが表示されます（図 1-8 を参照）。

図 1-8　[Inventory] の選択肢



選択肢は次のとおりです。

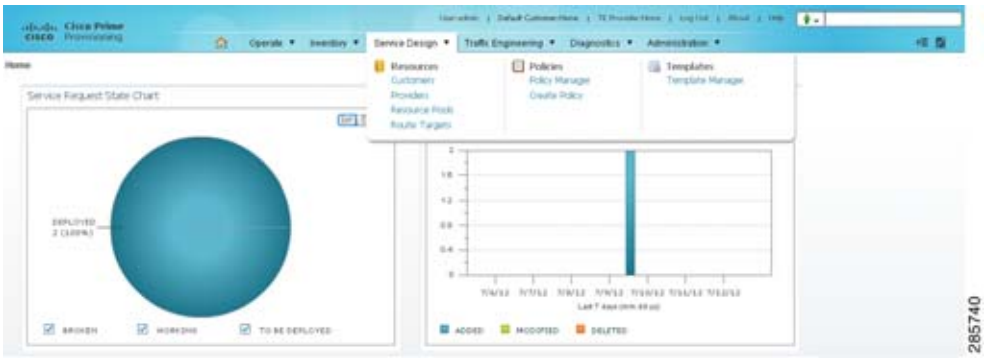
- [Physical Inventory]：デバイス、デバイス グループ、インベントリ マネージャ、および Discovery を作成および管理します。
  - [Devices]：デバイスを作成および管理します。第 2 章「Prime Provisioning を設定する前に」の「デバイス」（P.2-1）の項で詳しく説明されています。
  - [Device Groups]：デバイス グループを作成および管理します。第 2 章「Prime Provisioning を設定する前に」の「デバイス グループ」（P.2-29）の項で詳しく説明されています。
  - [Inventory Manager]：インベントリ要素を一括管理します。第 13 章「インベントリ マネージャの使用」で詳しく説明されています。
  - [Discovery]：デバイス、接続、およびサービスを検出します。付録 E「インベントリ - ディスカバリ」で詳しく説明されています。
- [Logical Inventory]：VRF、VPN、名前付き物理回線、物理リング、および疑似回線クラスを作成および管理します。これは、第 2 章「Prime Provisioning を設定する前に」の「論理的インベントリの設定」（P.2-56）の項で詳しく説明されています。
- [Resources]：カスタマー サイトとデバイス、プロバイダー リージョンとデバイス、およびアクセス ドメインを作成および管理します。これは、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」（P.2-42）の項で詳しく説明されています。
- [Device Tools]：次の中から選択します。
  - [Ping]：Ping 接続性テストを実行します。第 10 章「モニタリング」の「ping」（P.10-1）の項で詳しく説明されています。
  - [SLA]：サービス レベル契約（SLA）プローブを管理します。第 10 章「モニタリング」の「SLA」（P.10-3）の項で詳しく説明されています。
  - [Device Console]：デバイスにコマンドとコンフィグレットをダウンロードし、デバイス構成を表示します。第 13 章「インベントリ マネージャの使用」の「[Inventory] - [Device Console]」（P.13-1）の項で詳しく説明されています。
- [Reports]：Prime Provisioning のさまざまなレポートを作成および管理します。これは、第 10 章「モニタリング」の「レポート」（P.10-29）の項で説明されています。

Service Design

[Service Design] には、リソース、ポリシー、およびテンプレートを作成および管理するための管理ツールが含まれています。

ログイン時に表示される [Home] ウィンドウで [Service Design] タブをクリックすると、図 1-9 に示されているように、ウィンドウが表示されます。

図 1-9　[Service Design] の選択肢



選択肢は次のとおりです。

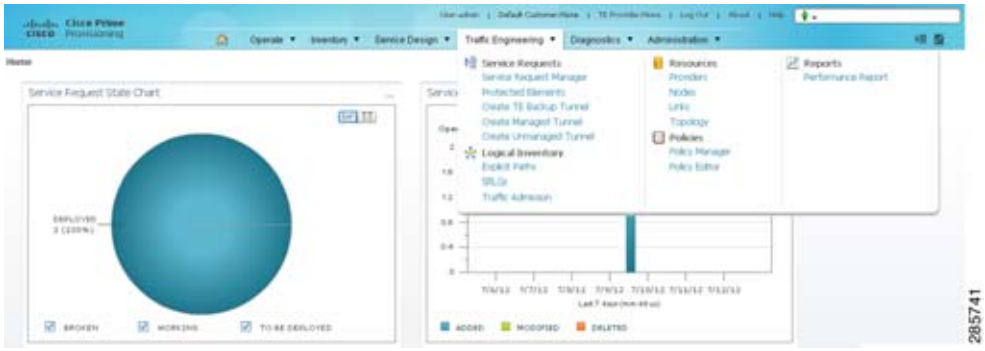
- [Resources]：[Customers]、[Providers]、[Resource Pools]、および [Route Targets] を作成および管理します。次の選択肢は、第 2 章「Prime Provisioning を設定する前に」の「リソースの設定」（P.2-42）の項で詳しく説明されています。
  - [Customers]：カスタマーを作成および管理します。
  - [Providers]：プロバイダーを作成および管理します。
  - [Resource Pools]：IP アドレス プール、マルチキャスト アドレス、ルート識別子、ルート ターゲット、Site of Origin、VC ID、および VLAN を作成および管理します。
  - [CE Routing Communities]：CE ルーティング コミュニティを作成および管理します。
- [Policies]：ライセンスを受けたサービスのポリシーを作成および管理します。
- [Templates]：テンプレートと、関連付けられたデータを作成および管理します。第 9 章「テンプレートおよびデータ ファイルの管理」で詳しく説明されています。

Traffic Engineering

[Traffic Engineering] には、トラフィック エンジニアリング管理の要素を作成、展開、および管理するためのツールが含まれています。これは、第 7 章「MPLS トラフィック エンジニアリング サービスの管理」で詳しく説明されています。

ログイン時に表示される [Home] ウィンドウで [Traffic Engineering] タブをクリックすると、ウィンドウが表示されます（図 1-10 を参照）。

図 1-10　[Traffic Engineering] の選択

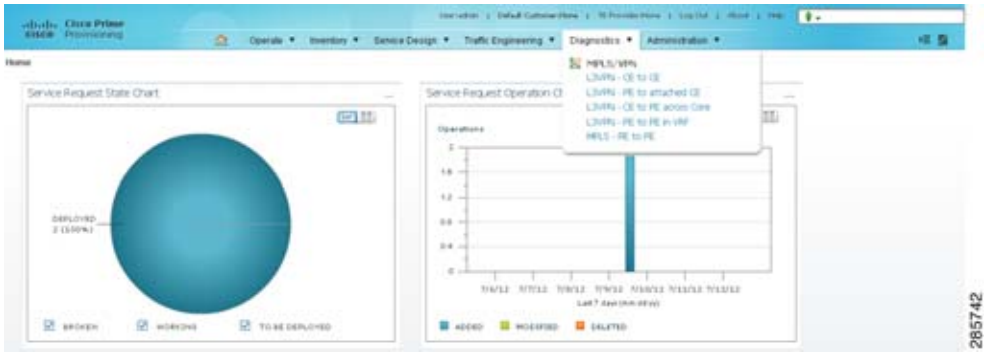


Diagnostics

[Diagnostics] には、MPLS VPN の自動トラブルシューティングと診断が含まれています。これは、第 5 章「MPLS VPN サービスの管理」で詳しく説明されています。

図 1-11 に示されているように、ログイン時に表示される [Home] ウィンドウで [Diagnostic] タブをクリックすると、ウィンドウが表示されます。

図 1-11　[Diagnostic] の選択

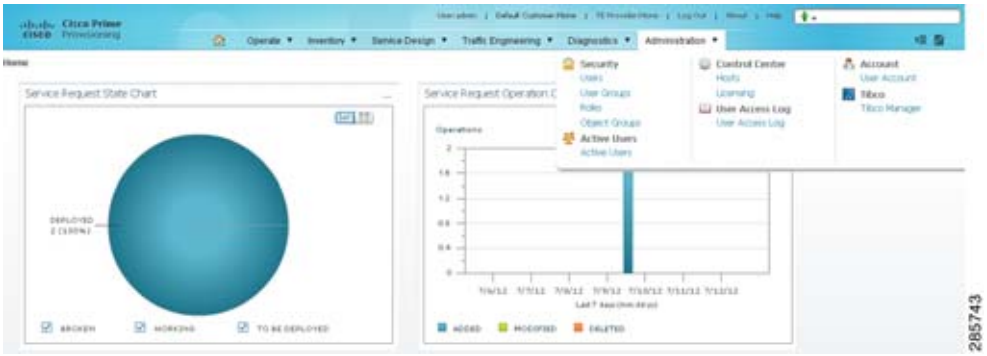


Administration

[Administration] には、ユーザ、Prime Provisioning 設定、サーバ、およびライセンスを管理し、ユーザおよびユーザ アクセス ログを表示し、一部のメッセージの属性を指定するためのツールが含まれています。

ログイン時に表示される [Home] ウィンドウで [Administration] タブをクリックすると、ウィンドウが表示されます（図 1-12 を参照）。

図 1-12　Administration Selections



選択肢は次のとおりです。

- [Security]：[Users]、[User Groups]、[User Roles]、および [Object Groups] を作成および管理します。次の選択肢は、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* で詳しく説明されています。
  - [Users]：インベントリ マネージャ、トポロジ、および Northbound API にもアクセスするためにユーザを作成し管理します。
  - [User Groups]：[User Groups] を作成および管理します。[Group] は、それに含まれているすべてのロールの特権を結合するために使用されます。
  - [User Roles]：特権セットを定義する [User Roles] を作成および管理します。
  - [Object Groups]：デバイス、インターフェイス、および名前付き物理回線など、オブジェクト グループを作成し管理します。
- [Control Center]：Prime Provisioning の設定、サーバ、およびライセンスを管理します。次の選択肢は、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* で詳しく説明されています。
  - **Hosts**

（注）　**カスタム** インストールを行う場合にこれを使用するには、*『Cisco Prime Provisioning 6.3 Installation Guide』* で説明されているインストール手順に従う必要があります。

  - **Collection Zones**
  - **Licensing**
- [Active Users]：現在 Prime Provisioning に接続しているユーザを表示します。ユーザを切断します（*『Cisco Prime Provisioning Administrator’s Guide 6.3』* で詳しく説明されています）。
- [User Access Log]：ユーザのアクセス ログを表示します（*『Cisco Prime Provisioning Administrator’s Guide 6.3』* で詳しく説明されています）。
- [Manage TIBCO Rendezvous]：すべての Java Web Start 分散アプリケーション内で適切に管理するための属性を指定します。これは、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* で詳しく説明されています。

CHAPTER 2

Prime Provisioning を設定する前に

この章では、サービスの設定方法について説明します。次の事項について説明します。

デバイスおよびデバイス グループを設定する方法

この項では、物理的なサービス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。

デバイス

Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義する必要があります。要素は、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、MPLS VPN でプロバイダー エッジ ルータ（PE）、またはカスタマー エッジ ルータ（CE）として機能する Cisco IOS ルータです。

（注） Prime Provisioning でサービスをプロビジョニングするには、IPv4 接続が必要です。

ここでは、SSH または SSHv2 を設定し、SNMP を設定し、RTR 応答側を手動でイネーブル化し、サポートされているさまざまなデバイスのタイプの作成、編集、削除、および設定を行う方法について説明します。この項では、次のトピックについて取り上げます。

SSH または SSHv2 の設定

Prime Provisioning には、ルータとスイッチを含むデバイスのコンフィギュレーション ファイルにセキュアにアクセスし、それらのファイルを展開するメカニズムが必要です。また、コンフィグレットをセキュアにダウンロードし、デバイスからコンフィギュレーション ファイルをアップロードするには、Secure Shell（SSH）または SSH バージョン 2（SSHv2）をイネーブルにする必要があります。

次の章では、次の内容について説明します。

ドメイン名を使用した Cisco IOS ルータでの SSH の設定

Cisco IOS ルータで SSH を設定する手順は、次のとおりです。

	コマンド	説明
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# ip domain-name <domain_name>`	IP ドメイン名を指定します。
ステップ 3	`Router(config)# username <username> password <password>`	ユーザ ID およびパスワードを設定します。Prime Provisioning のユーザ名およびパスワードを入力します。たとえば、次のように入力します。 `username admin password iscpwd`
ステップ 4	`Router(config)# crypto key generate rsa`	SSH セッションのキーを生成します。
ステップ 5	次のプロンプトが表示されます。 `Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. How many bits in the modulus (nnn):` デフォルトのビット数を受け入れるには、Enter キーを押します。	ビット数を設定します。
ステップ 6	`Router(config)# line vty 0 4`	vty ログイン転送の一部として、SSH をイネーブルにします。
ステップ 7	`Router(config-line)# login local`	**login local** コマンドは、ルータが認証情報をローカルに格納することを示します。
ステップ 8	`Router(config-line)# transport input telnet ssh`	SSH 転送をイネーブルにします。

	コマンド	説明
ステップ 9	`Router(config-line)# Ctrl+Z`	特権 EXEC モードに戻ります。
ステップ 10	`Router# copy running startup`	不揮発性 RAM（NVRAM）に対する設定変更を保存します。

RSA キー ペアを使用した Cisco IOS ルータの SSHv1 または SSHv2 の設定

Cisco IOS ルータで SSHv1 または SSHv2 を設定する手順は次のとおりです。

	コマンド	説明
ステップ 1	`Router# enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`Router(config)# ip ssh rsa keypair-name <keypair-name>`	SSH を使用する際に使用する RSA キー ペアを指定します。（注）Cisco IOS ルータでは、複数の RSA キー ペアを指定できます。
ステップ 4	`Router(config)# crypto key generate rsa usage-keys label <key-label> modulus <modulus-size>`	ルータでローカルおよびリモート認証を行う SSH サーバをイネーブルにします。 SSH バージョン 2 では、絶対サイズは 768 ビット以上である必要があります。 注：Rivest、Shamir、および Adelman（RSA）キー ペアを削除するには、**crypto key zeroize rsa** コマンドを使用します。RSA コマンドを削除すると、SSH サーバが自動的にディセーブルになります。
ステップ 5	`Router(config)# ip ssh [timeout <seconds> | authentication-retries <integer>]`	ルータに SSH 制御変数を設定します。
ステップ 6	`Router(config)# ip ssh version [1 | 2]`	ルータで実行する SSH のバージョンを指定します。

Cisco IOS XR ルータでの SSH または SSHv2 の設定

Cisco IOS XR ルータで SSHv2 を設定する手順は次のとおりです。

	コマンド	説明
ステップ 1	`RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`RP/0/RP0/CPU0:router(config)# hostname <hostname>`	ルータのホスト名を設定します。
ステップ 3	`RP/0/RP0/CPU0:router(config)# domain name <domain-name>`	不完全なホスト名を補完するために使用するデフォルトのドメイン名を定義します。
ステップ 4	`RP/0/RP0/CPU0:router(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを EXEC モードに戻します。
ステップ 5	`RP/0/RP0/CPU0:router(config)# crypto key generate rsa [usage keys | general-keys] [<keypair-label>]`	RSA キー ペアを生成します。

	コマンド	説明
ステップ 6	RP/0/RP0/CPU0:router# **crypto key generate dsa**	ルータでローカルおよびリモート認証を行う SSH サーバをイネーブルにします。 推奨する最小絶対サイズは 1024 ビットです。 DSA キー ペアを生成します。DSA キー ペアを削除するには、**crypto key zeroize dsa** コマンドを使用します。このコマンドは SSHv2 だけに使用されます。
ステップ 7	RP/0/RP0/CPU0:router# **configure**	グローバル コンフィギュレーション モードを開始します。
ステップ 8	RP/0/RP0/CPU0:router# **ssh timeout <***seconds***>**	（任意）認証、許可、アカウンティング（AAA）に対するユーザ認証のタイムアウト値を設定します。 設定された時間内にユーザ自身の認証が AAA に対してできないと、接続は中断されます。 値を設定しなければ、30 秒のデフォルト値が使用されます。範囲は 5 ～ 120 です。
ステップ 9	RP/0/RP0/CPU0:router(config)# **ssh server** or RP/0/RP0/CPU0:router(config)# **ssh server v2**	SSH サーバを起動します。 SSH サーバを停止するには、**no ssh server** コマンドを使用します。 （任意）**ssh server v2** コマンドを使用して SSHv2 オプションを設定した場合、SSH サーバは SSHv2 クライアントだけを受け入れるように強制されます。**ssh server v2** コマンドを選択すると、SSH v2 クライアント接続だけが受け入れられます。
ステップ 10	RP/0/RP0/CPU0:router(config)# **end** or RP/0/RP0/CPU0:router(config)# **commit**	設定変更を保存します。 **end** コマンドを発行すると、次に示す変更のコミットを求めるプロンプトが表示されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)?[cancel] **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 **cancel** と入力すると、ルータは現在のコンフィギュレーション セッションで継続されます。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンド	説明
ステップ 11	`RP/0/RP0/CPU0:router# show ssh`	（任意）ルータで送受信している SSHv1 および SSHv2 の接続をすべて表示します。
ステップ 12	`RP/0/RP0/CPU0:router# show ssh session details`	（任意）ルータとの間の SSHv2 接続の詳細レポートを表示します。

デバイスの作成

[Create] ウィンドウから、さまざまなデバイス タイプを定義できます。

デバイスを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create] オプションのウィンドウが表示されます。

[Create] オプションには、次のものがあります。

- [Catalyst Switch] : Catalyst オペレーティング システムを実行する Catalyst デバイス。
- [Cisco Device] : Cisco IOS を実行している任意のルータ。これには、Cisco IOS を実行している Catalyst デバイスが含まれます。
- [Terminal Server] : エッジ ルータをプロビジョニングするために使用できるワークステーションを表すデバイス。
- [Cisco Configuration Engine（IE2100）] : Cisco Intelligence Engine（IE）2100 シリーズ ネットワーク デバイス。

ステップ 3　各タイプのデバイスの作成方法については、次の項を参照してください。

- 「Catalyst スイッチの作成」（P.2-5）
- 「シスコ デバイスの作成」（P.2-6）
- 「ターミナル サーバの作成」（P.2-7）
- 「Cisco Configuration Engine サーバの作成」（P.2-12）

Catalyst スイッチの作成

Catalyst スイッチを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create] オプションのウィンドウが表示されます。

ステップ 3　[Catalyst Switch] を選択します。

[Create Catalyst Device] ウィンドウが表示されます。

これらの属性フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-7）
- 「ログインとパスワードの属性」（P.2-9）
- 「[Device and Configuration Access Information] の属性」（P.2-9）
- 「[SNMP v1/v2c] の属性」（P.2-10）

ステップ 4　作成している Catalyst デバイスに必要な情報を入力します。

ステップ 5　[Create Catalyst Device] の [Additional Properties] セクションにアクセスするには、[Show] をクリックします。

[Additional Properties] ウィンドウが表示されます。

[Additional Properties] の属性フィールドの説明については、次の項を参照してください。

- 「SNMP v3 属性」（P.2-10）
- 「[Terminal Server] オプションの属性」（P.2-11）
- 「[Device Platform Information] の属性」（P.2-11）

ステップ 6　作成している Catalyst デバイスに関する、必要な追加プロパティ情報を入力します。

ステップ 7　[Save] をクリックします。

新しい Catalyst デバイスがリストされて、[Devices] ウィンドウが再表示されます。

シスコ デバイスの作成

シスコ デバイスを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create] オプションのウィンドウが表示されます。

ステップ 3　[Cisco Device] を選択します。

[Create Cisco Device] ウィンドウが表示されます。

フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-7）
- 「ログインとパスワードの属性」（P.2-9）
- 「[Device and Configuration Access Information] の属性」（P.2-9）
- 「[SNMP v1/v2c] の属性」（P.2-10）

ステップ 4　作成している Cisco IOS デバイスに必要な情報を入力します。

ステップ 5　[Create Cisco Device] の [Additional Properties] セクションにアクセスするには、[Show] をクリックします。

[Additional Properties] ウィンドウが表示されます。

[Additional Properties] フィールドの説明については、次の項を参照してください。

- 「SNMP v3 属性」（P.2-10）
- 「[Terminal Server] オプションの属性」（P.2-11）

- 「[Device Platform Information] の属性」（P.2-11）

ステップ 6　作成している Cisco IOS デバイスに関する、必要な追加プロパティ情報を入力します。

ステップ 7　[Save] をクリックします。

新しい Cisco IOS デバイスがリストされて、[Devices] ウィンドウが再表示されます。

ターミナル サーバの作成

ターミナル サーバ デバイスを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create] オプションのウィンドウが表示されます。

ステップ 3　[Terminal Server] を選択します。

[Create Terminal Server] ウィンドウが表示されます。

フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-7）
- 「ログインとパスワードの属性」（P.2-9）
- 「[Device and Configuration Access Information] の属性」（P.2-9）
- 「[SNMP v1/v2c] の属性」（P.2-10）

ステップ 4　作成しているターミナル サーバに必要な情報を入力します。

ステップ 5　[Create Terminal Server] の [Additional Properties] セクションにアクセスするには、[Show] をクリックします。

[Additional Properties] ウィンドウが表示されます。

[Additional Properties] フィールドの説明については、次の項を参照してください。

- 「SNMP v3 属性」（P.2-10）
- 「[Terminal Server] オプションの属性」（P.2-11）
- 「[Device Platform Information] の属性」（P.2-11）

ステップ 6　作成しているターミナル サーバ デバイスに関する、必要な追加プロパティ情報を入力します。

ステップ 7　[Save] をクリックします。

新しいターミナル サーバ デバイスがリストされて、[Devices] ウィンドウが再表示されます。

一般属性

[General Attributes] セクションには、次のフィールドが含まれています。

- [Device Host Name]（必須）：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。

- [Device Domain Name]（任意）：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。名前は、ターゲット ルータ デバイスのドメイン名と一致させる必要があります。
- [Description]（任意）：80 文字に制限されています。デバイスのタイプ、デバイスの場所、サービス プロバイダー オペレータを支援するその他の情報など、デバイスに関する情報を含めることができます。
- [Collection Zone]（任意）：Prime Provisioning 内のすべての収集ゾーンのドロップダウン リスト。選択肢には、[None] および Prime Provisioning 内のすべての収集ゾーンがあります。デフォルト：[None]。
- [Management IP Address] : Prime Provisioning がターゲット ルータ デバイスの設定に使用するデバイスの有効な IP アドレス。
- [Element Management Key]: デバイス（Prime Provisioning）の有効な IP アドレス。
- [Interfaces]（任意）: [Edit] ボタンをクリックして、デバイスに関連付けられたすべてのインターフェイスを表示、追加、編集、および削除します。使用可能なインターフェイス フィールドの説明については、表 2-1 を参照してください。

表 2-1　Catalyst デバイス インターフェイスの作成フィールド

フィールド	説明	詳細
Interface Name	このインターフェイスの名前。	このフィールドでリストをソートできます。80 文字に制限されています。
IPV4 Address	このインターフェイスに関連付けられている IPv4 アドレス。	
IPV6 Address	このインターフェイスに関連付けられている IPv6 アドレス。	
Encapsulation	このデバイスのレイヤ 2 カプセル化。	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE

表 2-1　Catalyst デバイス インターフェイスの作成フィールド （続き）

フィールド	説明	詳細
Port Type		NONE ACCESS TRUNK ROUTED
Description	デバイス インターフェイスの説明。	デバイス インターフェイスの説明。
IP Address Type	IP アドレス タイプ。	IP アドレス タイプ。

- [Associated Groups]（任意）: [Edit] ボタンをクリックして、デバイス グループのすべての関連付けを表示、追加、および削除します。

ログインとパスワードの属性

[Login and Password Information] セクションには、次のフィールドが含まれています。

- [Login User]（任意）: Prime Provisioning では必要ありません。ただし、Prime Provisioning はデバイスにアクセスできないため、[Login User] と [Login Password] がないと収集とアップロードまたはダウンロードは機能しません。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Login Password]（任意）: Prime Provisioning では必要ありません。ただし、Prime Provisioning はデバイスにアクセスできないため、[Login User] と [Login Password] がないと収集とアップロードまたはダウンロードは機能しません。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Verify Login Password]（任意）: [Login Password] フィールドと一致する必要があります。80 文字に制限されています。
- [Enable User]（任意）: Prime Provisioning では必要ありません。ただし、収集およびアップロードまたはダウンロードは、ログイン ユーザが EXEC モードでルータを設定するのに十分な特権を持っている場合にだけ機能します。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Enable Password]（任意）: Prime Provisioning では必要ありません。ただし、収集およびアップロードまたはダウンロードは、ログイン ユーザが EXEC モードでルータを設定するのに十分な特権を持っている場合にだけ機能します。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Verify Enable Password]（任意）: [Enable Password] フィールドと一致する必要があります。80 文字に制限されています。

[Device and Configuration Access Information] の属性

[Device and Configuration Access Information] セクションには、次のフィールドが含まれています。

- [Terminal Session Protocol]（任意）: Prime Provisioning とデバイスの間の通信方式を設定します。選択肢には、[Telnet]、[Secure Shell（SSH）]、[CNS]、[RSH]、および [SSH version 2（SSHv2）] があります。前のバージョンの Prime Provisioning では、このフィールドは [Transport] フィールドと呼ばれていました。デフォルト：DCPL プロパティで設定されるデフォルト。

- [Config Access Protocol]（任意）：設定のアップロードおよびダウンロード用のアクセス プロトコルを管理します。選択肢には、[Terminal]、[TFTP]、[FTP]、および [RCP] があります。デフォルト：DCPL プロパティで設定されるデフォルト。
- [OS]（任意）：選択肢には、[IOS] および [IOS_XR] があります。シスコ デバイスを作成したり、ターミナル サーバを作成するために適用できます。
- [SNMP Version]（任意）：デバイスと通信する場合に使用する SNMP バージョンを設定します。選択肢には、[SNMP v1/v2c] および [SNMP v3] があります。デフォルト：DCPL プロパティで設定されるデフォルト。

[SNMP v1/v2c] の属性

[SNMP v1/v2c] セクションには、次のフィールドが含まれています。

- [Community String RO]（任意）：SNMP Read-Only コミュニティ ストリング。多くのタスクが SNMP を使用してデバイスにアクセスします。このフィールドは、ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。
- [Community String RW]（任意）：SNMP Read-Write コミュニティ ストリング。多くのタスクが SNMP を使用してデバイスにアクセスします。このフィールドは、ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。

SNMP v3 属性

[SNMP v3] セクションには、次のフィールドが含まれています。

- [SNMP Security Level]（任意）：選択肢には、[Default]（<*default_set_in_DCP*L>）、[Authentication/No Encryption]、[Authentication/Encryption]、および [No Authentication/No Encryption] があります。Default：デフォルト（<*default_set_in_DCP*L>）。注 :DCPL プロパティを変更すると、<*default_set_in_DCPL*> 変数は変更されます。
- [Authentication User Name]（任意）：指定したデバイス ルータに対して設定されるユーザ名。ユーザには、セキュリティ要求で指定したオブジェクト ID（OID）番号に対する権限が必要です（set 要求に対する書き込み権限、および get 要求に対する読み取り権限）。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。80 文字に制限されています。
- [Authentication Password]（任意）：[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Verify Authentication Password]（任意）：[Encryption Password] フィールドと一致する必要があります。80 文字に制限されています。
- [Authentication Algorithm]（任意）：[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。選択肢には、[None]、[MD5]、および [SHA] があります。デフォルト：[None]。
- [Encryption Password]（任意）：前のバージョンの Prime Provisioning では、このフィールドは、[Privacy Password] と呼ばれていました。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。[SNMP Security Level] が [Authentication/Encryption] の場合は、プロビジョニングする必要があります。80 文字に制限されています。
- [Verify Encryption Password]（任意）：[Encryption Password] フィールドと一致する必要があります。80 文字に制限されています。

- [Encryption Algorithm]（任意）：前のバージョンの Prime Provisioning では、このフィールドは、[Privacy Protocol] と呼ばれていました。[SNMP Security Level] が [Authentication/Encryption] の場合は、プロビジョニングする必要があります。選択肢には、[None] および [DES 56] があります。デフォルト：[None]。

[Terminal Server] オプションの属性

[Terminal Server] オプションのセクションには、次のフィールドが含まれます。

- [Terminal Server]（任意）：選択肢には、[None] や既存のターミナル サーバ名のリストなどがあります。デフォルト：[None]。
- [Port]（任意）：ターミナル サーバが選択されるまでディセーブルです。範囲は 0 ～ 65535 です。デフォルト：[0]。

  次のフィールドは、シスコ デバイスを作成するときにも使用できます。

  - [Fully Managed]（任意）：[Fully Managed] チェックボックスがオンの場合、デバイスは、完全管理対象デバイスになります。Prime Provisioning は、完全管理対象デバイスに対してだけ追加の管理操作を実行します。これらの操作には、Prime Provisioning の外部から行われたデバイス設定変更を受信した際の電子メール通知および侵入の可能性を検出するための強制監査タスクのスケジューリングが含まれます。デフォルトはオフ、つまり、選択されていません。
  - [Device State]（任意）：選択肢には、[ACTIVE] や [INACTIVE] などがあります。[ACTIVE] は、ルータがネットワークに組み込まれていて、コンフィギュレーションの収集やプロビジョニングなど、Prime Provisioning タスクの一部として使用できることを示します。[INACTIVE] は、ルータが組み込まれていないことを示します。デフォルト：[ACTIVE]。
  - [CNS Identification]：[Device Event Identification] フィールドを [CNS_ID] に設定する場合に必要です。Cisco IOS で許可される有効な文字は、英数字と（.）、(-)、(_）だけです。
  - [Device Event Identification]（任意）：[CNS Identification] フィールドに [HOST_NAME] または [CNS_ID] が含まれていることを示します。デフォルト：[HOST_NAME]。
  - [Most Recent CNS event]（任意）：選択肢には、[None]、[CONNECT]、[DISCONNECT] などがあります。デフォルトから [None] への変更は、推奨されません。（注）各 CNS-enabled IOS デバイスについて Prime Provisioning によって受信される CNS TIBCO の最後の接続または接続解除イベントは、自動的に記録されます。
  - [IE2100]（任意）：[Device State] フィールドが [INACTIVE] でない場合、または [Terminal Session Protocol] フィールドが [CNS] でない場合はディセーブルです。 [Terminal Session Protocol] が [CNS] の場合、有効な [IE2100] を選択する必要があります。選択肢には、[None] および既存の IE2100 名のリストすべてが含まれています。デフォルト：[None]。
  - [Cisco Configuration Engine Software Version]（任意）：選択肢には、[1.3]、[1.3.1]、[1.3.2]、[1.4]、[1.5]、[2.0]、[3.0]、[3.5] などがあります。これは、IOS デバイスを管理する Cisco Configuration Engine のリリースのバージョンです。デフォルト：[1.4]。
  - [CNS Device Transport]（任意）：選択肢には、[HTTP] や [HTTPS] などがあります。このフィールドは、Cisco Configuration Engine リポジトリで、デバイスを作成、削除、または編集するために Prime Provisioning が使用する転送メカニズムを決定します。[HTTPS] を使用する場合、Cisco Configuration Engine をセキュア モードで実行する必要があります。デフォルト：[HTTP]。

[Device Platform Information] の属性

[Device Platform Information] セクションには、次のフィールドが含まれています。

- [Platform]（任意）：ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。

- [Software Version]（任意）：ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。
- [Image Name]（任意）：ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。
- [Serial Number]（任意）：ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。
- [Device Owner’s Email Address]（任意）：デバイス リストから [Email] ボタンが選択されたときに、[To:] フィールドで使用されます。80 文字に制限され、有効な電子メールの形式にする必要があります。

Cisco Configuration Engine サーバの作成

（注）　Prime Provisioning で Cisco Configuration Engine サーバ機能を使用するには、*『Cisco Prime Provisioning 6.3 Installation Guide』* の付録 B「Setting Up Cisco Configuration Engine with Prime Provisioning」の説明に従って、まず Cisco Configuration Engine サーバおよび Prime Provisioning ワークステーションを設定する必要があります。Cisco IOS デバイスを作成して、Cisco Configuration Engine サーバと通信する必要もあります。付録 A「Cisco CNS デバイス アクセス プロトコルを使用した Cisco IOS デバイスの作成」を参照してください。Cisco Configuration Engine サーバは、Prime Provisioning ユーザ インターフェイス全体を通して IE2100 と呼ばれています。これは、コンフィギュレーション エンジン ソフトウェアの実行に使用されるアプリケーションのモデル番号です。

Cisco Configuration Engine サーバを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create] オプションのウィンドウが表示されます。

ステップ 3　[Cisco Configuration Engine] を選択します。

[Create New Cisco Configuration Engine] ウィンドウが表示されます。

[Create IE2100 Device] ウィンドウの [General] セクションには、次のフィールドが含まれています。

- [Host Name]（必須）：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Device Domain Name]（任意）：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。名前は、ターゲット ルータ デバイスのドメイン名と一致させる必要があります。
- [Description]（任意）：80 文字に制限されています。デバイスのタイプ、デバイスの場所、サービス プロバイダー オペレータを支援するその他の情報など、デバイスに関する情報を含めることができます。
- [IPV4 Address]（任意）：Prime Provisioning がターゲット ルータ デバイスの設定に使用する Cisco Configuration Engine サーバの有効な IPv4 アドレス。

ステップ 4　作成している Cisco Configuration Engine サーバに必要な情報を入力します。

ステップ 5　[Save] をクリックします。

新しい Cisco Configuration Engine サーバがリストされて、[Devices] ウィンドウが再表示されます。

デバイスのコピー

[Copy] ウィンドウで、選択したデバイスのコピーを受信し、それに名前を付け、値を変更できます。

[Copy] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Device] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、コピーする単一のデバイスを選択します。

ステップ 3　[Copy] ボタンをクリックします。このボタンは、1 つのデバイスが選択されている場合だけイネーブルになります。

コピー対象として選択したデバイス タイプに適切なウィンドウが表示されます。選択したデバイスの正確なコピーを受信します。ただし、Cisco IOS を実行している Catalyst スイッチの名前、管理 IP アドレス、すべてのインターフェイス、および VPNSM ブレードは空白です。必要な情報を入力し、新しいデバイスを保存する必要があります。詳細については、「デバイスの作成」（P.2-5）を参照してください。

デバイスの編集

[Edit] ウィンドウから、特定のデバイスに指定されているフィールドを変更できます。

[Edit] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるボックスをオンにして、編集する単一のデバイスを選択します。デバイス名のハイパーリンクをクリックして、編集するデバイスを選択することもできます。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのデバイスが選択されている場合だけイネーブルになります。

選択したデバイスのタイプに適切な [Edit] ウィンドウが表示されます。たとえば、Cisco IOS デバイスを選択した場合、[Edit Cisco IOS Device] ウィンドウが表示されます。

ステップ 4　選択したデバイスに対して行う変更を入力します。

ステップ 5　[Save] をクリックします。

変更が保存され、[Devices] ウィンドウが再表示されます。

デバイスの削除

[Delete] ウィンドウで、選択したデバイスをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、削除する 1 つ以上のデバイスを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のデバイスが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　[Delete] ボタンをクリックして、リストされたデバイスを削除することを確認します。

指定したデバイスが削除されて、[Devices] ウィンドウが再表示されます。

デバイス設定の編集

[Config] ウィンドウから、指定のデバイスのコンフィギュレーションを編集できます。

[Config] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、変更する単一のデバイスを選択します。

ステップ 3　[Config] ボタンをクリックします。

選択したデバイス用の [Device Configurations] ウィンドウが表示されます。

ステップ 4　変更するコンフィギュレーションの日付の左にあるボックスをオンにし、[Edit] ボタンをクリックします。このボタンは、1 つのデバイスが選択されている場合だけイネーブルになります。

選択したデバイス用の [Device Configuration] ウィンドウが表示されます。

ステップ 5　選択したデバイス設定に対して行う変更を入力します。

ステップ 6　[Save] をクリックします。

変更が保存され、[Device Configurations] ウィンドウが再表示されます。

ステップ 7　[OK] をクリックし、[Devices] ウィンドウに戻ります。

デバイスの所有者への電子メールの送信

[E-mail] ウィンドウから、電子メールを使用して、指定のデバイスの所有者にデバイス レポートを送信できます。

[E-mail] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、デバイス レポートを送信するデバイスを選択します。

ステップ 3　[E-mail] ボタンをクリックします。このボタンは、1 つ以上のデバイスが選択されている場合だけイネーブルになります。

[Send Mail to Device Owners] ウィンドウが表示されます。

ステップ 4　選択したデバイスの所有者に送信する電子メールを作成します。

ステップ 5　[Send] をクリックします。

電子メールが送信され、[Devices] ウィンドウが再表示されます。

デバイス設定の収集

タスク マネージャの Collect Configuration タスクを使用して、リポジトリのデバイスにインターフェイス設定を追加することを推奨します。タスク マネージャの Collect Configuration タスクはネットワークの物理デバイスに接続し、ルータからデバイス情報（インターフェイス設定を含む）を収集して、その情報を Prime Provisioning リポジトリに入力します。

タスク マネージャの Collect Configuration タスクを使用してデバイス インターフェイスの設定を追加する方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

デバイス設定と Prime Provisioning リポジトリの同期

（注）　診断の精度は最新のデバイス情報に依存します。デバイス設定に何らかの変更を加えた後および定期的に、デバイス設定を物理デバイスと再同期することを推奨します。これにより、Prime Provisioning インベントリに保持されているデバイス設定がネットワークの物理デバイスと一致します。

タスク マネージャのスケジュール タスクを使用して、デバイス設定を最新に保つことを推奨します。Collect Configuration と Collect Configuration from File のどちらでも使用できます。タスク マネージャの Collect Configuration スケジュール タスクの作成方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。MPLS ネットワークの PE および P ルータは、すべてがタスク マネージャのスケジュール タスク Collect Configuration を使用してその設定を収集する必要があります。タスク マネージャの Collect Configuration タスクでは、インターフェイス設定およびその他のデバイス属性の詳細が収集されます。タスク マネージャの Collect Configuration タスクの実行スケジュール間隔は、ネットワークに対する設定変更の頻度に依存します。タスク マネージャの Collect Configuration タスクを各 P および PE ルータで毎日実行することを推奨します。

プロバイダー

ここでは、プロバイダーを作成し、管理する方法について説明します。この項では、次のトピックについて取り上げます。

- 「プロバイダーの作成」（P.2-16）
- 「プロバイダーの編集」（P.2-16）

- 「プロバイダーの削除」（P.2-17）

プロバイダーの作成

[Create Provider] ウィンドウから、さまざまなプロバイダーを作成できます。

プロバイダーを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Providers] を選択します。

[Providers] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Provider] ウィンドウが表示されます。

[Create Provider] ウィンドウには、次のフィールドが含まれています。

- [Name]（必須）：先頭は文字にする必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。80 文字に制限されています。
- [BGP AS]（必須）：各 BGP 自律システムには、IP ネットワーク番号を割り当てる同じ中央認証局によって一意の 16 ビットの番号が割り当てられます。範囲：1 ～ 65535。
- [Contact Information]（任意）：サービス プロバイダーのオペレータにとって役に立つプロバイダーに関する関連情報。256 文字に制限されています。

ステップ 3　作成しているプロバイダーの名前、[BGP AS]、および連絡先情報を入力します。

ステップ 4　[Save] をクリックします。

[Providers] ウィンドウが再表示され、新しいプロバイダーが示されます。

プロバイダーの編集

[Edit Provider] ウィンドウから、特定のプロバイダーに指定されているフィールドを変更できます。

[Edit Provider] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Providers] を選択します。

[Providers] ウィンドウが表示されます。

ステップ 2　プロバイダー名の左にあるチェックボックスをオンにして、変更する単一のプロバイダーを選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのカスタマーが選択されている場合だけイネーブルになります。

[Edit Provider] ウィンドウが表示されます。

ステップ 4　選択したプロバイダーに対して行う変更を入力します。

ステップ 5　[Save] をクリックします。

変更が保存され、[Providers] ウィンドウが再表示されます。

プロバイダーの削除

[Delete] ウィンドウで、選択したプロバイダーをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Providers] を選択します。

[Providers] ウィンドウが表示されます。

ステップ 2　プロバイダー名の左にあるチェックボックスをオンにして、削除するプロバイダーを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のプロバイダーが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　[Delete] ボタンをクリックして、リストされたプロバイダーを削除することを確認します。

指定したプロバイダーが削除されて、[Providers] ウィンドウが再表示されます。

プロバイダー リージョン

プロバイダー リージョンは、1 つの BGP 自律システム内のプロバイダー エッジ ルータ（PE）のグループであると見なされます。プロバイダー リージョンを定義する主な目的は、プロバイダーがヨーロッパ、アジア太平洋などの広い地域で一意の IP アドレス プールを使用できるようにすることです。

ここでは、次の内容について説明します。

- 「プロバイダー リージョンの作成」（P.2-17）
- 「プロバイダー リージョンの編集」（P.2-18）
- 「プロバイダー リージョンの削除」（P.2-18）

プロバイダー リージョンの作成

[Create Provider Region] ウィンドウから、さまざまな PE リージョンを作成できます。

プロバイダー リージョンを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Regions] を選択します。

[Provider Regions] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Provider Regions] ウィンドウが表示されます。

ステップ 3　作成しているプロバイダーの名前および情報を入力します。プロバイダー名を入力するには、次のステップを実行します。

a.　[Provider] フィールドの隣の [Select] ボタンをクリックします。

プロバイダー名のリストが表示されます。

b.　プロバイダー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customer Site] ウィンドウが再表示されます。

プロバイダー リージョンの編集

[Edit Provider Regions] ウィンドウから、特定のプロバイダー リージョンに指定されているフィールドを変更できます。

[Edit Provider Regions] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Regions] を選択します。

[Provider Regions] ウィンドウが表示されます。

ステップ 2　PE リージョン名の左にあるチェックボックスをオンにして、変更する単一のサイト名を選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つの PE リージョン名が選択されている場合だけイネーブルになります。

[Edit Provider Region] ウィンドウが表示されます。

ステップ 4　選択したプロバイダー リージョンに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Provider Region] ウィンドウが再表示されます。

プロバイダー リージョンの削除

[Delete] ウィンドウで、選択したプロバイダー リージョンをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Regions] を選択します。

[Provider Regions] ウィンドウが表示されます。

ステップ 2　PE リージョン名の左にあるチェックボックスをオンにして、削除する 1 つ以上のリージョンを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上の PE リージョン名が選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたリージョン名を削除することを確認します。指定した PE リージョン名が削除されて、[Provider Regions] ウィンドウが再表示されます。

プロバイダー デバイス

PE デバイス機能では、PE エディタまたはインベントリ マネージャを使用してリージョンに関連付けられたプロバイダー エッジ（PE）ルータのリストが提供されます。

具体的な内容は、次のとおりです。

- 「プロバイダー デバイスの作成」（P.2-19）
- 「プロバイダー デバイスの編集」（P.2-19）
- 「プロバイダー デバイスの削除」（P.2-20）

プロバイダー デバイスの作成

[Create Provider Device] ウィンドウから、さまざまな PE リージョンを作成できます。

プロバイダー リージョンを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Devices] を選択します。

[PE Devices] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create New Provider Devices] ウィンドウが表示されます。

ステップ 3　デバイス名を入力するには、次のステップを実行します。

a.　[Device Name] フィールドの横にある [Select] ボタンをクリックします。

[Device Name] ウィンドウのリストが表示されます。

b.　デバイス名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　PE リージョン名を入力するには、次のステップを実行します。

a.　[PE Region Name] フィールドの横にある [Select] ボタンをクリックします。

[Region Name] ウィンドウのリストが表示されます。

b.　デバイス名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 5　ドロップダウン リストから [PE Role Type] を選択します。選択肢は、[N-PE]、[U-PE]、[P] および [PE-AGG] です。

ステップ 6　6VPE の横にあるチェックボックスをオンにします。

ステップ 7　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Provider Device] ウィンドウが再表示されます。

プロバイダー デバイスの編集

[Edit Provider Device] ウィンドウから、特定のプロバイダー リージョンに指定されているフィールドを変更できます。

[Edit Provider Devices] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Devices] を選択します。

[PE Devices] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、変更する単一のサイト名を選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つの PE デバイス名が選択されている場合だけイネーブルになります。

[Edit Provider Region] ウィンドウが表示されます。

ステップ 4　選択した PE デバイス名に対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Provider Device] ウィンドウが再表示されます。

プロバイダー デバイスの削除

[Delete] ウィンドウで、選択したプロバイダー デバイスをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Provider Devices] を選択します。

[PE Devices] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、削除する 1 つ以上のリージョンを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上の PE デバイス名が選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたプロバイダー デバイスを削除することを確認します。指定したプロバイダー デバイスが削除されて、[Provider Devices] ウィンドウが再表示されます。

[Inventory Manager] ウィンドウの使用

インベントリ マネージャにアクセスするには、[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

[Inventory Manager] ウィンドウから、デバイスをインポートすることや、デバイス、プロバイダー、またはカスタマーのリストを開くことができます。

具体的な内容は、次のとおりです。

- 「デバイスのインポート」（P.2-21）
- 「デバイスのオープンおよび編集」（P.2-21）
- 「PE のオープンおよび編集」（P.2-22）
- 「CE のオープンおよび編集」（P.2-23）
- 「デバイスの割り当て」（P.2-28）

デバイスのインポート

デバイスをインポートするには、そのデバイスが、Prime Provisioning を実行している同じサーバの既存のディレクトリに存在している必要があります。デバイスは、Prime Provisioning リポジトリにインポートした後に、必要に応じてカスタマーまたはプロバイダーに割り当てることができます。

コンフィギュレーション ファイルとともにデバイスをインポートするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

ステップ 2　[Import Devices] ボタンをクリックします。

[Import Devices from Configuration Files] ウィンドウが表示されます。

ステップ 3　[Select] ボタンをクリックします。

[Select Device Configuration File] ウィンドウが表示されます。

ステップ 4　[Select Device Configuration File] ウィンドウで、コンフィギュレーション ファイルが格納されている Prime Provisioning サーバ上のディレクトリを入力し、[Import Devices from Configuration Files] ウィンドウを表示します。

ステップ 5　コンフィギュレーション ファイル名の左のチェックボックスをオンにすることで、インポートするコンフィギュレーション ファイルを必要なだけ選択します。

ステップ 6　複数のディレクトリからデバイスをインポートする場合、ステップ 3 ～ 6 を繰り返します。

ステップ 7　[Import] をクリックします。

追加情報を含む [General Attributes] ウィンドウが表示されます。

ステップ 8　[Save] をクリックします。

デバイスのオープンおよび編集

一括編集のためにデバイス コンフィギュレーション ファイル ファイルを開くには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

ステップ 2　[Open] ボタンをクリックします。

[Open] ドロップダウン リストが表示されます。[Open] オプションには、次のものがあります。

- [Devices] : Prime Provisioning が管理するすべてのネットワーク要素。

（注）　PE を編集するには、[Devices] *ではなく* [Provider] を開きます。

- [Provider] : 特定のプロバイダーに属する PE。
- [Customer] : 特定のカスタマーに属する CE。

ステップ 3　[Devices] を選択します。

[Select Device] ウィンドウが表示されます。

ステップ 4　デバイス名の左のチェックボックスをオンにすることで、開くデバイスを選択します。開くデバイスを複数選択できます。

ステップ 5　[Select] ボタンをクリックします。

[General Attributes] ウィンドウが表示され、選択したデバイスに関する情報が示されます。

ステップ 6　特定の属性を表示するには、[Attributes] ボタンをクリックします。

[Attributes] オプションのウィンドウが表示されます。

ステップ 7　表示する属性のタイプを選択します。

これらの属性フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-24）
- 「パスワード属性」（P.2-25）
- 「SNMP の属性」（P.2-25）
- 「CNS の属性」（P.2-26）
- 「プラットフォーム属性」（P.2-26）
- 「インターフェイス」（P.2-27）

ステップ 8　属性を一括編集するには、次の作業を行います。

a.　デバイス名の左のチェックボックスを 1 つ以上オンにします。

b.　属性名列の上のチェックボックスをオンにします。

c.　[Edit] ボタンをクリックします。

ステップ 9　必要な変更を入力します。

ステップ 10　[Save] をクリックします。

これにより、変更内容が保存されます。

PE のオープンおよび編集

一括編集のために PE ファイル ファイルを開くには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

ステップ 2　[Open] ボタンをクリックします。

[Open] ドロップダウン リストが表示されます。[Open] オプションには、次のものがあります。

- [Devices]：Prime Provisioning が管理するすべてのネットワーク要素。
- [Provider]：特定のプロバイダーに属する PE。
- [Customer]：特定のカスタマーに属する CE。

ステップ 3　[Provider] を選択します。

[Select Provider] ウィンドウが表示されます。

ステップ 4　プロバイダー名の左側にあるオプション ボタンをクリックして、プロバイダーを選択します。

ステップ 5　[Select] ボタンをクリックします。

[General Attributes Provider] ウィンドウが表示され、選択したプロバイダーに割り当てられた PE が示されます。

ステップ 6　特定の属性を表示するには、[Attributes] ボタンをクリックします。

[Attributes] オプションのウィンドウが表示されます。

ステップ 7　表示する属性のタイプを選択します。

これらの属性フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-24）
- 「パスワード属性」（P.2-25）
- 「SNMP の属性」（P.2-25）
- 「CNS の属性」（P.2-26）
- 「プラットフォーム属性」（P.2-26）
- 「PE の属性」（P.2-28）
- 「インターフェイス」（P.2-27）

ステップ 8　属性を一括編集するには、次の作業を行います。

a.　ホストまたはデバイス名の左のチェックボックスを 1 つ以上オンにします。

b.　属性名列の上のチェックボックスをオンにします。

c.　[Edit] ボタンをクリックします。

ステップ 9　必要な変更を入力します。

ステップ 10　[Save] をクリックします。

これにより、変更内容が保存されます。

CE のオープンおよび編集

一括編集のために CE ファイル ファイルを開くには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

ステップ 2　[Open] ボタンをクリックします。

[Open] ドロップダウン リストが表示されます。[Open] オプションには、次のものがあります。

- [Devices]：Prime Provisioning が管理するすべてのネットワーク要素。
- [Provider]：特定のプロバイダーに属する PE。
- [Customer]：特定のカスタマーに属する CE。

ステップ 3　カスタマーの選択

[Select Customer] ウィンドウが表示されます。

ステップ 4　カスタマー名の左側にあるオプション ボタンをクリックして、カスタマーを選択します。

ステップ 5　[Select] ボタンをクリックします。

[General Attributes Customer] ウィンドウが表示され、選択したカスタマーに割り当てられている CE が示されます。

ステップ 6　特定の属性を表示するには、[Attributes] ボタンをクリックします。

[Attributes] オプションのウィンドウが表示されます。

ステップ 7　表示する属性のタイプを選択します。

これらの属性フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-24）

- 「パスワード属性」（P.2-25）
- 「SNMP の属性」（P.2-25）
- 「CNS の属性」（P.2-26）
- 「プラットフォーム属性」（P.2-26）
- 「CPE の属性」（P.2-28）
- 「インターフェイス」（P.2-27）

ステップ 8　属性を一括編集するには、次の作業を行います。

a. ホストまたはデバイス名の左のチェックボックスを 1 つ以上オンにします。

b. 属性名列の上のチェックボックスをオンにします。

c. [Edit] ボタンをクリックします。

ステップ 9　必要な変更を入力します。

ステップ 10　[Save] をクリックします。

これにより、変更内容が保存されます。

一般属性

[General Attributes Devices] ウィンドウには、次の項目が含まれます。

- [Host]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Device Type]：デバイス タイプには次のデバイスが含まれます。
  - Cisco ルータ
  - Catalyst OS デバイス
  - ターミナル サーバ
  - IE2100（Cisco Configuration Engine サーバ）
- [Description]：デバイスのタイプ、デバイスの場所、サービス プロバイダー オペレータを支援するその他の情報など、デバイスに関する情報を含めることができます。80 文字に制限されています。
- [Management IP Address]：Prime Provisioning がターゲット ルータ デバイスの設定に使用するデバイスの有効な IP アドレス。この IP アドレスは、Prime Provisioning ホストから到達可能である必要があります。
- [Device Domain Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。名前は、ターゲット ルータ デバイスのドメイン名と一致させる必要があります。
- [Terminal Session Protocol]：Prime Provisioning とデバイスの間の通信方式を設定します。選択肢には、[Telnet]、[Secure Shell（SSH）]、[SSH version 2（SSHv2）]、[CNS]、および [RSH] があります。デフォルト：[Telnet]。
- [Config Access Protocol]：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用のアクセス プロトコルを管理します。選択肢には、[Terminal]、[TFTP]、[FTP]、および [RCP] があります。デフォルト：[Terminal]

- [Device Groups]：デバイス グループの名前を示します。このカラムのデバイス グループは、追加または変更できます。

パスワード属性

[Password Attributes Devices] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Login User]：Prime Provisioning では必要ありません。ただし、Prime Provisioning はデバイスにアクセスできないため、[Login User] と [Login Password] がないと収集とアップロードまたはダウンロードは機能しません。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Login Password]：アスタリスク（*）で表示されます。Prime Provisioning では必要ありません。ただし、Prime Provisioning はデバイスにアクセスできないため、[Login User] と [Login Password] がないと収集とアップロードまたはダウンロードは機能しません。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Enable User]：Prime Provisioning では必要ありません。ただし、収集およびアップロードまたはダウンロードは、ログイン ユーザが EXEC モードでルータを設定するのに十分な特権を持っている場合にだけ機能します。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Enable Password]：アスタリスク（*）で表示されます。Prime Provisioning では必要ありません。ただし、収集およびアップロードまたはダウンロードは、ログイン ユーザが EXEC モードでルータを設定するのに十分な特権を持っている場合にだけ機能します。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Community String RO]：多くのタスクが SNMP を使用してデバイスにアクセスします。このフィールドは、ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。
- [Community String RW]：多くのタスクが SNMP を使用してデバイスにアクセスします。このフィールドは、ターゲット ルータ デバイスで設定されているものと一致する必要があります。80 文字に制限されています。

SNMP の属性

[SNMP Attributes Devices] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [SNMP Version]：選択肢には、[SNMP v1/v2c] および [SNMP v3] があります。デフォルト値は、DCPL プロパティ SnmpService\defaultSNMPVersion の設定によって決まります。（詳細については、Appendix B, “Property Settings” を参照してください）。
- [Security Level]：選択肢には、[No Authentication/No Encryption]、[Authentication/No Encryption]、および [Authentication/Encryption] があります。デフォルト :[No Authentication/No Encryption]。
- [Authentication User Name]：指定したデバイス ルータに対し設定されるユーザ名。ユーザには、セキュリティ要求で指定したオブジェクト ID（OID）番号に対する権限が必要です（set 要求に対する書き込み権限、および get 要求に対する読み取り権限）。ターゲット ルータ デバイスで設定さ

れている内容と一致させる必要があります。[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。80 文字に制限されています。

- [Authentication Password]：アスタリスク（*）で表示されます。[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- Authentication Algorithm：[SNMP Security Level] が [Authentication/No Encryption] または [Authentication/Encryption] の場合は、プロビジョニングする必要があります。選択肢には、[None]、[MD5]、および [SHA] があります。デフォルト：[None]。
- [Encryption Password]：アスタリスク（*）で表示されます。前のバージョンでは、このフィールドは、[Privacy Password] と呼ばれていました。ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。[SNMP Security Level] が [Authentication/Encryption] の場合は、プロビジョニングする必要があります。80 文字に制限されています。
- [Encryption Algorithm]：前のバージョンでは、このフィールドは、[Privacy Protocol] と呼ばれていました。[SNMP Security Level] が [Authentication/Encryption] の場合は、プロビジョニングする必要があります。選択肢には、[None] および [DES 56] があります。デフォルト：[None]。

CNS の属性

[CNS Attributes Devices] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [IE2100 Name]：[Device State] フィールドが [Inactive] でない場合、または [Terminal Session Protocol] フィールドが [CNS] でない場合はディセーブルです。 [Terminal Session Protocol] が [CNS] の場合、有効な Cisco Configuration Engine サーバを選択する必要があります。選択肢には、[None] および既存の Cisco Configuration Engine サーバ名のリストがあります。デフォルト：[None]。
- [Device State]：選択肢には、[Active] と [Inactive] があります。[Active] は、ルータがネットワークに組み込まれていて、コンフィギュレーションの収集やプロビジョニングなど、Prime Provisioning タスクの一部として使用できることを示します。[Inactive] は、ルータが組み込まれていないことを示します。デフォルト：[Active]。
- [Event Identification]：[CNS Identification] フィールドに [HOST NAME] または [CNS ID] のいずれが含まれるかを示します デフォルト：[HOST NAME]。
- [CNS Identification]：[Event Identification] フィールドを [CNS ID] に設定する場合に必要です。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。

プラットフォーム属性

[Platform Attributes Devices] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Platform]：ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。

- [Software Version]：ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Image Name]：ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。
- [Serial Number]：ターゲット ルータ デバイスで設定されている内容と一致させる必要があります。80 文字に制限されています。

インターフェイス

[Interfaces Devices] ウィンドウには、次の項目が含まれます。

- [Host]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Interface Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須です。256 文字に制限されています。
- [Interface Type]：インターフェイスのタイプを指定します。これは表示専用フィールドです。
- [Interface Description]：インターフェイスの説明。このフィールドは、表示専用です。コンフィギュレーション ファイルをインポートすると、フィールドに入力されます。
- [Interface IP Address]：このインターフェイスに関連付けられた IPv4 アドレス。
- [Interface IPv6 Address]：このインターフェイスに関連付けられた IPv6 アドレス。
- [Encapsulation]：このデバイスのレイヤ 2 カプセル化。これは表示専用フィールドです。有効な値は次のとおりです。
  - DEFAULT
  - DOT1Q
  - ETHERNET
  - ISL
  - FRAME_RELAY
  - FRAME_RELAY_IETF
  - HDLC
  - PPP
  - ATM
  - AAL5SNAP
  - AAL0
  - AAL5
  - AAL5MUX
  - AAL5NLPID
  - AAL2
  - ENCAP_QinQ
  - GRE
- [Port Type]：選択肢には、[Access]、[Trunk]、[Routed]、および [None] があります。

PE の属性

[PE Attributes Provider] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Provider]：プロバイダーの名前を示します。先頭は英字にする必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。80 文字に制限されています。プロバイダー名でリストをソートできます。
- [Region]：リージョンの名前を示します。先頭は英字にする必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。80 文字に制限されています。リージョン名でリストをソートできます。
- [Role]：選択肢には、[N-PE]、[U-PE]、[P]、[PE_AGG] があります。
- [Loopback Interface]：ループバック アドレスは、デバイス上のループバック インターフェイスの IP アドレスです。このフィールドで 1 つのループバック インターフェイスを選択し、そのループバック インターフェイスの IP アドレスを使用できます。
- [Managed]:Prime Provisioning によってプロビジョニングされます。[yes] のチェックボックスをオンにします。デフォルトは [no] です。

CPE の属性

[CPE Attributes Customer] ウィンドウには、次の項目が含まれます。

- [Device Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Customer]：顧客の名前を示します。先頭は英字にする必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。80 文字に制限されています。カスタマー名でリストをソートできます。
- [Site]：サイトの名前を示します。先頭は英字にする必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。80 文字に制限されています。サイト名順にリストをソートできます。
- [Management Type]：選択肢には、[Managed]、[Unmanaged]、[Managed - Management LAN]、[Unmanaged - Management LAN]、[Directly Connected]、[Directly Connected Management Host]、[Multi-VRF]、および [Unmanaged Multi-VRF] があります。

デバイスの割り当て

デバイスをプロバイダーまたはカスタマーに割り当てるには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

ステップ 2　[Open] ボタンをクリックします。

[Open] ドロップダウン リストが表示されます。

ステップ 3　[Devices] を選択します。

[Select Device] ウィンドウが表示されます。

ステップ 4　デバイス名の左のボックスをオンにすることで、開くデバイスを選択します。開くデバイスを複数選択できます。

ステップ 5　[Select] ボタンをクリックします。

[General Attributes - Devices] ウィンドウが表示され、選択したデバイスに関する情報が示されます。

ステップ 6　[Assign CE/PE] ボタンをクリックします。

ステップ 7　[Customer] または [Provider] を選択します。

対応する [Select Customer] ウィンドウまたは [Select Provider] ウィンドウが表示されます。

ステップ 8　カスタマー名またはプロバイダー名の左側にあるチェックボックスをオンにして、デバイスを割り当てるプロバイダーまたはカスタマーを選択します。

ステップ 9　[Select] ボタンをクリックします。

プロバイダーにデバイスを割り当てた場合は、[PE Attributes] ウィンドウが表示されます。カスタマーにデバイスを割り当てた場合は、[CPE Attributes] ウィンドウが表示されます。

ステップ 10　Prime Provisioning リポジトリに割り当てられたデバイスを保存するには、[CPE Attributes] ウィンドウでサイトを指定するか、[PE Attributes] ウィンドウでリージョンを指定する必要があります。次の操作を行います。

a. デバイス名の左のチェックボックスを 1 つ以上オンにします。

b. [Site] 列または [Region] 列の上のチェックボックスをオンにします。

c. [Edit] ボタンをクリックします。[Edit Attributes] ウィンドウが表示されます。

d. [Select] をクリックします。[Select Site] ウィンドウまたは [Select Region] ウィンドウが表示されます。

e. サイト名またはリージョン名の左側のチェックボックスをオンにして、サイトまたはリージョンを選択します。

f. [Save] をクリックします。

ステップ 11　必要に応じて、属性の編集を選択できます。必要な変更を入力します。

ステップ 12　[Save] をクリックします。

PE または CPE は、Prime Provisioning リポジトリに保存されます。

デバイス グループ

Cisco Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義する必要があります。ネットワーク要素をデバイスとして定義した後、収集および管理の目的で、デバイスをグループに編成できます。

ここでは、デバイス グループを作成、編集、および削除する方法、ならびにデバイス グループの所有者に電子メールを送信する方法について説明します。この項では、次のトピックについて取り上げます。

デバイス グループの作成

[Create Device Group] ウィンドウから、さまざまなデバイス グループを作成できます。

デバイス グループを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Device Groups] を選択します。

[Device Groups] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Device Group] ウィンドウが表示されます。

ステップ 3　作成しているデバイス グループの名前および説明を入力します。

ステップ 4　[Edit] をクリックします。

[Select Group Members] ウィンドウが表示されます。

ステップ 5　デバイス名の左にあるチェックボックスをオンにして、グループ メンバーにするデバイスを選択します。

ステップ 6　[OK] をクリックします。

選択したデバイスをリストした [Create Device Group] ウィンドウが表示されます。

ステップ 7　[Save] をクリックします。

新しいデバイス グループがリストされ、[Device Groups] ウィンドウが再表示されます。

デバイス グループの編集

[Edit Device Group] ウィンドウから、特定のデバイス グループに指定されているフィールドを変更できます。

[Edit Device Group] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Device Groups] を選択します。

ステップ 2　デバイス グループ名の左にあるチェックボックスをオンにして、変更する単一のデバイス グループを選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのデバイス グループが選択されている場合だけイネーブルになります。

[Edit Device Group] ウィンドウが表示されます。

ステップ 4　選択したデバイス グループに対して行う変更を入力します。

ステップ 5　[Save] をクリックします。

変更が保存され、[Device Groups] ウィンドウが再表示されます。

デバイス グループの削除

[Delete] ウィンドウで、選択したデバイス グループをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Device Groups] を選択します。

[Device Groups] ウィンドウが表示されます。

ステップ 2　デバイス グループ名の左にあるチェックボックスをオンにして、削除する 1 つ以上のデバイス グループを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のデバイス グループが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　[Delete] ボタンをクリックして、リストされたデバイス グループを削除することを確認します。

指定したデバイス グループが削除されて、[Device Groups] ウィンドウが再表示されます。

デバイス グループの電子メール送信

[E-mail] ウィンドウから、電子メールを使用して、指定のデバイス グループの所有者にデバイス レポートを送信できます。

[E-mail] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Device Groups] を選択します。

[Device Groups] ウィンドウが表示されます。

ステップ 2　デバイス グループ名の左にあるチェックボックスをオンにして、デバイス レポートを送信するデバイス グループを選択します。

ステップ 3　[E-mail] ボタンをクリックします。このボタンは、1 つ以上のデバイス グループが選択されている場合だけイネーブルになります。

[Send Mail to Device owners of selected groups] ウィンドウが表示されます。

ステップ 4　選択したデバイス グループの所有者に送信する電子メールを作成します。

ステップ 5　[Send] をクリックします。

電子メールが送信され、[Device Groups] ウィンドウが再表示されます。

イーサネット アクセス トポロジ情報

具体的な内容は、次のとおりです。

物理リング

物理リングには、2 ノード リングを作成する機能が表示されます。2 台以上のデバイスで、NPC リングを作成できます。

ここでは、物理リングを作成、編集、および削除する方法について説明します。この項では、次のトピックについて取り上げます。

物理リングの作成

2 台のデバイスからなるリングには、追加または編集オプションを通じて、同じリングにより多くのデバイスを追加するオプションがあります。

物理リングを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Logical Inventory] > [Physical Rings] を選択します。

[Physical Circuits] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Ring] ウィンドウが表示されます。リングには、リングを形成する 2 つ以上の物理リンクがあります。

（注）　任意の時点で、[Cancel] をクリックすると、選択したすべてが消去されます。

ステップ 3　最初の物理リンクを表す最初の行から開始します。

ステップ 4　[Source Device] 列で、[Select source device] をクリックすると、[Select Source Device - CPE/PE] のウィンドウが表示されます。

（注）　選択する CPE は、Multi-VRF CE にする*必要があります*。

ステップ 5　この物理リンクのリンク元デバイスになるデバイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Source Device] で、[Create Ring] ウィンドウが再表示されます。

（注）　物理リンクの [Source Device] を選択すると、前の物理リンク（または、最初の物理リンクを選択している場合は、最後の物理リンク）の [Destination Device] でも同じデバイスが選択されます。選択したデバイスに対して、リンク元インターフェイスとリンク先インターフェイスに同じインターフェイスを選択しないでください。

ステップ 6　この新しいバージョンの [Create Ring] ウィンドウの [Source Interface] 列で、[Select source interface] をクリックすると、[Select Source Interface] ウィンドウが、インターフェイスのリストとともに表示されます。

ステップ 7　この物理リンクのリンク元インターフェイスになるインターフェイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Source Interface] で、[Create Ring] ウィンドウが再表示されます。

ステップ 8　この新しいバージョンの [Create Rind] ウィンドウの [Destination Device] 列で、[Select destination device] をクリックすると、[Select Source Device - CPE/PE] ウィンドウが表示されます。

ステップ 9　この物理リンクのリンク先デバイスになるデバイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。

選択した [Destination Device] で、[Create Ring] ウィンドウが再表示されます。

（注）　物理リンクの [Destination Device] を選択すると、次の [Source Device] でも同じデバイスが選択されます。これらのデバイスに対して、同じインターフェイスを選択しないでください。リングに参加できるデバイスの最小台数は 2 です。

ステップ 10　この新しいバージョンの [Create Ring] ウィンドウの [Destination Interface] 列で、[Select destination interface] をクリックすると、[Select Source Interface] ウィンドウが、インターフェイスのリストとともに表示されます。

ステップ 11　この NPC の宛先インターフェイスになるインターフェイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。

選択した [Destination Interface] で、[Create Ring] ウィンドウが再表示されます。

ステップ 12　中間の物理リンクに対して、ステップ 4、最後の物理リンクに対してステップ 4 ～ステップ 7 を繰り返します。

ステップ 13　リングに追加の物理リンクを挿入する場合は、新しい物理リンクのリンク先の物理リンクを示す行のチェックボックスをオンにし、[Insert] をクリックします。ステップ 4 を実行し、新しい物理リンクの残りのエントリに入力します。

ステップ 14　リング内の物理リンクを削除する必要があり、3 つ以上の物理リンクが残る場合は、削除する物理リンクを示す行のチェックボックスをオンにし、[Delete] をクリックします。

ステップ 15　このリング内で隣接していないデバイス間に追加のクロス リンクを確立する場合は、[Create Ring] ウィンドウで [Edit Cross Links] をクリックします。エントリのない新しい [Create Ring] ウィンドウが表示されます。[Add] ボタンをクリックし、すでにリング内にあるデバイスから選択できます。その結果、このデバイスを [Source Device] として [Create Ring] ウィンドウに新しいエントリが作成されます。リングの作成時と同様に、リンク先デバイスと、リンク元およびリンク先のインターフェイスを指定します。デバイスとインターフェイスの選択は、すでにリングで確立されたものに制限されます。

（注）　クロス リンクを編集するには、リングを形成するために、最低 4 台のデバイスが必要です。

ステップ 16　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

または、リングの設定が完了したときに、[Save] をクリックします。新しいリングが [Physical Rings] ウィンドウに追加され、正常終了を示す緑色のチェックマークが表示されます。新しいリングは、リンク元のデバイス、リンク元のインターフェイスによって識別されます。

ステップ 17　3 つ以上の物理リンクでリングを作成するには、[Create Ring] ウィンドウで、挿入するリンクのチェックボックスをオンにします。[Insert] ボタンがイネーブルになります。この項の説明に従って、リンクの追加を進めます。

物理リングの編集

物理リングを編集するには、次のステップを実行します。

（注）　指定した物理リングが名前付き物理回線のいずれかに参加している場合、このリングを編集できません。NPC リングを含む NPC の ID を示すエラー メッセージが表示されます。

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

ステップ 2　NPC リングを表す行の横のチェックボックスをオンにし、[Edit] をクリックします。

[Create Ring] ウィンドウが表示され、このリングのすべてのデータが示されます。必要な変更を加えるには、「物理リングの作成」（P.2-32）と同様に作業を進めます。

ステップ 3　必要なリングを作成したら、[Save] をクリックします。[Physical Rings] ウィンドウが表示され、適切な名前（リンク元のデバイスとリンク元のインターフェイス）が示され、[Succeeded] に緑のチェックマークが表示されます。

物理リングの削除

2 つを超えるノードがあるリングでは、編集または削除オプションを使用してリング トポロジからデバイスを削除することにより、2 台のデバイス リングに変更することができます。

物理リングを削除するには、次のステップを実行します。

（注）　指定した NPC リングが名前付き物理回線のいずれかに参加している場合、このリングを削除できません。NPC リングを含む NPC の ID を示すエラー メッセージが表示されます。

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

ステップ 2　削除する NPC リングを示す行の横にあるチェックボックスをオンにし、[Delete] をクリックします。

ステップ 3　選択したリングを削除する前に気が変わった場合は、[Cancel] をクリックします。実際にリングを削除するには、[Delete] をクリックします。

[Physical Rings] ウィンドウが表示され、残りのリングの名前が示され、[Succeeded] に緑のチェックマークが表示されます。

名前付き物理回線

名前付き物理回線（NPC）は、CPE または U-PE と N-PE との間の物理的な接続を表す名前付き回線です。NPC の中間ノードは CPE と PE のいずれかです。これらは、環状に接続でき、デバイスの環を形成します。これは、NPC リングと呼ばれるエンティティによって表されます。NPC リングはデバイス（CPE または PE）と名前付き物理回線とのリング型トポロジを表します。NPC を作成するには、送信元 CPE/U-PE と宛先 N-PE とがどのように接続されているかを指定し、中間ノードを指定する必要があります。

NPC の接続は、物理リンクとして動作する一連のデバイスの指定によって定義されます。各デバイスには、NPC の接続の一部である 2 つのインターフェイスがあります。着信インターフェイスは、CE 方向からのインターフェイスを定義します。発信インターフェイスは、PE 方向へのインターフェイスを定義します。

また、リンクに NPC リングを追加（選択したデバイスの後）または挿入（選択したデバイスの前）できます。

NPC を作成する場合は、次の事項に注意してください。

- Prime Provisioning ソフトウェアで、選択するデバイスは、リンク内の任意のノードにすることができます。Prime Provisioning ソフトウェアには、適切なデバイスだけが表示されます。最初のデバイスは、CPE または U-PE である*必要があり*、最後のデバイスは、N-PE である*必要があります*。

- NPC は、MPLS マルチデバイス、VPLS、または L2VPN のサービス要求が cpe1 および pe1 を使用して作成する前に作成する必要があります。したがって、SR を作成する場合、ポリシー、cpe1、pe1、および cpe1 と pe1 間のリンクを定義する NPC を選択します。

ここでは、NPC を作成および削除し、NPC リングを作成、編集、および削除する方法について説明します。この項では、次のトピックについて取り上げます。

- 「名前付き物理回線の作成」（P.2-35）
- 「名前付き物理回線の削除」（P.2-36）

名前付き物理回線の作成

NPC の物理リンクを追加するには、次のステップを実行します。

ステップ 1　[Inventory] > [Logical Inventory] > [Named Physical Circuit] 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] ボタンをクリックします。

[Create a Named Physical Circuits] ウィンドウが表示されます。

各行は物理リンクを表し、各物理リンクには次の属性が含まれます。

- **Device**
- **Incoming Interface**
- **Outgoing Interface**
- **Ring**（任意）

（注）　NPC でリングを追加する前に、「物理リングの作成」（P.2-32）で説明するように、リンクを作成してリポジトリに保存します。

（注）　NPC では、少なくとも 1 つのリンクを定義する必要があります。リンクには 2 つのデバイス（着信インターフェイスおよび発信インターフェイス）が必要です。

ステップ 3　[Add Device] または [Insert Device] をクリックします。

[Select Device] ウィンドウが表示されます。

ステップ 4　[Show] のドロップダウン リストが [CPE] または [PE] であることを確認します。

ステップ 5　デバイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Device] で、[Create a Named Physical Circuits] ウィンドウが再表示されます。

ステップ 6　NPC にデバイスを最後の項目として追加する場合、またはチェックボックスでオンにした項目の後に追加する場合、[Create a Named Physical Circuit] ウィンドウの [Add Device] ボタンをクリックし、前のステップの説明に従って、デバイスおよびインターフェイス情報を追加します。NPC にデバイスを最初の項目として挿入する場合、またはチェックボックスでオンにした項目の前に挿入する場合、[Create a Named Physical Circuit] ウィンドウの [Insert Device] ボタンをクリックし、前のステップの説明に従って、デバイスおよびインターフェイス情報を追加します。

ステップ 7　この新しいバージョンの [Create a Named Physical Circuit] ウィンドウの [Outgoing Interface] 列で、[Select outgoing interface] をクリックすると、インターフェイスのリストとともにウィンドウが表示されます。

ステップ 8　この NPC の送信元インターフェイスになるインターフェイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Interface] で、[Create a Named Physical Circuit] ウィンドウが再表示されます。

ステップ 9　この新しいバージョンの [Create a Named Physical Circuit] ウィンドウの [Incoming Interface] 列で、[Select incoming interface] をクリックすると、インターフェイスのリストとともにウィンドウが表示されます。

ステップ 10　この NPC の着信インターフェイスになるインターフェイスの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Incoming Interface] で、[Create a Named Physical Circuit] ウィンドウが再表示されます。

ステップ 11　「物理リングの作成」（P.2-32）の説明に従って、この NPC に挿入または追加する NPC リングを作成した場合、[Insert Ring] または [Add Ring] をクリックできます。このリングが、先頭または [Insert Ring] のチェックボックスでオンにした項目の前に表示されます。あるいは、このリングが、最後または [Add Ring] のチェックボックスでオンにした項目の後に表示されます。

（注）　リングを挿入する場合は、リンク元デバイスまたは NPC に接続するリングのリンク元デバイスと、NPC のリンク先デバイスに接続するリングのリンク先デバイスを選択します。

この NPC に挿入する NPC リングを作成していない場合は、ステップ 14進みます。

ステップ 12　選択するリングの横にあるオプション ボタンをクリックし、[Select] をクリックします。選択した [Ring] で、[Create a Named Physical Circuit] ウィンドウが再表示されます。

ステップ 13　「物理リングの作成」（P.2-32）で説明されているように、不足しているデバイスとインターフェイスを選択します。

ステップ 14　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。[Create a Named Physical Circuit] ウィンドウが再表示され、新しい NPC が示されます。

名前付き物理回線の削除

NPC を削除するには、次のステップを実行します。

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　左にあるチェックボックスをオンにして、削除する 1 つ以上の NPC を選択します。

ステップ 3　[Delete] ボタンをクリックします。

[Delete NPC] ウィンドウが表示されます。

（注）　指定した NPC がいずれかのサービス要求によって使用されている場合、その NPC は削除できません。このことを説明するエラー メッセージが表示されます。

ステップ 4　[Delete] ボタンをクリックして、リストされた NPC を削除することを確認します。

指定した NPC が削除され、[Create a Named Physical Circuits] ウィンドウが再表示されます。

CPE デバイスの管理

この項では、次のトピックについて取り上げます。

カスタマー

カスタマー サイトには、VPN を使用せずに、相互に IP 接続されている一連の IP システムがあります。各カスタマー サイトは、1 社のカスタマーだけに属しています。カスタマー サイトには、1 台以上のエッジ デバイス ルータ（ロード バランシング用）が含まれることがあります。ここでは、カスタマーを作成、編集、および削除する方法について説明します。

具体的な内容は、次のとおりです。

カスタマーの作成

[Create Customer] ウィンドウから、さまざまなカスタマーを作成できます。

カスタマーを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Customers] を選択します。

[Customers] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Customer] ウィンドウが表示されます。

ステップ 3　作成しているカスタマーの名前および情報を入力します。イネーブルにする必要がある場合は、[Site of Origin Enabled] チェックボックスをオンにします。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customers] ウィンドウが再表示されます。

カスタマーの編集

[Edit Custome] ウィンドウから、特定のカスタマーに指定されているフィールドを変更できます。

[Edit Customer] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Customers] を選択します。

[Customers] ウィンドウが表示されます。

ステップ 2　カスタマー名の左にあるチェックボックスをオンにして、変更する単一のカスタマーを選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのカスタマーが選択されている場合だけイネーブルになります。

[Edit Customer] ウィンドウが表示されます。

ステップ 4　選択したカスタマーに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customers] ウィンドウが再表示されます。

カスタマーの削除

[Delete] ウィンドウで、選択したカスタマーをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Customers] を選択します。

[Customers] ウィンドウが表示されます。

ステップ 2　カスタマー名の左にあるチェックボックスをオンにして、削除する 1 つ以上のカスタマーを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のカスタマーが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたカスタマーを削除することを確認します。指定したカスタマーが削除されて、[Customer] ウィンドウが再表示されます。

カスタマー サイト

[Customer Sites] ウィンドウ機能を使用して、カスタマー サイトの作成、編集、および削除を行います。

具体的な内容は、次のとおりです。

- 「カスタマー サイトの作成」（P.2-38）
- 「カスタマー サイトの編集」（P.2-39）
- 「カスタマー サイトの削除」（P.2-39）

カスタマー サイトの作成

[Create Customer Sites] ウィンドウから、さまざまなカスタマー サイトを作成できます。

カスタマー サイトを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Sites] を選択します。

[Customer Sites] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create New Customer Sites] ウィンドウが表示されます。

ステップ 3　作成しているカスタマーの名前および情報を入力します。カスタマー名を入力するには、次のステップを実行します。

a. [Customer] フィールドの横にある [Select] ボタンをクリックします。

カスタマー名のリストが表示されます。

b. カスタマー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　サイト情報を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customer Site] ウィンドウが再表示されます。

カスタマー サイトの編集

[Edit Customer Sites] ウィンドウから、特定のカスタマー サイトに指定されているフィールドを変更できます。

[Edit Customer Sites] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Sites] を選択します。

[Customer Sites] ウィンドウが表示されます。

ステップ 2　サイト名の左にあるチェックボックスをオンにして、変更する単一のサイト名を選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのカスタマーが選択されている場合だけイネーブルになります。

[Edit Customer] ウィンドウが表示されます。

ステップ 4　選択したカスタマー サイトに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customer Site] ウィンドウが再表示されます。

カスタマー サイトの削除

[Delete] ウィンドウで、選択したカスタマー サイトをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Sites] を選択します。

[Customer Sites] ウィンドウが表示されます。

ステップ 2　サイト名の左にあるチェックボックスをオンにして、削除する 1 つ以上のカスタマー サイトを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のカスタマー サイトが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を削除しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたカスタマー サイトを削除することを確認します。指定したカスタマー サイトが削除されて、[Customer Sites] ウィンドウが再表示されます。

カスタマー デバイス

CPE 機能では、CPE エディタまたはインベントリ マネージャを使用してサイトに関連付けられた CPE のリストが提供されます。

具体的な内容は、次のとおりです。

- 「CPE デバイスの作成」（P.2-41）
- 「CPE デバイスの編集」（P.2-41）
- 「CPE デバイスの削除」（P.2-42）

[Inventory] > [Resources] > [Customer Devices] を選択すると、[CPE Devices] ウィンドウが表示されます。

[CPE Devices] ウィンドウには、次の項目が含まれます。

- [Device Name] ：デバイスの名前を示します。最初の文字は文字である必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。制限：80 文字。デバイス名でリストをソートできます。
- [Customer Name] ：カスタマーの名前を示します。最初の文字は文字である必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。制限：80 文字。カスタマー名でリストをソートできます。
- [Site Name] ：サイトの名前を示します。最初の文字は文字である必要があります。英字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。制限：80 文字。サイト名順にリストをソートできます。
- [Management Type]：CE をカスタマー サイトに関連付けるときに、[Managed] または [Unmanaged] を選択できます。これ以外の選択肢も使用できますが（下記を参照）、この主な選択肢と混同しないようにしてください。
  - [Managed]：プロバイダーは、Prime Provisioning を使用して、管理対象の CE を直接プロビジョニングできます。CE は Prime Provisioning サーバから到達可能である必要があります。
  - [Unmanaged]：プロバイダーは管理対象外 CE を直接プロビジョニングできません。[Unmanaged] を選択すると、プロバイダーは Prime Provisioning を使用してコンフィギュレーションを生成した後、コンフィギュレーションを CE に配置するようカスタマーに送ることができます。
  - [Managed]：管理対象の Management LAN や Management CE（MCE）は管理対象の CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
  - [Unmanaged - Management LAN]：管理対象外の Management LAN や MCE は管理対象外 CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
  - [Directly Connected]：ほとんどの場合、CE は PE ルータに接続されます。この場合、CE はワークステーションまたはその他のデバイスに接続されます。

- [Directly Connected Management Host]：ほとんどの場合、CE は PE ルータに接続されます。このケースでは、CE は Prime Provisioning の存在するワークステーションや他のデバイスに接続されます。
- [Multi-VRF]：マルチ VRF CE（MVRFCE）はカスタマーの所有ですが、プロバイダー空間に存在します。これは、PE からトラフィックをオフロードするために使用されます。
- [Unmanaged Multi-VRF]：管理対象外のマルチ VRF CE は、管理対象外の CE のようにプロビジョニングされます（プロバイダーによってコンフィギュレーションのアップロードやデバイスへのアップロードが行われない）。これはカスタマーの所有であり、プロバイダー空間に存在します。

CPE デバイスの作成

[Create Customer Devices] ウィンドウから、さまざまな CPE デバイスを作成できます。

CPE デバイスを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Devices] を選択します。

[Customer Devices] ウィンドウが表示されます。

ステップ 2　新しい CPE デバイスを作成するには [Create] をクリックします。カスタマー サイトが選択されていない場合だけイネーブルになります。

[Create New CPE Device] ウィンドウが表示されます。

ステップ 3　必要な [Device Name] と [Site Name] に対して、[Select] をクリックします。

それぞれに対して、デバイスとサイトのリストが表示され、各ウィンドウでこのリストからいずれか 1 つを選択して、[Select] をクリックします。この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

（注）　[Customer Name] は、カスタマー サイトが作成されている場合だけ表示されます。

ステップ 4　[Management Type] のドロップダウン ウィンドウで、作成している CPE デバイスの管理タイプを選択できます。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[CPE Device] ウィンドウが再表示されます。

CPE デバイスの編集

[Edit Customer Device] ウィンドウから、特定の CPE デバイスに指定されているフィールドを変更できます。

CPE デバイスを編集するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Devices] を選択します。

[Customer Devices] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、変更する単一のデバイス名を選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのデバイス名が選択されている場合だけイネーブルになります。

[Edit Customer] ウィンドウが表示されます。

ステップ 4　選択した CPE デバイスに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Customer Device] ウィンドウが再表示されます。

CPE デバイスの削除

[Delete] ウィンドウで、選択したカスタマー デバイスをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Customer Devices] を選択します。

[Customer Devices] ウィンドウが表示されます。

ステップ 2　デバイス名の左にあるチェックボックスをオンにして、削除する 1 つ以上のデバイス名を選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のデバイス名が選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたデバイス名を削除することを確認します。指定したデバイス名が削除されて、[Customer Devices] ウィンドウが再表示されます。

リソースの設定

ここでは、リソース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。

アクセス ドメイン

[Access Domains] ウィンドウにアクセスするには、[Inventory] > [Resources] > [Access Domains] を選択します。

[Access Domains] ウィンドウから、アクセス ドメインを作成、編集、または削除できます。

ここでは、次の内容について説明します。

アクセス ドメインの作成

[Create Access Domains] ウィンドウから、さまざまなアクセス ドメインを作成できます。

アクセス ドメインを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Access Domains] を選択します。

[Access Domains] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create New Access Domains] ウィンドウが表示されます。

ステップ 3　アクセス ドメイン名を入力します。これは必須フィールドです。

ステップ 4　プロバイダーを入力するには、次のステップを実行します（これは必須のフィールドです）。

a.　[Provider] フィールドの隣の [Select] ボタンをクリックします。

[Provider Name] ウィンドウのリストが表示されます。

b.　プロバイダー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 5　PE 情報を入力します（必須フィールド）。PE に関するこの情報は、アクセス ドメインのオペレータにとって役に立ちます。256 文字に制限されています。

ステップ 6　予約済みの VLAN 情報を入力します（これは任意です）。

ステップ 7　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Access Domains] ウィンドウが再表示されます。

アクセス ドメインの編集

[Edit Access Domains] ウィンドウから、特定のプロバイダー リージョンに指定されているフィールドを変更できます。

[Edit Access Domains] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Access Domains] を選択します。

[Access Domains] ウィンドウが表示されます。

ステップ 2　アクセス ドメイン名の左にあるチェックボックスをオンにして、変更する単一のアクセス ドメインを選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのアクセス ドメイン名が選択されている場合だけイネーブルになります。

[Edit Access Domains] ウィンドウが表示されます。

ステップ 4　選択したアクセス ドメインに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Access Domains] ウィンドウが再表示されます。

アクセス ドメインの削除

[Delete] ウィンドウで、選択したアクセス ドメインをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Access Domains] を選択します。

[Access Domains] ウィンドウが表示されます。

ステップ 2　アクセス ドメイン名の左にあるチェックボックスをオンにして、削除する 1 つ以上のアクセス ドメインを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のアクセス ドメインが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたアクセス ドメインを削除することを確認します。指定したアクセス ドメインが削除されて、[Access Domains] ウィンドウが再表示されます。

インターフェイス アクセス ドメイン

[Interface Access Domains] ウィンドウにアクセスするには、[Inventory] > [Resources] > [Interface Access Domains] を選択します。

[Access Domains] ウィンドウから、アクセス ドメインを作成、編集、または削除できます。

ここでは、次の内容について説明します。

- 「インターフェイス アクセス ドメインの作成」（P.2-44）
- 「インターフェイス アクセス ドメインの編集」（P.2-45）
- 「インターフェイス アクセス ドメインの削除」（P.2-45）

（注）　インターフェイス アクセス ドメインの作成後に、外部 VLAN ID リソース プールを作成できます。

インターフェイス アクセス ドメインの作成

[Create Interface Access Domains] ウィンドウから、さまざまなインターフェイス アクセス ドメインを作成できます。

インターフェイス アクセス ドメインを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Interface Access Domains] を選択します。

[Interface Access Domains] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create New Interface Access Domains] ウィンドウが表示されます。

ステップ 3　インターフェイス アクセス ドメイン名を入力します。これは必須フィールドです。

ステップ 4　プロバイダーを入力するには、次のステップを実行します（これは必須のフィールドです）。

a. [Provider] フィールドの隣の [Select] ボタンをクリックします。

[Provider Name] ウィンドウのリストが表示されます。

b. プロバイダー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 5　選択したプロバイダーで使用可能なプロバイダー デバイスのリストから、PE デバイス（必須フィールド）を選択します。

ステップ 6　[Interface] ポップアップ ウィンドウから、インターフェイス（必須フィールド）を選択します。[Interface] ポップアップ ウィンドウには、選択した NPE デバイスから、EVC をサポートするすべての使用可能な物理ポートが表示されます。

（注）　要件に基づいて、1 つのインターフェイスまたはグループの複数のインターフェイスを選択できます。

ステップ 7　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Interface Access Domains] ウィンドウが再表示されます。

インターフェイス アクセス ドメインの編集

[Edit Interface Access Domains] ウィンドウから、特定のプロバイダー リージョンに指定されているフィールドを変更できます。

[Edit Interface Access Domains] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Interface Access Domains] を選択します。

[Interface Access Domains] ウィンドウが表示されます。

ステップ 2　インターフェイス アクセス ドメイン名の左にあるチェックボックスをオンにして、変更する単一のインターフェイス アクセス ドメインを選択します。

ステップ 3　[Edit] ボタンをクリックします。このボタンは、1 つのインターフェイス アクセス ドメイン名が選択されている場合だけイネーブルになります。

[Edit Access Domains] ウィンドウが表示されます。

ステップ 4　選択したインターフェイス アクセス ドメインに対して行う変更を入力します。

ステップ 5　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Save] をクリックします。変更が保存され、[Interface Access Domains] ウィンドウが再表示されます。

インターフェイス アクセス ドメインの削除

[Delete] ウィンドウで、選択したアクセス ドメインをデータベースから削除できます。

[Delete] ウィンドウにアクセスするには、次のステップを実行します。

ステップ 1　[Inventory] > [Resources] > [Interface Access Domains] を選択します。

[Interface Access Domains] ウィンドウが表示されます。

ステップ 2　インターフェイス アクセス ドメイン名の左にあるチェックボックスをオンにして、削除する 1 つ以上のアクセス ドメインを選択します。

ステップ 3　[Delete] ボタンをクリックします。このボタンは、1 つ以上のアクセス ドメインが選択されている場合だけイネーブルになります。

[Confirm Delete] ウィンドウが表示されます。

ステップ 4　この情報を保存しない場合は [Cancel] をクリックして、前のウィンドウに進みます。

それ以外の場合は、[Delete] をクリックして、リストされたアクセス ドメインを削除することを確認します。指定したアクセス ドメインが削除されて、[Interface Access Domains] ウィンドウが再表示されます。

リソース プール

Cisco IP Solution Center では、操作中に複数のプールを定義し、使用できます。次のリソース プールを使用できます。

- IP アドレス プール：IP アドレス プールは、リージョンまたは VPN に対して定義および割り当てできます。この機能によって、サービス オペレータは、ネットワーク内のすべての IP アドレスの割り当てを柔軟に管理できます。
- マルチキャスト プール：マルチキャスト プールは、マルチキャスト MPLS VPN 用に使用されます。
- ルート ターゲット（RT）プール：ルート ターゲットは、どのルートを適切な VRF に挿入する必要があるかを PE に通知する MPLS メカニズムです。すべての VPN ルートは、VRF からエクスポートされ、別の VRF に提供されるときに、1 つ以上のルート ターゲットでタグ付けされます。ルート ターゲットは、MPLS VPN アーキテクチャの VPN 識別子と見なすことができます。RT は、64 ビットの数です。
- ルート識別子（RD）プール：CE ルータによって PE ルータに対してアドバタイズされる IP サブネットは、ルート識別子（RD）と呼ばれる 64 ビットのプレフィックスによって増加され、一意になります。次に、結果として得られる 96 ビットのアドレスは、マルチプロトコル BGP（MP-BGP と呼ばれる）の特別なアドレス ファミリを使用して、PE 間で交換されます。RD プールは、ネットワーク内の IP アドレスが一意であることを確認するために Cisco IP Solution Center が使用する 64 ビット RD 値のプールです。
- Site of Origin プール：Site-of-Origin（SoO）属性の値のプール。Site-of-Origin 属性は、サイトが MPLS VPN バックボーンに対してマルチホームになっている場合に、ルーティング ループの発生を防止します。これは、SOO 値に基づいて、ルートの学習元のサイトを識別することによって実現されます。したがって、MPLS VPN ネットワークの PE からはそのサイトに再アドバタイズされません。
- VC ID プール：VC ID プールは、VC ID プールの先頭値およびサイズによって定義されます（VC ID は、回線およびポートを識別する 32 ビットの一意の識別子です）。指定の VC ID プールは、任意のインベントリ オブジェクトに接続されません。イーサネット サービス（EWS、ERS など）の展開の間、VC ID は、VC ID プールから自動で割り当てられます。

- VLAN ID プール：VLAN ID プールは、VLAN プールの先頭値およびサイズによって定義されます。指定の VLAN ID プールは、アクセス ドメインに接続できます。イーサネット サービス（EWS、ERS など）の展開の間、VLAN ID は、アクセス ドメインの VLAN プールから自動割り当てできます。これにより、サービス プロバイダーは、VLAN ID の割り当てを厳密に制御できます。

サービス プロバイダーが使用できる、これらすべてのリソースにより、サービスの展開の自動化が可能になります。

ここでは、さまざまなタイプのリソースのプールを作成し、管理する方法について説明します。この項では、次のトピックについて取り上げます。

IP アドレス プールの作成

Prime Provisioning は、IP アドレス プールを使用して、IP アドレスを PE および CE に自動的に割り当てます。各リージョンには、IP 番号指定アドレス（/30 プール）に使用する IP アドレス プール、および IP アンナンバード アドレス（/32 ループバック アドレス プール）に使用する別の IP アドレス プールがあります。

VPN 内または Extranet 内では、すべての IP アドレスが一意である必要があります。カスタマー IP アドレスは、プロバイダーの IP アドレスとオーバーラップしてはいけません。IP アドレスのオーバーラップは、2 つのデバイスが相互に認識できない場合（つまり、これらが独立した VPN にある場合）にだけ発生する可能性があります。

[Create IP Address Pool] ウィンドウから、IP アドレス プールを作成できます。

IP アドレス プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [IPV4 Address] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New IP Address Resource Pool] ウィンドウが表示されます。

[Create New IP Address Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [IP Address Pool]（必須）：a.b.c.d/mask の形式のテキスト フィールド（たとえば、172.0.0.0/8）。
- [Pool Mask (bits)]（必須）：選択肢には、[30]、[32] などがあります。

  ここで、

  [30] は、IP 番号指定アドレス プール（/30）に使用します。

  [32] は、IP アンナンバード ループバック アドレス プール（/32）に使用します。

- [Pool Association]（必須）：選択肢には、ドロップダウン リストから [Region]、[VPN]、[Customer] などがあります。[Select] ボタンをクリックすると、ドロップダウン リストで行った選択に対する、すべての選択肢を確認できます。新しいウィンドウで選択し、[Select] をクリックします。

（注）　[VPN] を選択すると、追加のオプション フィールド [Pool Name Suffix] が表示されます。このフィールドでは、同じ VPN 内に複数のアドレス プールを作成できます。DMVPN を使用するためにこのアドレス プールを作成している場合、このフィールドを使用して、サフィクスを指定することを推奨します。

- [Pool Name Suffix]（任意）：サフィクスは、プール名を一意にするために使用されます。以前に定義したサフィクスを選択するか、または [New] をクリックして新しいプールを作成することにより、この IP アドレス プールを既存のプールに付加できます。

ステップ 4　作成している IP アドレス プールに関する必要な情報を入力します。

ステップ 5　[Save] をクリックします。

新しい IP アドレス プールがリストされ、[Resource Pools] ウィンドウが再表示されます。

マルチキャスト プールの作成

[Create Multicast Pool] ウィンドウから、マルチキャスト プールを作成できます。これらのプールはグローバルで、プロバイダーやカスタマーと関連付けられていません。

マルチキャスト プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [Multicast] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New Multicast Resource Pool] ウィンドウが表示されます。

[Create New Multicast Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [Multicast Address]（必須）：a.b.c.d/mask の形式のテキスト フィールド（たとえば、239.0.0.0/8）。範囲：224.0.1.0/8 ～ 239.255.255.255/32。
- [Use for default MDT]（任意）：これはチェックボックスです。デフォルト：オンになっています。
- [Use for Data MDT]（任意）：これはチェックボックスです。*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 CE 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。デフォルト：オンになっています。

ステップ 4　作成しているマルチキャスト プールに関する必要な情報を入力します。

ステップ 5　[Save] をクリックします。

新しいマルチキャスト プールがリストされ、[Resource Pools] ウィンドウが再表示されます。

ルート識別子およびルート ターゲット プールの作成

MPLS-based VPN は、ボーダー ゲートウェイ プロトコル（BGP）を使用して、PE 間の通信を行い、カスタマー ルートを簡易化します。これは、IPv4 アドレス以外のアドレスを伝送する、BGP の拡張機能によって可能となります。注目すべき拡張機能として、Route Distinguisher（RD; ルート識別子）があります。

ルート識別子（RD）の目的は、ネットワーク バックボーン間でプレフィックスの値を一意にすることです。プレフィックスは、Route Target（RT; ルート ターゲット）およびルーティング ポリシーの選択に使用されるその他のものとの同じセットに関連付けられている場合、同じ RD を使用する必要があります。関与の対応関係は、Network Layer Reachability Information（NLRI; ネットワーク層到着可能性情報）によって配布されるルート ターゲット（RT）拡張コミュニティ属性に基づいています。RD 値は、その他のプレフィックスとの競合を回避するために、グローバルに一意の値である必要があります。

MPLS ラベルは BGP ルーティング アップデートの一部です。ルーティング アップデートには、アドレッシング情報と到着可能性情報も含まれています。RD が MPLS VPN ネットワーク内で一意である場合は、異なるカスタマーが一意でない IP アドレスを使用していても接続は正常に確立されます。

RD のためには、全体的なロールが同じであるすべての CE において、同じ名前、RD、および RT 値を持つ VRF を使用する必要があります。RD と RT は、BGP を実行する PE 間のルート交換にのみ使用されます。つまり、PE が MPLS VPN の処理を実行するためには、IPv4 ルートについて通常よりフィールド数が多いルーティング情報を交換する必要があります。そうした追加の情報には、RD や RT などが含まれます。

[Create Route Distinguisher Pool] ウィンドウから、ルート識別子プールを作成できます。

ルート識別子プールの作成

ルート識別子プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [Route Distinguisher] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New Route Distinguisher Resource Pool] ウィンドウが表示されます。

[Create New Route Distinguisher Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [RD Pool Start]（必須）：範囲：0 ～ 2147483646。
- [RD Pool Size]（必須）：範囲：1 ～ 2147483647。
- [Provider]（必須）

ステップ 4　作成しているルート識別子プールの [RD Pool Start] および [RD Pool Size] の情報を入力します。

ステップ 5　[Select] ボタンをクリックします。

[Provider for new Resource Pool] ウィンドウが表示されます。

ステップ 6　リストされたプロバイダーのいずれかを選択し、[Select] をクリックします。

ステップ 7　[Save] をクリックします。

新しいルート識別子プールがリストされ、[Resource Pools] ウィンドウが再表示されます。

ルート ターゲット プールの作成

ルート ターゲット プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [Route Target] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New Route Target Resource Pool] ウィンドウが表示されます。

[Create New Route Target Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [RT Pool Start]（必須）：範囲：0 ～ 2147483646。
- [RT Pool Size]（必須）：範囲：1 ～ 2147483647。
- [Provider]（必須）

ステップ 4　作成しているルート ターゲット プールの [RT Pool Start] および [RT Pool Size] の情報を入力します。

ステップ 5　[Select] ボタンをクリックします。

[Provider for new Resource Pool] ウィンドウが表示されます。

ステップ 6　リストされたプロバイダーのいずれかを選択し、[Select] をクリックします。

ステップ 7　[Save] をクリックします。

新しいルート ターゲット プールがリストされ、[Resource Pools] ウィンドウが再表示されます。

Site of Origin プールの作成

MPLS VPN では、CE サイトは、1 つの AS 番号が各 VPN に使用されていて、同じ VPN に属しているすべてのサイトが同じプライベート AS 番号またはパブリック AS 番号を共有している場合、プライベート AS 番号またはパブリック AS 番号を使用します。デフォルトの BGP の動作では、独自の AS 番号が AS パスにすでにある場合、プレフィックスをドロップします。この結果、カスタマー サイトは、この状況ではリモート サイトのプレフィックスを学習しません。PE ルータによってこれらのプレフィックスを送信するには、[AS-OVERRIDE] を設定する必要があります（ハブ サイトが関係する場合、[ALLOWAS-IN] を設定する必要があります）。ただし、ルーティング ループが発生する可能性があります。

たとえば、CE1 および CE2 が同じカスタマー VPN に属していて、同じ AS 番号 65001 を持っている場合です。2 つのカスタマー サイト間の AS パスは、65001 - 1234 - 65001 で、AS 65001 がパスにすでにあるため、カスタマー サイト間でプレフィックスを交換できません。この問題を解決するには、PE ルータで [AS-OVERRIDE] オプションを設定します。ただし、このオプションを設定すると、拡張コミュニティ Site of Origin 属性を使用しないネットワークでルーティング ループが発生します。

Site of Origin は、MPLS VPN バックボーンにマルチホームされているサイト内および同時に [AS-OVERRIDE] を使用しているサイト内でのルーティング ループを防止する MPLS VPN アーキテクチャの概念です。Site of Origin は、プレフィックスのサイトへの再アドバタイズを防止するために、サイトに起因するプレフィックスを識別するために使用する一種の BGP 拡張コミュニティ属性です。

この属性は、PE ルータがルートを学習したサイトを一意に識別します。Site of Origin は、着信ルートマップを使用して、BGP ネイバーとピアリングしている PE においてタグ付けされ、BGP CE-PE ルーティング プロトコルとともに動作します。

Site of Origin は、VPN またはカスタマーごとのカスタマー サイトにつき一意である必要があります（これらのサイトがマルチホームの場合）。したがって、Site of Origin の同じ値を同じ CE ルータまたは同じカスタマー サイトに接続されている PE ルータで使用する必要があります。

（注）　カスタマー サイトが作成されるたびに、Prime Provisioning は、Site of Origin がイネーブルの場合、選択した Site of Origin プロバイダー プールから一意の Site of Origin 値を生成します。この Site of Origin 値は、カスタマーまたは VPN ごとのカスタマー サイトにつき一意である必要があります。

[Create Site of Origin Pool] ウィンドウから、Site of Origin プールを作成できます。

Site of Origin プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [Site of Origin] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New Site of Origin Resource Pool] ウィンドウが表示されます。

[Create New Site of Origin Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [SOO Pool Start]（必須）：範囲：0 ～ 2147483646。
- [SOO Pool Size]（必須）：範囲：1 ～ 2147483647。
- [Provider]（必須）

ステップ 4　作成している Site of Origin プールの [SOO Pool Start] および [SOO Pool Size] の情報を入力します。

ステップ 5　[Select] ボタンをクリックします。

[Provider for new Resource Pool] ウィンドウが表示されます。

ステップ 6　リストされたプロバイダーのいずれかを選択し、[Select] をクリックします。

ステップ 7　[Save] をクリックします。

新しいルート ターゲット プールがリストされ、[Site of Origin pools] ウィンドウが再表示されます。

VC ID プールの作成

[Create VC ID Pool] ウィンドウから、VC ID プールを作成できます。これらのプールはグローバルで、プロバイダーやカスタマーと関連付けられていません。

VC ID プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [VC ID] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New VC ID Resource Pool] ウィンドウが表示されます。

[Create New VC ID Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [VC Pool Start]（必須）：範囲：1 ～ 2147483646。
- [VC Pool Size]（必須）：範囲：1 ～ 2147483647。

ステップ 4　作成している Site of Origin プールの必要な情報を入力します。

ステップ 5　[Save] をクリックします。

新しい VC ID プールがリストされ、[VC ID Pools] ウィンドウが再表示されます。

VLAN プールの作成

[Create VLAN Pool] ウィンドウから、VLAN プールを作成できます。

VLAN プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [VLAN] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New VLAN Resource Pool] ウィンドウが表示されます。

[Create New VLAN Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [VLAN Pool Start]（必須）：範囲：1 ～ 4094。
- [VLAN Pool Size]（必須）：範囲：1 ～ 4094。
- [Access Domain]（必須）

ステップ 4　作成している VLAN プールの [VLAN Pool Start] および [VLAN Pool Size] の情報を入力します。

ステップ 5　[Select] ボタンをクリックします。

[Access Domain for new VLAN Pool] ウィンドウが表示されます。

ステップ 6　リストされたアクセス ドメインのいずれかを選択し、[Select] をクリックします。

ステップ 7　[Save] をクリックします。

新しい VLAN プールがリストされ、[VLAN Pools] ウィンドウが再表示されます。

EVC Outer VLAN プールの作成

[Create EVC OUTER VLAN Pool] ウィンドウから、EVC OUTER VLAN プールを作成できます。

OUTER VLAN プールを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] から [EVC OUTER VLAN] を選択します。

ステップ 3　[Create] ボタンをクリックします。

[Create New OUTER VLAN Resource Pool] ウィンドウが表示されます。

[Create New OUTER VLAN Resource Pool] ウィンドウには、次のフィールドが含まれています。

- [OUTER VLAN Pool Start]（必須）：範囲：1 ～ 4094。
- [OUTER VLAN Pool Size]（必須）：範囲：1 ～ 4094。
- [Interface Access Domain]（必須）

ステップ 4　作成している OUTER VLAN プールの [OUTER VLAN Pool Start] および [OUTER VLAN Pool Size] の情報を入力します。

ステップ 5　[Select] ボタンをクリックします。

[Interface Access Domain for new OUTER VLAN Pool] ウィンドウが表示されます。

ステップ 6　リストされたインターフェイス アクセス ドメインのいずれかを選択し、[Select] をクリックします。

ステップ 7　[Save] をクリックします。

新しい OUTER VLAN プールがリストされ、[OUTER VLAN Pools] ウィンドウが再表示されます。

リソース プールの削除

[Resource Pool] ウィンドウから、特定のリソース プールを削除できます。

リソース プールを削除するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Resource Pools] ウィンドウの左上にある [Pool Type] からプール タイプを選択します。

ステップ 3　リソース プールの左にあるチェックボックスをオンにして、削除する 1 つ以上のリソース プールを選択します。

ステップ 4　[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 5　新しい [Delete] ボタンをクリックして、リストされたリソース プールを削除することを確認します。

指定したプールが削除されて、[Resource Pools] ウィンドウが再表示されます。

ルート ターゲット

VPN は、*ルート ターゲット*と呼ばれるサブセットに編成できます。ルート ターゲットは、VPN 内の CE が相互に通信する方法を示します。つまり、ルート ターゲットは VPN の論理トポロジを表します。Prime Provisioning を使用して、ハブ アンド スポークまたはフル メッシュの CE ルーティング コミュニティを作成することにより、CE 間にさまざまな VPN トポロジを形成できます。ルート ターゲットは、複雑な VPN トポロジや CE 接続の作成を可能にする構築ブロックです。

最も一般的なタイプの VPN は、*ハブ アンド スポーク*および*フル メッシュ*です。

- ハブアンドスポーク形式のルート ターゲットでは、1 つまたは数台の CE がハブとして動作し、スポーク CE は、ハブとの間で、またはハブを介して通信し、相互に直接通信することはありません。
- フル メッシュ形式のルート ターゲットでは、各 CE が他のすべての CE と接続されます。

これらの基本的な 2 種類の VPN（フル メッシュとハブアンドスポーク）は、1 つのルート ターゲットで表すことができます。VPN を作成すると、Prime Provisioning ソフトウェアにより、1 つのデフォルト ルート ターゲットが作成されます。したがって、高度なカスタマー レイアウト方法が必要となるまでは、新しいルート ターゲットを定義する必要はありません。それまでは、ルート ターゲットが VPN それ自体を表していると考えることができます。つまり、ルート ターゲットと VPN は同一のものです。何らかの理由で、ソフトウェアが選択したルート ターゲットの値を上書きする必要がある場合、これを実行できるのは、Prime Provisioning ソフトウェアでルート ターゲットを作成するときだけです。

きわめて複雑なトポロジを作成するには、CE 間の必要な接続をいくつかのグループに分割する必要があります。このとき、各グループをフル メッシュとハブアンドスポークのいずれかのパターンとします （CE は、各グループに 2 つの基本的なパターンのいずれかがある場合、同時に複数のグループに属することができます）。VPN 内の各サブグループには、独自のルート ターゲットが必要です。1 つのグループだけに属している CE は、対応するルート ターゲットに参加します（必要な場合はスポークとして）。CE が複数のグループに属している場合は、プロビジョニングの実行時に [Advanced Setup] を選択することにより、その CE を 1 回のサービス要求で該当するすべてのグループに追加できます。この情報に基づいてプロビジョニング ソフトウェアが以降の処理を実行し、ルート ターゲット値と VRF テーブルを割り当てることにより、カスタマーの要求に合致した接続を提供します。トポロジ ツールを使用することで、ルート ターゲットのメンバーシップと作成される VPN 接続を二重チェックできます。

Prime Provisioning では、1 つのサイトに複数の CE が存在でき、同じ PE に複数のサイトを接続できます。各ルート ターゲットには、一意のルート ターゲット（RT）、ルート識別子（RD）、および VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス命名があります。ルート ターゲットをプロビジョニングした後で、監査レポートを実行することにより、ルート ターゲットの配置を検証し、サービス要求によって作成されたトポロジを表示することを推奨します。この製品は、同じ VPN 内での 2 つ以上の CE ルーティング コミュニティのリンクをサポートしています。

ここでは、CE ルーティング コミュニティの作成および管理の方法について説明します。この項では、次のトピックについて取り上げます。

- 「ルート ターゲットの作成」（P.2-54）
- 「ルート ターゲットの削除」（P.2-55）

ルート ターゲットの作成

VPN を作成するときは、Prime Provisioning ソフトウェアによって、1 つのデフォルトのルート ターゲットが作成されます。ただし、ネットワーク トポロジおよびコンフィギュレーションでカスタマイズされたルート ターゲットの定義が必要な場合、ご使用のネットワーク用にカスタマイズされたルート ターゲットを定義できます。

ヒント　カスタマイズされたルート ターゲットは、必ず VPN ネットワーク管理者と相談して定義する必要があります。複雑なトポロジを作成するには、CE 間の必要な接続をグループに分割する必要があります。ここで、各グループは、フル メッシュにされるか、またはハブ アンド スポーク パターンを持ちます。CE は、各グループに 2 つの基本的なコンフィギュレーション パターンのいずれかがある場合、同時に複数のグループに属することができます。

VPN 内の各サブグループには、独自のルート ターゲットが必要です。1 つのグループだけに属している CE は、対応するルート ターゲットに参加します（必要な場合はスポークとして）。CE が複数のグループに属している場合は、プロビジョニングの実行時に [Advanced Setup] を選択することにより、その CE を 1 回のサービス要求で該当するすべてのグループに追加できます。この情報から、Cisco IP Solution Center は、残りの作業を行い、ルート ターゲット値および VRF テーブルを割り当て、カスタマーが要求する接続を正確に行います。

CE ルーティング コミュニティを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Route Targets] を選択します。

[Route Targets] 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 CE Routing Community] ウィンドウが表示されます。

ステップ 3　CE ルーティング コミュニティの要求に応じて [Route Target] フィールドに入力します。

a. [Provider Name]（必須）：このルート ターゲットに関連付けられたサービス プロバイダーを指定するには、[Select] をクリックします。

[Select Provider] ウィンドウが表示されます。

b. 新しいウィンドウから、サービス プロバイダーの名前を選択し、[Select] をクリックします。

c. [Name]（必須）：ルート ターゲットの名前を入力します。

d. [Route Target Type] : ルート ターゲットのタイプ（ハブ アンド スポークまたはフル メッシュ）を指定します。

e. [Auto-Pick Route Target Values] : Cisco IP Solution Center にルート ターゲット（RT）の値を自動的に設定させるか、または手動で RT の値を設定するかを選択します。

デフォルトでは、[Auto-pick route target values] チェックボックスはオンになっています。このチェックボックスをオフにすると、ルート ターゲットの値を手動で入力できます。

注意　[Auto-pick route target values] オプションをバイパスし、ルート ターゲット（RT）の値を手動で設定することを選択する場合、RT の値が Prime Provisioning ソフトウェアで定義された後に、この値を編集できなくなることに注意してください。

ステップ 4　[Create CE Routing Community] ウィンドウへの情報の入力が完了したら、[Save] をクリックします。

ルート ターゲットを作成した後、ルート ターゲットを VPN に追加できます。

ルート ターゲットの削除

[CE Routing Community] ウィンドウから、特定のルート ターゲットを削除できます。

ルート ターゲットを削除するには、次のステップを実行します。

ステップ 1　[Service Design] > [Resources] > [Route Targets] を選択します。

[Route Targets] ウィンドウが表示されます。

ステップ 2　ルート ターゲット名の左にあるチェックボックスをオンにして、削除するルート ターゲットを選択します。

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　[OK] をクリックして、リストされたルート ターゲットを削除することを確認します。

指定したルート ターゲットが削除されて、[Route Targets] ウィンドウが再表示されます。

論理的インベントリの設定

VPN

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。Cisco IP Solution Center : MPLS VPN Management 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 から出ることはできません（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ありません。

ここでは、さまざまなタイプのリソースのプールを作成し、管理する方法について説明します。この項では、次のトピックについて取り上げます。

- 「VPN の作成」（P.2-56）
- 「VPN の削除」（P.2-58）

VPN の作成

VPN を作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Logical Inventory] > [VPN] 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] をクリックします。

[Create New VPN] ウィンドウが表示されます。

ステップ 3　必要に応じて、VPN に対するフィールドに入力します。

a. [Name]（必須）: VPN 名（選択した任意の名前）を入力します。

b. [Customer]（必須）: この VPN に関連付けられたカスタマーを選択するには、[Select] を選択します。

c. カスタマーのリストから、適切なカスタマーを選択し、[Select] をクリックします。

d. MPLS 属性が必要な場合は、ウィンドウの [MPLS Attributes] セクションのフィールドに入力します。VPLS では、ステップ w. **に進みます。**

e. [Create Default Route Targets]（任意）: デフォルト ルート ターゲットを作成するには、[Create Default Route Targets）] チェックボックスをオンにし、プロバイダーを選択します。

f. [Enable Unique Route Distinguisher] : MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング機能は、IPv4 VRF アドレス ファミリ コンフィギュレーション モードだけでイネーブルにされます。この機能がイネーブルにされると、VRF にインポートされた eBGP パスまたは iBGP パスあるいはその両方でロード バランシングを実行できます。

g. [Enable IPv4 Multicast] : マルチキャスト IPv4 VPN ルーティングをイネーブルにするには、[Enable IPv4 Multicast] チェックボックスをオンにします。

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。

h. [Enable IPv6 Multicast] : マルチキャスト IPv6 VPN ルーティングをイネーブルにするには、[Enable IPv6 Multicast] チェックボックスをオンにします。

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。

i. [Enable Auto Pick MDT Addresses]（任意）: マルチキャスト リソース プールから [Default MDT Address] および [Default MDT Subnet] 値を使用するには、このチェックボックスをオンにします。

j. [Default MDT Address] : [Enable Auto Pick MDT Addresses] をオンにした場合は、[Default MDT Address] が必要です。

k. [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。

l. [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 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カスタマー サイトからのマルチキャスト トラフィックを伝送します。

m. [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。

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 CE 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。

n. [Default PIM Mode]（任意）: デフォルトの Protocol Independent Multicast（PIM）モードの場合は、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。

o. [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。

p. [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（**ip pim vpn** <*vpnName*> **ssm default**）を作成します。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 vpn** <*vpnName*> **ssm range {ACL#!named-ACL-name}**）が作成されます。

q. [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。

r. [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。

s. [Configure Static-RP]（任意）：スタティック RP を設定するには、関連付けられたチェックボックスをオンにします。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。

t. [PIM Static-RPs] : PIM スタティック RP を編集または追加するには、[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。次に [OK] をクリックします。

u. [Route Targets]（任意）: [Enable Multicast] がオンに設定されている場合、**ルート ターゲット**が必要です。デフォルト ルート ターゲットをイネーブルにしないことを選択した場合、Prime Provisioning で作成済みのカスタマイズされたルート ターゲットを選択できます。[Route Targets] ペインから、[Select] をクリックします。

[Select Route Targets] ウィンドウが表示されます。

v. このサービス ポリシーで使用するルート ターゲットのチェックボックスをオンにし、[Select] をクリックします。

[Create VPN] ウィンドウに戻り、新しいルート ターゲットの選択がハブ ルート ターゲット（HRT）およびスポーク ルート ターゲット（SRT）の値とともに表示されます。

w. VPLS の属性が必要な場合、そのオプション フィールドは、x. ～ aa. にあります。

x. [Enable VPLS]（任意）：この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。

y. [VPLS VPN ID]（任意）：1 ～ 2147483646 の範囲の整数を入力します。

z. [Service Type]（任意）：ドロップダウン リストをクリックして、[ERS]（イーサネット リレー サービス）または [EWS]（イーサネット ワイヤ サービス）から選択します。

aa. [Topology]（任意）：ドロップダウン リストから次のいずれかの VPLS トポロジを選択します。[Full Mesh]（各 CE は、その他すべての CE に直接接続されます）または [Hub and Spoke]（ハブ CE だけが各スポーク CE に接続され、スポーク CE は相互に直接接続されません）。

ステップ 4　この VPN の設定が終了したら、[Save] をクリックします。

[VPNs] ウィンドウの左下隅の [Status] 表示で示されるように、VPN が正常に作成されました。

VPN の削除

[VPNs] ウィンドウから、特定の VPN を削除できます。

（注）　MPLS サービス要求に関連付けられていない VPN だけを削除できます。

VPN を削除するには、次のステップを実行します。

ステップ 1　[Inventory] > [Logical Inventory] > [VPN] 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 名の左側にあるチェックボックスをオンにして、削除する VPN 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　[OK] をクリックして、リストされた VPN を削除することを確認します。
指定した VPN が削除されて、[VPNs] ウィンドウが再表示されます。

CHAPTER 3

L2VPN とキャリア イーサネット サービスの管理

この章では、Prime Provisioning ポリシーとサービス要求を使用して、さまざまな L2VPN およびキャリア イーサネット サービスを管理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。

L2VPN サービスの概要

この章では、Cisco Prime Provisioning 6.3 で L2VPN コンポーネントの使用を開始する際に役立つロード マップを提供します。次の事項について説明します。

概要

L2VPN コンポーネントを使用してレイヤ 2 サービスをプロビジョニングするには、この項で概説しているインストールおよび設定手順を完了しておく必要があります。さらに、Prime Provisioning および L2VPN サービスの基本概念について理解しておく必要があります。次のサブセクションでは、Prime Provisioning を使用して L2VPN、VPLS、および EVC サービスをプロビジョニングできるようにするために実行すべき主要なタスクについて概説します。この項の情報は、チェックリストとして使用できます。必要に応じて、このマニュアルの他の項や Prime Provisioning マニュアル セットの他のマニュアルへの参照情報が示されています。詳細については、参照先のマニュアルをご覧ください。Prime Provisioning および L2VPN コンポーネントに対する基本的なインストールおよび設定手順が完了したら、後続の項を参照して、L2VPN、VPLS、および EVC サービスを作成およびプロビジョニングします。

Prime Network でエンドポイントを選択してサービスにデータを取り込む

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。

ステップ 1　いずれかのマップで、CTRL をクリックし、1 つ以上のエンドポイント デバイスを選択します。

ステップ 2　右クリック メニューで [Fulfill/Create Service] を選択します。

ステップ 3　Prime Provisioning でサービスを作成した場合と同じ初期画面が表示されます。

ステップ 4　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。

ステップ 5　ポリシーを選択すると、サービス要求のメイン ページはリンクと選択したデバイスが事前に読み込まれて、通常どおりに表示されます。

Prime Provisioning のインストールおよびネットワークの設定

Prime Provisioning で L2VPN モジュールを使用して L2VPN または VPLS サービスをプロビジョニングするには、まず Prime Provisioning をインストールして、Prime Provisioning のサポートに必要となる基本ネットワーク設定を実行する必要があります。これらの手順の詳細については、第 2 章「Prime Provisioning を設定する前に」を参照してください。Prime Provisioning のインストールと、全般的なネットワーク設定要件については、該当する章を参照してください。

（注）　Prime Provisioning 内の L2VPN コンポーネントを使用するには、L2VPN ライセンスを購入してアクティブ化する必要があります。

レイヤ 2 サービスをサポートするためのネットワークの設定

Prime Provisioning に必要な基本ネットワーク設定の他に、レイヤ 2 サービスをサポートするために次のネットワーク設定手順を実行する必要があります。次の手順の詳細は、Prime Provisioning のマニュアルでは説明されていません。これらのステップの実行方法については、ご使用のデバイスのマニュアルを参照してください。

1. プロバイダー コアに接続されている N-PE デバイスのコアに面しているインターフェイス上の MPLS をイネーブルにします。
2. N-PE デバイス上の /32 ループバック アドレスを設定します。これらのループバック アドレスは LDP 接続で終端する必要があります。
3. すべてのレイヤ 2 デバイス（スイッチ）を VTP トランスペアレント モードに設定します。これにより、必ずどのスイッチも VLAN サーバとして動作することはなく、VLAN 情報がネットワーク経由で自動的に伝搬しなくなります。

基本 Prime Provisioning サービスの設定

Prime Provisioning サービスおよび L2 サービスをサポートするための基本ネットワーク設定タスクが完了したら、Prime Provisioning を使用して、プロバイダーとリージョン、カスタマーとサイト、デバイス、VLAN プールと VC プール、NPC、および L2 サービスをプロビジョニングするために必要な他のリソースなどの、Prime Provisioning リポジトリ内の要素を定義します。一般的な Prime Provisioning のタスクを実行するための詳細な手順については、第 2 章「Prime Provisioning を設定する前に」を参照してください。一部の重要な Prime Provisioning セットアップ タスクの概要については、「Prime Provisioning サービスの設定」（P.3-6）を参照してください。次の情報は、L2 サービスをプロビジョニングする前に設定する必要がある基本的な Prime Provisioning サービスのチェックリストです。

プロバイダー、カスタマー、およびデバイスの設定

次のステップを実行して、Prime Provisioning リポジトリ内のプロバイダー、カスタマー、およびデバイスを設定します。これらの要素は、すべての Prime Provisioning サービスで使用できるグローバル リソースです。

1. **サービス プロバイダーおよびリージョンを設定します。**単一のプロバイダーに複数のネットワークがあることがあるため、リージョンは重要です。そのような環境に対応するために、リージョンはさらなる細分化のレベルとして使用されます。プロバイダーおよびリージョンを作成するには、「リソースの設定」（P.2-42）を参照してください。「サービス プロバイダーとそのリージョンの定義」（P.3-9）も参照してください。
2. **カスタマーおよびカスタマー サイトを設定します。**カスタマーは、ISP からの VPN サービスのリクエスタです。各カスタマーは、多数のカスタマー サイトを所有できます。各カスタマー サイトは唯一のカスタマーだけに所属して、多数の CE を所有できます。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、「リソースの設定」（P.2-42）を参照してください。「カスタマーとそのサイトの定義」（P.3-9）も参照してください。
3. **未処理のデバイスをインポートまたは追加します。**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、自動検出、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。また、「L2 サービスに対する自動検出の使用」（P.3-177）も参照してください。

4. **デバイスに PE または CE としてロールを割り当てます。**Prime Provisioning にデバイスが作成されたら、デバイスをカスタマー（CE）デバイスまたはプロバイダー（PE）デバイスとして定義する必要があります。個々のデバイスのデバイス属性を編集することで、または Prime Provisioning インベントリ マネージャでのバッチ編集で実行できます。デバイス属性を設定するには、「デバイスおよびデバイス グループを設定する方法」（P.2-1）を参照してください。

N-PE ループバック アドレスの設定

Prime Provisioning 内では、N-PE デバイス上でループバック アドレスを設定する必要があります。この手順の詳細については、「N-PE ループバック アドレスの設定」（P.3-4）を参照してください。

L2VPN および VPLS サービスの Prime Provisioning リソースの設定

アクセス ドメイン、VLAN プール、VC プールなどの一部の Prime Provisioning リソースは、Prime Provisioning L2VPN および VPLS サービスだけをサポートするように設定されます。これらのリソースを設定するには、次のステップを実行します。

1. **アクセス ドメインを作成します。**L2VPN および VPLS では、イーサネット ベースのサービスをプロビジョニングして、Prime Provisioning が VLAN プールからのリンクに VLAN を自動的に割り当てるようにする場合、アクセス ドメインを作成します。レイヤ 2 アクセス ドメインごとに、Prime Provisioning 内の対応するアクセス ドメインオブジェクトが必要です。作成中に、このドメインに関連付けられているすべての N-PE デバイスを選択します。後で、1 つのアクセス ドメインに 1 つの VLAN プールを作成できます。アクセス ドメインを作成する手順の詳細については、「リソースの設定」（P.2-42）を参照してください。「アクセス ドメインの作成」（P.3-10）も参照してください。
2. **VLAN プールを作成します。**VLAN プールは、各アクセス ドメインに対して作成されます。L2VPN および VPLS では、Prime Provisioning が VLAN をリンクに割り当てられるように VLAN プールを作成します。VLAN ID プールは、開始する値およびサイズで定義されます。VLAN プールを作成する手順の詳細については、「リソースの設定」（P.2-42）を参照してください。「VLAN プールの作成」（P.3-10）も参照してください。
3. **VC プールを作成します。**VC ID プールは、VC ID プールの開始する値およびサイズで定義します。指定された VC ID プールは、どのインベントリ オブジェクト（プロバイダーまたはカスタマー）にも接続されません。ネットワークごとに VC ID プールを 1 つ作成します。VC プールを作成する手順の詳細については、「リソースの設定」（P.2-42）を参照してください。「VC ID プールの作成」（P.3-12）も参照してください。

NPC の設定

L2VPN サービス要求または VPLS サービス要求を作成するには、CE と PE の間、または U-PE と N-PE との間の物理リンクを事前に定義する必要があります。Named Physical Circuit（NPC; 名前付き物理回線）は、物理ポートのグループを通過するリンクを表します。したがって、同じ NPC 上で複数の論理リンクをプロビジョニングできます。このため、NPC は一度定義されますが、複数の L2VPN サービス要求または VPLS サービス要求によって使用されます。NPC を作成する手順の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。「名前付き物理回線の作成」（P.3-13）も参照してください。

VPN の設定

L2VPN サービスまたは VPLS サービスをプロビジョニングする前に、VPN を定義する必要があります。L2VPN では、1 つの VPN をさまざまなサービス タイプで共有できます。VPLS では、VPLS インスタンスごとに 1 つの VPN が必要です。VPN を定義するには、「論理的インベントリの設定」（P.2-56）を参照してください。「VPN の定義」（P.3-10）も参照してください。

EVC ポリシー、L2VPN ポリシー、VPLS ポリシー、およびサービス要求の操作

Prime Provisioning にプロバイダー、カスタマー、デバイス、およびリソースを設定したら、EVC ポリシー、L2VPN ポリシーまたは VPLS ポリシー、プロビジョンのサービス要求（SR）の作成、およびサービスの展開を開始できます。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、次のステップを実行します。

1. **L2 サービスの概念に関する概要を確認します。**『*Cisco Prime Provisioning 6.3 Administration Guide*』の章「Prime Provisioning Layer 2 VPN Concepts」を参照してください。
2. **EVC ポリシー、L2VPN ポリシー、または VPLS ポリシーを設定します。**作成するポリシーのタイプに応じて、該当する項を参照してください。
   - 「EVC イーサネット ポリシーの作成」（P.3-20）
   - 「EVC ATM-Ethernet インターワーキング ポリシーの作成」（P.3-58）
   - 「L2VPN ポリシーの作成」（P.3-95）
   - 「VPLS ポリシーの作成」（P.3-138）
3. **EVC サービス要求、L2VPN サービス要求、または VPLS 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。
   - 「EVC イーサネット サービス要求の管理」（P.3-36）
   - 「EVC ATM-Ethernet インターワーキング サービス要求の管理」（P.3-74）
   - 「L2VPN サービス要求の管理」（P.3-126）
   - 「VPLS サービス要求の管理」（P.3-168）
4. **サービス要求を展開します。**「サービス要求の展開、モニタリング、および監査」（P.3-176）を参照してください。
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。「サービス要求の展開、モニタリング、および監査」（P.3-176）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）を参照してください。
   - L2 レポートおよび VPLS レポートを実行します。「L2 および VPLS のレポートの生成」（P.10-34）を参照してください。

用語の表記法についての注意事項

Prime Provisioning GUI およびユーザ ガイドのこの章では、イーサネット サービス特有の命名表記法を使用しています。これらの表記法は、初期の MEF 表記法と密接に整合されています。今後のリリースでは、現在の MEF 表記法に適合するように更新される予定です。MEF フォーラムによって使用される同等の用語の概要については、表 3-1 に参照用として記載されています。

用語の表記法、および基本的なネットワーク テクノロジーとの整合方法の詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』*の「Prime Provisioning Layer 2 VPN Concepts」の章を参照してください。

表 3-1　　イーサネット サービス用語の対応

GUI およびこのユーザ ガイドで使用される用語	現在の MEF での同義語
L2VPN over MPLS Core	
イーサネット ワイヤ サービス（EWS）	Ethernet Private Line（EPL; イーサネット専用回線）
イーサネット リレー サービス（ERS）	Ethernet Virtual Private Line（EVPL; イーサネット仮想専用回線）
ATM over MPLS（ATMoMPLS）	—
Frame Relay over MPLS（FRoMPLS）	—
VPLS over MPLS Core	
イーサネット ワイヤ サービス（EWS）またはイーサネット マルチポイント サービス（EMS）	Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）
イーサネット リレー サービス（ERS）またはイーサネット リレー マルチポイント サービス（ERMS）	Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）
VPLS over Ethernet Core	
イーサネット ワイヤ サービス（EWS）	Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）
イーサネット リレー サービス（ERS）	Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）

Prime Provisioning サービスの設定

L2VPN、VPLS、および EVC ポリシーとサービス要求を作成するには、ターゲット デバイス、VPN、およびネットワーク リンクなどのサービス関連要素を最初に定義する必要があります。通常、これらの要素は 1 回作成します。

この項では、L2VPN サービス用の Cisco Prime Provisioning 6.3 リソースを設定するための基本的な手順について説明します。次の事項について説明します。

- 「ターゲット デバイスの作成およびロール（N-PE または U-PE）の割り当て」（P.3-7）
- 「Prime Provisioning をサポートするためのデバイス設定」（P.3-7）
- 「サービス プロバイダーとそのリージョンの定義」（P.3-9）
- 「カスタマーとそのサイトの定義」（P.3-9）
- 「VPN の定義」（P.3-10）
- 「アクセス ドメインの作成」（P.3-10）

- 「VLAN プールの作成」（P.3-10）
- 「外部 VLAN プールの作成」（P.3-12）
- 「VC ID プールの作成」（P.3-12）
- 「名前付き物理回線の作成」（P.3-13）
- 「疑似回線クラスの作成および変更」（P.3-16）
- 「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）

（注）　この項は、L2VPN に関連する Prime Provisioning サービスに関する概要を示しています。これらとその他の基本 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」を参照してください。

ターゲット デバイスの作成およびロール（N-PE または U-PE）の割り当て

Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義する必要があります。要素は、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、N-PE、U-PE、または P として機能する Cisco IOS ルータです。デバイスを作成する手順の詳細については、「デバイスおよびデバイス グループを設定する方法」（P.2-1）を参照してください。

Prime Provisioning をサポートするためのデバイス設定

ネットワークでの Prime Provisioning の使用をサポートするには、2 つのデバイスを設定する必要があります。

- ネットワーク内のスイッチは、VTP トランスペアレント モードで操作する必要があります。
- N-PE デバイスでループバック アドレスを設定する必要があります。

（注）　これらは、Prime Provisioning がネットワークで正しく機能するために必要な 2 つの最小のデバイス設定です。ネットワークでデバイスが正しく機能するには、その他のデバイス設定手順を実行する必要があります。

VTP トランスペアレント モードでのスイッチの設定

セキュリティの理由から、Prime Provisioning では、L2VPN サービス要求をプロビジョニングする前に、ERS または EWS サービスで使用するすべてのスイッチで VTP をトランスペアレント モードで設定する必要があります。VTP モードを設定するには、次の Cisco IOS コマンドを入力します。

```
Switch# configure terminal
Switch(config)# vtp mode transparent
```

次の Cisco IOS コマンドを入力して、VTP モードがトランスペアレント モードに変更されたことを確認します。

```
Switch# Show vtp status
```

N-PE デバイスでのループバック アドレスの設定

Any Transport over MPLS（AToMPLS）接続では、N-PE のループバック アドレスを正しく設定する必要があります。ループバック インターフェイスで指定する IP アドレスは、リモート ペア PE から到達可能でなければなりません。PE ペアの 2 つのループバック インターフェイス間でラベル配布プロトコル（LDP）トンネルを確立する必要があります。PE ループバック アドレスを設定するには、次のステップを実行します。

ステップ 1　[Inventory] > [Provider Devices] を選択します。

[Provider Devices] ウィンドウが表示されます。

ステップ 2　特定の PE デバイスを選択して、[Edit] ボタンをクリックします。

[Edit Provider Device] ウィンドウが表示されます。

システムに誤ったループバック アドレスが入力されるのを防止するために、GUI の [Loopback IP Address] フィールドは読み取り専用です。

ステップ 3　（[Loopback IP Address] 属性の）[Select] ボタンをクリックして、ループバック アドレスを選択します。

[Select Device Interface] ウィンドウが表示されます。

ステップ 4　[Interface Name] 列にリストされるループバック アドレスの 1 つを選択します。

これを行うことで、デバイスで定義されている有効なループバック アドレスのみが必ず選択されるようになります。

ステップ 5　検索をさらに絞り込むには、[LDPTermination Only] チェックボックスをオンにして、[Select] ボタンをクリックします。

これによって、リストは LDP 終端ループバック インターフェイスに制限されます。

IOS XR サポートのためのデバイスの設定

Cisco Prime Provisioning 6.3 の L2VPN は、Cisco IOS XR ソフトウェアを実行しているデバイスをサポートします。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。L2VPN では、IOS XR は、Network Provider Edge（N-PE; ネットワーク プロバイダー エッジ）デバイスとして機能する Cisco XR12000 と CRS-1 シリーズ ルータだけでサポートされます。

L2VPN では、次の E-Line サービスが IOS XR でサポートされます。

- CE を備えているか、備えていないポイントツーポイント ERS。
- CE を備えているか、備えていないポイントツーポイント EWS。

次の L2VPN 機能は、IOS XR ではサポートされません。

- IOS XR を実行している N-PE での標準の UNI ポート （[Link Attributes] ウィンドウの属性 [Standard UNI Port] は、IOS XR が実行されている N-PE デバイス上に UNI がある場合はディセーブルにされます）。
- IOS XR が実行されている N-PE 上の SVI インターフェイス（[Link Attributes] ウィンドウの属性 [N-PE Pseudo-wire On SVI] は、IOS XR デバイスではディセーブルにされます）。
- 疑似回線トンネルの選択（[Link Attributes] ウィンドウの属性 [PW Tunnel Selection] は、IOS XR デバイスではディセーブルにされます）。

- IOS XR を実行している N-PE での EWS UNI（dot1q トンネルまたは Q-in-Q）。
- フレーム リレー /ATM と VPLS サービス。

L2VPN で IOS XR サポートをイネーブルにするには、次のステップを実行します。

ステップ 1　DCPL プロパティ Provisioning\Service\l2vpn\platform\CISCO_ROUTER\IosXRConfigType を [XML] に設定します。

可能な値は、[CLI]、[CLI_XML]、および [XML]（デフォルト）です。

ステップ 2　次のようにして、Prime Provisioning でデバイスを IOS XR デバイスとして作成します。

a. [Inventory] > [Devices] > [Create Cisco Devcie] を選択して、シスコ デバイスを作成します。

b. ドロップダウン リストから [Cisco Device] を選択します。

[Create Cisco Router] ウィンドウが表示されます。

c. [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 3　このマニュアルの手順に従って、L2VPN 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.3-186）で提供されています。

サービス プロバイダーとそのリージョンの定義

L2VPN をプロビジョニングする前に、サービス プロバイダー管理ドメインを定義する必要があります。プロバイダー管理ドメインは、1 つの BGP 自律システム（AS）番号が指定された ISP の管理ドメインです。プロバイダー管理ドメインによって所有されるネットワークは、バックボーン ネットワークと呼ばれます。ISP に 2 つの AS 番号がある場合は、2 つのプロバイダー管理ドメインとして定義する必要があります。各プロバイダー管理ドメインは、多数のリージョン オブジェクトを所有できます。

プロバイダー管理ドメインを定義する手順の詳細については、「リソースの設定」（P.2-42）を参照してください。

カスタマーとそのサイトの定義

L2VPN をプロビジョニングする前に、カスタマーとそのサイトを定義する必要があります。カスタマーは、ISP からの VPN サービスのリクエスタです。各カスタマーは、多数のカスタマー サイトを所有できます。各カスタマー サイトは 1 つのカスタマーに属しており、1 つのカスタマーだけが多数の CPE を所有できます。カスタマーを作成するための詳細な手順については、「リソースの設定」（P.2-42）を参照してください。

VPN の定義

L2VPN または VPLS をプロビジョニングする前に、VPN を定義する必要があります。L2VPN では、1 つの VPN をさまざまなサービス タイプで共有できます。VPLS では、VPLS インスタンスごとに 1 つの VPN が必要です。VPN を作成するための詳細な手順については、「論理的インベントリの設定」（P.2-56）を参照してください。

（注）　L2VPN 内の VPN は、すべての L2VPN リンクをグループ化するために使用される唯一の名前です。これは、MPLS VPN 向けであるため、本質的な意味を持ちません。

アクセス ドメインの作成

L2VPN および VPLS では、イーサネット ベースのサービスをプロビジョニングして、Prime Provisioning が VLAN プールからのリンクに VLAN を自動的に割り当てるようにする場合、アクセス ドメインを作成します。

レイヤ 2 アクセス ドメインごとに、Prime Provisioning 内の対応するアクセス ドメインオブジェクトが必要です。作成中に、このドメインに関連付けられているすべての N-PE デバイスを選択します。後で、1 つのアクセス ドメインに 1 つの VLAN プールを作成できます。この方法で、N-PE に VLAN が自動的に割り当てられます。

始める前に、次の点を確認してください。

- 作成するアクセス ドメインの名前を把握している。
- 新しいアクセス ドメインに関連付けるサービス プロバイダーを作成してある。
- プロバイダーと PE デバイスに関連付けられたプロバイダー リージョンを作成してある。
- 新しいアクセス ドメインに関連付ける PE デバイスを作成してある。
- 新しいアクセス ドメインに関連付ける各 VLAN の開始値とサイズを把握している。
- 管理 VLAN として機能する VLAN を把握している。

アクセス ドメインの詳細な作成手順については、「リソースの設定」（P.2-42）を参照してください。

VLAN プールの作成

L2VPN および VPLS では、Prime Provisioning が VLAN をリンクに割り当てられるように VLAN プールを作成します。VLAN ID プールは、VLAN プールの開始値とサイズを使用して定義されます。VLAN プールは、アクセス ドメインに接続できます。イーサネット サービスの展開中に、アクセス ドメインの既存の VLAN プールから VLAN ID を自動的に割り当てすることができます。新規サービスの展開時に、Prime Provisioning は、VLAN プールのステータスを [Available] から [Allocated] に変更します。自動割り当てによって、サービス プロバイダーは VLAN ID の割り当てを厳密に制御できます。

VLAN ID を手動で割り当てることもできます。

（注）　Prime Provisioning サービスで手動による VLAN ID を設定する場合に、VLAN ID が定義済みの VLAN プールの有効な範囲外にあると、Prime Provisioning が警告を出します。その場合は、Prime Provisioning は、手動で定義された VLAN ID を VLAN プールに含めません。手動で割り当てる VLAN ID の範囲を含めるよう、VLAN プールの範囲をプリセットすることを推奨します。

アクセス ドメインごとに VLAN プールを 1 つ作成します。VLAN プール内で、複数の範囲を定義できます。

始める前に、次の点を確認してください。

- 各 VLAN プールの開始番号がわかっている。
- 各 VLAN プールのサイズがわかっている。
- VLAN プールのアクセス ドメインを作成してある。
- 各 VLAN プールを割り当てるアクセス ドメインの名前がわかっている。

Prime Provisioning に自動的に VLAN をリンクに割り当てさせるには、次のステップを実行します。

ステップ 1　[Service Design] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Pool Type] ドロップダウン リストから [VLAN] を選択します。

ステップ 3　[Create] をクリックします。

[Create New VLAN Resource Pool] ウィンドウが表示されます。

ステップ 4　[VLAN Pool Start number] を入力します。

ステップ 5　[VLAN Pool Size number] を入力します。

ステップ 6　[Access Domain] フィールドに正しいアクセス ドメインが表示されない場合は、[Access Domain] フィールドの右側にある [Select] をクリックします。

[Select Access Domain] ダイアログボックスが表示されます。

正しいアクセス ドメインが表示される場合は、ステップ 9 に進みます。

a. そのアクセス ドメインの左側にある [Select] 列でボタンをクリックして、[Access Domain Name] を選択します。

b. [Select] をクリックします。更新された [Create New VLAN Resource Pool] ウィンドウが表示されます。

ステップ 7　[Save] をクリックします。

更新された [VLAN Resource Pool] ウィンドウが表示されます。

（注）　プール名は、プロバイダー名とアクセス ドメイン名の組み合わせを使用して自動的に作成されます。

（注）　アクセス ドメインの作成時に [Reserved VLANs information] にすでに入力した場合は、[Status] フィールドには [Allocated] が示されます。アクセス ドメインの作成時に [Reserved VLANs information] に入力しなかった場合は、[Status] フィールドには [Available] が示されます。VLAN プールを割り当てるには、アクセス ドメインを編集して対応する VLAN 情報を入力する必要があります （「アクセス ドメインの作成」（P.3-10）を参照）。VLAN プールのステータスは、作業の保存時に [Resource Pools] ウィンドウで自動的に [Allocated] に設定されます。

ステップ 8　VLAN 内で定義する範囲ごとにこの手順を繰り返します。

外部 VLAN プールの作成

外部 VLAN プールは EVC のイーサネットおよび EVC ATM Etherner ポリシーで AutoPick の外部 VLAN の属性とともに使用されます。外部 VLAN プールを設定する方法については、「リソース プール」（P.2-46）の項を参照してください。

VC ID プールの作成

VC ID プールは、VC ID プールの開始値とサイズを使用して定義されます。指定された VC ID プールは、どのインベントリ オブジェクト（プロバイダーまたはカスタマー）にも接続されません。L2VPN または VPLS サービスの展開中に、同じ VC ID プールから VC ID を自動割り当てすることも、手動で設定することもできます。

（注）　Prime Provisioning サービスで手動による VC ID を設定する場合は、VC ID が定義済みの VC ID プールの有効な範囲外にあると、Prime Provisioning が警告を出します。その場合、Prime Provisioning は手動で定義された VC ID を VC ID プールに入れません。手動で割り当てる VC ID の範囲を含めるよう、VC ID プールの範囲をプリセットすることを推奨します。

ネットワークごとに VC ID プールを 1 つ作成します。

VPLS インスタンスでは、すべての N-PE ルータが、エミュレーテッド仮想回線（VC）を確立するために同じ VC ID を使用します。VC-ID は、VPLS VPN のコンテキストでは VPN ID とも呼ばれます（VPLS インスタンス内のプロバイダー コアは、複数の接続回線を結合する必要があります。プロバイダー コアは、複数の接続回線を接続する仮想ブリッジをシミュレーションする必要があります。この仮想ブリッジをシミュレーションするには、VPLS インスタンスに参加するすべての N-PE ルータがその間にエミュレーテッド VC を作成する必要があります）。

（注）　VC ID は、回線またはポートを識別する 32 ビットの固有識別子です。

始める前に、作成する必要がある VC ID プールごとに次の情報があることを確認します。

- VC プールの開始番号
- VC プールのサイズ

L2VPN サービスおよび VPLS サービスの場合はすべて、次の手順を実行します。

ステップ 1　[Service Design] > [Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 2　[Pool Type] ドロップダウン リストから [VC ID] を選択します。

このプールはグローバル プールであるため、他のオブジェクトには関連付けられません。

ステップ 3　[Create] をクリックします。

[Create New VC ID Resource Pool] ウィンドウが表示されます。

ステップ 4　VC プールの開始番号を入力します。

ステップ 5　VC プールのサイズ番号を入力します。

ステップ 6　[Save] をクリックします。

更新された [Resource Pools] ウィンドウが表示されます。

名前付き物理回線の作成

L2VPN または VPLS サービス要求を作成する前に、CE と PE 間の物理リンクを事前定義する必要があります。Named Physical Circuit（NPC; 名前付き物理回線）は、物理ポートのグループを通過するリンクを表します。したがって、複数の論理リンクを同じ NPC でプロビジョニングできます。そのため、NPC は一度定義されますが、L2VPN または VPLS サービス要求のいくつかの作成中に使用されます。

NPC リンクの作成には 2 つの方法があります。

- NPC GUI エディタから。この方法の詳細については、「NPC GUI エディタによる NPC の作成」（P.3-13）を参照してください。
- 自動検出プロセスから。この方法の詳細については、「自動検出プロセスによる NPC リンクの作成」（P.3-15）を参照してください。

NPC 定義は、次の作成ルールを守る必要があります。

- NPC は、UNI があるデバイスの CE またはアップリンクあるいはリングで開始する必要があります。
- NPC は、N-PE または N-PE で終了するリングで終了する必要があります。

CE と UNI 間のリンクの NPC 情報を挿入する場合は、次のように情報を入力します。

- [Source Device] は CE デバイスです。
- [Source Interface] は UNI に接続している CE ポートです。
- [Destination Device] は UNI ボックスです。
- [Destination interface] は UNI ポートです。

CE が存在しない場合の NPC 情報を挿入する場合は、次のように情報を入力します。

- [Source Device] は UNI ボックスです。
- [Source Interface] は、N-PE あるいは別の U-PE または PE-AGG に接続している UNI ボックス上にある、UNI ポートではなく UP-LINK ポートです。
- [Destination Device] は U-PE、PE-AGG、または N-PE です。
- [Destination Interface] は、N-PE あるいは別の U-PE または PE-AGG に接続している DOWN-LINK ポートです。

単一の N-PE があり、CE がない（U-PE と CE がない）場合は、物理リンクは存在する必要がないため、NPC を作成する必要はありません。

NPC に複数のリンク（3 つ以上のデバイス）が必要な場合（たとえば、ence11、enpe1、および enpe12 に接続する）は、この NPC を次のように構築できます。

- 2 つの端 mlce1 と mlpe4 を接続するリンクを構築します。
- 作成したリンクにデバイス（enpe12）を挿入します。

NPC GUI エディタによる NPC の作成

NPC GUI エディタから NPC を作成するには、次のステップを実行します。

ステップ 1　[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。

新しい NPC を作成するには、リンクの開始として CE、終了として N-PE を選択します。複数のデバイスがリンクにある場合は、さらにデバイス（またはリング）を NPC に追加または挿入できます。

（注）　追加される新しいデバイスまたはリングは常に、選択したデバイスの後に配置され、挿入される新しいデバイスまたはリングは、選択したデバイスの前に配置されます。

[Point-to-Point Editor] の各行は物理リンクを表しています。各物理リンクには次の 5 つの属性があります。

- **Source Device**
- **Source Interface**
- **Destination Device**（N-PE でなければなりません）
- **Destination Interface**
- **Ring**

（注）　NPC でリングを追加または挿入する前に、リンクを作成してリポジトリに保存する必要があります。NPC リングの作成に関する情報を取得するには、「論理的インベントリの設定」（P.2-56）を参照してください。

[Source Device] はリンクの開始で、[Destination Device] はリンクの終了です。

ステップ 2　[Create] をクリックします。

[Create Named Physical Circuits] 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 a Device] ウィンドウが表示されます。

ステップ 4　リンクの開始として CE を選択します。

ステップ 5　[Select] をクリックします。

[Create a Named Physical Circuits] ウィンドウにデバイスが表示されます。

ステップ 6　別のデバイスまたはリングを挿入するには、[Insert Device] または [Insert Ring] をクリックします。

別のデバイスまたはリングを NPC に追加するには、[Add Device] または [Add Ring] をクリックします。この例では、N-PE を追加するには [Add Device] をクリックします。

ステップ 7　宛先デバイスとして PE を選択します。

ステップ 8　[Select] をクリックします。

デバイスが表示されます。

ステップ 9　[Outgoing Interface] 列で、[Select outgoing interface] をクリックします。

デバイスに対して定義されたインターフェイスのリストが表示されます。

ステップ 10　リストからインターフェイスを選択して、[Select] をクリックします。

ステップ 11　[Save] をクリックします。

[Create Named Physical Circuits] ウィンドウには、作成した NPC が表示されるようになります。

Ring-Only NPC の作成

CE を指定せずにリングだけが含まれている NPC を作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Named Physical Circuits] を選択します。

ステップ 2　[Create] をクリックします。

[Create Named Physical Circuits] ウィンドウが表示されます。

ステップ 3　[Add Ring] をクリックします。

[Select NPC Ring] ウィンドウが表示されます。

ステップ 4　リングを選択して、[Select] をクリックします。リングが表示されます。

ステップ 5　リングの開始を選択するには、[Select device] リンクをクリックします。

デバイスのリストが示されたウィンドウが表示されます。

ステップ 6　リングの開始であるデバイスを選択して、[Select] をクリックします。

ステップ 7　リングの終了を選択するには、[Select device] リンクをクリックします。

ステップ 8　リングの終了であるデバイスを選択して、[Select] をクリックします。

（注）　Ring-Only NPC でのリングの終了であるデバイスは、N-PE でなければなりません。

ステップ 9　Ring-Only NPC が示された [Named Physical Circuits] ウィンドウが表示されます。

ステップ 10　NPC をリポジトリに保存するには、[Save] をクリックします。

2 台の N-PE 上でのアクセス リングの終端

Prime Provisioning はサービス トポロジ内のデバイス レベルの冗長性をサポートして、1 つのアクセス リンクがドロップした場合にフェールオーバーを行います。これは、アクセス リンクが 2 台の異なる N-PE デバイスで終端できるようにする、特殊用途の NPC リングを使用することで実行できます。リング内の N-PE は、N-PE でループバック インターフェイスを使用して、論理リンクによって接続されます。冗長リンクは、U-PE デバイスから開始して、任意で PE-AGG デバイスを含めることができます。

Prime Provisioning でこれを実装する方法については、付録 C「2 台の N-PE 上でのアクセス リングの終端」を参照してください。

自動検出プロセスによる NPC リンクの作成

自動検出を使用して、ネットワーク デバイスの既存の接続を自動的に取得して、Prime Provisioning データベースに格納できます。NPC は、検出された接続からさらに抽象化されます。

自動検出を使用して NPC を作成する手順の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

疑似回線クラスの作成および変更

疑似回線クラス機能は、IOS XR 対応デバイスに L2VPN サービス要求の一部として展開される疑似回線に関連付けられたさまざまな属性を設定できるようにします。

（注）　疑似回線クラス機能は、IOS XR 3.6.1 以降でサポートされます。

疑似回線クラス機能では、カプセル化、トランスポート モード、フォールバック オプションの設定、および疑似回線を転送できるトラフィック エンジニアリング トンネルの選択がサポートされます。トンネルの選択では、Prime Provisioning Traffic Engineering Management（TEM）アプリケーションが使用されている場合は、このアプリケーションを使用してトンネルを選択できます。それ以外の場合は、ネットワーク内ですでにプロビジョニングされているトンネルの ID を指定できます。IOS XR 対応デバイスでは、疑似回線クラスは、Prime Provisioning リポジトリで別個に定義されるオブジェクトです。これは、L2VPN サービス ポリシーまたはサービス要求に接続できます。疑似回線クラス機能は、L2VPN ERS、EWS、および ATM ポリシーとサービス要求だけで使用できます。

ここでは、疑似回線クラスの作成方法および検出方法について説明します。疑似回線クラスを L2VPN ポリシーに関連付けて、サービス要求内で使用する方法については、「L2VPN ポリシーの作成」（P.3-95）と「L2VPN サービス要求の管理」（P.3-126）を参照してください

疑似回線クラスの作成

疑似回線クラスを作成するには、次のステップを実行します。

ステップ 1　[Inventory] > [Pseudowire Class] を選択します。

[Pseudowire Class] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

[Create Pseudowire Class] ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、有効な PseudoWireClass 名を入力します。

疑似回線クラス名は、IOS XR デバイスで **pw-class** コマンドをプロビジョニングするために使用されます。この名前は 32 文字を超えることはできず、スペースは使用できません。

ステップ 4　[Description] フィールドに、意味のある説明を 128 文字未満で入力します。

このフィールドはオプションです。

ステップ 5　[Encapsulation] ドロップダウン リストから、[MPLS] カプセル化タイプを選択します。

（注）　現在サポートされている唯一のカプセル化タイプは、MPLS です。

ステップ 6　[TransportMode] ドロップダウン リストからトランスポート モードを選択します。選択できる基準は、次のとおりです。

- [NONE]（デフォルト）
- Vlan
- Ethernet

（注）　[TransportMode] を [Vlan] に設定する場合は、使用する IOS XR のバージョンでサポートされるときは、疑似回線クラスから行うことを推奨します。疑似回線クラスが特定のバージョンの IOS XR でサポートされない場合は、「疑似回線クラスがサポートされない場合のトランスポート モードの設定」（P.3-19）で説明されているように、Dynamic Component Properties Library（DCPL）プロパティを使用して [TransportMode] を設定する必要があります。

ステップ 7　[Protocol] ドロップダウン リストからプロトコルを選択します。選択できる基準は、次のとおりです。

- [NONE]（デフォルト）
- [LDP]：この疑似回線クラスのシグナリング プロトコルとして LDP を設定します。

ステップ 8　受信または送信でのシーケンス処理を設定するには、[Sequencing] ドロップダウン リストから選択します。選択できる基準は、次のとおりです。

- [NONE]（デフォルト）
- [BOTH]：受信と送信でシーケンス処理を設定します。
- [TRANSMIT]：送信でシーケンス処理を設定します。
- [RECEIVE]：受信でシーケンス処理を設定します。

ステップ 9　Prime Provisioning によってすでにプロビジョニングされているか、デバイスで手動でプロビジョニングした TE トンネルの [Tunnel ID] を入力します。

この値はオプションです。次のステップで説明されているように、Prime Provisioning によってすでにプロビジョニングされている TE トンネルを選択することもできます。

ステップ 10　Prime Provisioning によって以前にプロビジョニングされた TE トンネルを選択する場合は、[Select TE Tunnel] をクリックします。

[Select TE Tunnel] ポップアップ ウィンドウが表示されます。TE トンネルを選択して、[Select] をクリックします。これによって、選択した TE トンネルの ID が [TE Tunnel] フィールドに入力されます。

（注）　TE トンネルを疑似回線クラスに関連付けるか、サービス要求でプロビジョニングした後で、Traffic Engineering Management（TEM）アプリケーションを使用して TE トンネルを削除しようとすると、エラー メッセージが表示されます。疑似回線クラスまたはサービス要求に関連付けられた TE トンネルは削除できません。

ステップ 11　疑似回線トンネルのフォールバック オプションをディセーブルにするには、[Disable Fallback] チェックボックスをオンにします。

このオプションは、IOS XR のバージョンに基づいて選択します。IOS XR 3.6.1 では必須で、IOS XR 3.7 以降では任意です。

疑似回線クラスの変更

ここでは、既存の疑似回線クラスの変更（編集）方法、および編集操作が L2VPN サービス要求に与える可能性がある影響について説明します。

疑似回線クラスを変更するには、次のステップを実行します。

ステップ 1　[Inventory] > [Pseudowire Class] を選択します。

[Pseudowire Class] ウィンドウが表示されます。

ステップ 2　変更する疑似回線クラス オブジェクトを選択して、[Edit] をクリックします。

[PseudoWire Class Edit] ウィンドウが表示されます。

ステップ 3　必要な変更を行って、[Save] をクリックします。

（注）　疑似回線クラスがサービス要求に関連付けられている場合は、[Name] フィールドは編集不可能です。

変更する疑似回線クラスが L2VPN サービス要求に関連付けられている場合は、影響を受けるサービス要求のリストが示された [Affected Jobs] ウィンドウが表示されます。

（注）　影響を受けるサービス要求のリストは、変更する疑似回線クラスで [Transport Mode]、[Tunnel ID]、または [Disable Fallback] 値を変更した場合だけ表示されます。

ステップ 4　変更した疑似回線クラスに関連付けられたサービス要求を更新するには、[Save] をクリックします。

影響を受けるサービス要求は、[Requested] 状態に移行されます。

ステップ 5　変更した疑似回線クラスに関連付けられたサービス要求を更新して展開するには、[Save and Deploy] をクリックします。

展開タスクは、以前に [Deployed] 状態だった、影響を受けるサービス要求で作成されます。

ステップ 6　変更した疑似回線クラスに行った変更を廃棄するには、[Cancel] をクリックします。

この場合は、疑似回線クラスに関連付けられたサービス要求では状態の変更は行われません。

疑似回線クラスの削除

疑似回線クラスを削除するには、次の手順を実行します。

（注）　サービス要求またはポリシーで使用中の疑似回線クラスは削除できません。

ステップ 1　[Inventory] > [Pseudowire Class] を選択します。

[Pseudowire Classes] ウィンドウが表示されます。

ステップ 2　削除する疑似回線クラスの横にあるチェックボックスをオンにします。

ステップ 3　[Delete] ボタンをクリックすると、選択した疑似回線クラスの名前とともにウィンドウが表示されます。

ステップ 4　[Delete] ボタンをクリックして、指定した疑似回線クラスを削除することを確定します。

ステップ 5　指定した疑似回線クラスを削除せずに戻るには、[Cancel] をクリックします。

疑似回線クラスがサポートされない場合のトランスポート モードの設定

ここでは、疑似回線クラスがサポートされないバージョンの IOS XR で、タイプ Vlan にする疑似回線トランスポート モードの設定方法について説明します。これは、Dynamic Component Properties Library（DCPL）プロパティを設定することで行います。追加情報については、ステップの後の使用方法に関する注釈を参照してください。

次のステップを実行します。

ステップ 1　Prime Provisioning で、[Administration] > [Hosts] と移動します。

ステップ 2　特定のホストのチェックボックスをオンにして、[Config] ボタンをクリックします。

ステップ 3　DCPL プロパティ **Services\Common\pseudoWireVlanMode** にナビゲートします。

ステップ 4　プロパティを **true** に設定します。

ステップ 5　[Set Property] をクリックします。

Prime Provisioning は、疑似回線の VLAN トランスポート モード設定を生成します。

使用方法に関する注釈：

- トランスポート モードを Vlan に設定する場合は、使用する IOS XR のバージョンでサポートされるときは、疑似回線クラスから行うことを推奨します。疑似回線クラス機能がサポートされない場合は、トランスポート モードは、ステップで説明されているように DCPL プロパティを使用して設定する必要があります。
- DCPL プロパティ pseudoWireVlanMode は、DCPL プロパティが true に設定されている場合は、PseudoWireClass TransportMode のデフォルト値を Vlan に設定するだけです。ユーザは、これを常に上書きできます。
- DCPL プロパティ pseudoWireVlanMode は 2 つの方法で機能します。
  - これは、PseudoWireClass TransportMode のデフォルト値を Vlan に設定します。
  - 疑似回線クラスがない場合は、非推奨のコマンドである **transport-mode vlan** を生成します。**transport-mode vlan** コマンドは、IOS XR 3.6 以降では非推奨のコマンドです。そのため、IOS XR デバイスで疑似回線クラスを選択して、さらに DCPL プロパティが true に設定されている場合は、**transport-mode vlan** コマンドは生成されません。疑似回線クラスと **transport-mode vlan** コマンドは共存しません。疑似回線クラスが存在する場合は、これは非推奨の **transport-mode vlan** コマンドに優先します。
- DCPL プロパティ pseudoWireVlanMode の値は、サービス要求の存続期間中に変更することはできません。

IOS XR デバイスの L2VPN グループ名の定義

ここでは、IOS XR デバイスのポリシーとサービス要求に使用可能な L2VPN グループ名を指定する方法について説明します。選択項目は、ポリシーとサービス要求の [L2VPN Group Name] 属性のドロップダウン リストに表示されます。選択した名前は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。選択は、Dynamic Component Properties Library（DCPL）プロパティを設定することで定義されます。

次のステップを実行します。

ステップ 1　Prime Provisioning で、[Administration] > [Hosts] と移動します。

ステップ 2　特定のホストのチェックボックスをオンにして、[Config] ボタンをクリックします。

ステップ 3　DCPL プロパティ **Services\Common\l2vpnGroupNameOptions** にナビゲートします。

ステップ 4　[New Value] フィールドに L2VPN グループ名のコンマ区切りのリストを入力します。

ステップ 5　[Set Property] をクリックします。

EVC イーサネット ポリシーの作成

この項には、Cisco Prime Provisioning 6.3 での EVC サポートの概要、および EVC イーサネット ポリシーを作成するための基本的な手順が記載されています。具体的な内容は、次のとおりです。

- 「EVC イーサネット ポリシーの定義」（P.3-20）
- 「サービス オプションの設定」（P.3-22）
- 「EVC 属性の設定」（P.3-25）
- 「インターフェイス属性の設定」（P.3-30）
- 「テンプレートの関連付けのイネーブル化」（P.3-36）

EVC イーサネット サービス要求の作成については、「EVC イーサネット サービス要求の管理」（P.3-36）を参照してください。

（注）　Prime Provisioning での EVC サポートの一般的な概要については、*『Cisco Prime Provisioning 6.3 Administration Guide』*の「Layer 2 Concepts」の章を参照してください。

（注）　イーサネット（E-Line および E-LAN）サービスでは、EVC ポリシーとサービス要求を使用することを推奨します。EVC 構文を使用してサービスのプロビジョニングを行っている場合、または今後その予定がある場合は、EVC サービスを使用します。L2VPN および VPLS のサービス ポリシー タイプを使用してプロビジョニングした既存のサービスは、現在もサポートされており、そのサービス タイプとともに保守できます。ATM サービスと FRoMPLS サービスでは、以前と同様に、L2VPN サービス ポリシーを使用します。

EVC イーサネット ポリシーの定義

サービスをプロビジョニングするには、EVC イーサネット ポリシーを定義する必要があります。ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。

ポリシーは、EVC サービス要求の定義に必要な大部分のパラメータのテンプレートです。定義後に、共通する一連の特性を共有するすべての EVC サービス要求で EVC ポリシーを使用できます。新しいタイプのサービスまたは異なるパラメータを持つサービスを作成する場合は、常に新しい EVC ポリシーを作成します。EVC ポリシーの作成は通常、経験のあるネットワーク エンジニアが実行します。

ネットワーク オペレータは、ポリシーの属性の [Editable] チェックボックスを使用すると、フィールドを編集可能にするオプションを利用できます。値が [editable] に設定されている場合は、サービス要求の作成者は、特定のポリシー属性の値を変更できます。値が [editable] に設定*されていない*場合は、サービス要求の作成者は属性を変更できません。

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 ファイルの使用方法の詳細については、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。

EVC イーサネット ポリシーを定義するには、最初にサービス タイプ属性を設定します。これを行うには、次のステップを実行します。

ステップ 1　[Service Design] > [Create Policy] 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　[Policy Type] ドロップダウン リストから [EVC] 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　EVC ポリシーの [Policy Name] を入力します。

ステップ 4　EVC ポリシーの [Policy Owner] を選択します。

EVC 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：すべてのサービス オペレータがこの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 EVC 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。

ステップ 5　EVC ポリシーの所有者を選択するには、[Select] をクリックします。

ポリシー所有者は、Prime Provisioning の設定中にカスタマーまたはプロバイダーを作成した際に設定しました。所有権がグローバルの場合は、[Select] 機能は表示されません。

ステップ 6　[Policy Type] を選択します。

選択できる基準は、次のとおりです。

- [ETHERNET]：この項です。
- [ATM]：「ATM ポリシーの作成」（P.4-19）を参照してください。
- [ATM-Ethernet Interworking]：「EVC ATM-Ethernet インターワーキング ポリシーの作成」（P.3-58）を参照してください。
- [TDM Circuit Emulation]：「CEM TDM ポリシーの作成」（P.4-6）を参照してください。

ステップ 7　[Next] をクリックします。

[Service Options] ウィンドウが表示されます。

ステップ 8　次の項である「サービス オプションの設定」（P.3-22）に記載されているステップに進みます。

サービス オプションの設定

この項では、EVC イーサネット ポリシーのサービス オプションの設定方法について説明します。

EVC サービス オプションを設定するには、次の手順を実行します。

ステップ 1　CE が N-PE に直接接続されている場合は、[CE Directly Connected to EVC] 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は、デフォルトでオフになっています。

（注）　[Editable] チェックボックスを使用すると、フィールドを編集可能にするオプションを使用できます。[Editable] チェックボックスをオンにすると、この EVC ポリシーを使用しているサービス オペレータは、EVC サービス要求の作成中に編集可能パラメータを変更できます。

使用方法に関する注釈：

- チェックボックスをオンにすると、このポリシーを使用して作成されたサービス要求は、直接接続リンクだけを持つことができます。イーサネット アクセス ノードは含められません。
- チェックボックスをオフにすると、このポリシーを使用して作成されたサービス要求は、リンクにイーサネット アクセス ノードを持つ場合と、持たない場合があります。
- CE が N-PE に直接接続されている場合は、NPC は、サービス要求の作成中にリンクには適用されません。
- CE が N-PE に直接接続されていない場合は、NPC は、Prime Provisioning の標準の動作に従って、サービス要求の作成中に使用されます。EVC 機能をサポートするための NPC の実装への変更はありません。

ステップ 2　EVC 機能を使用してすべてのリンクを設定する必要がある場合は、[All Links Terminate on EVC] 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は、デフォルトでオフになっています。使用方法に関する注釈：

- チェックボックスをオンにすると、そのようなポリシーを使用して作成されたサービス要求は、EVC 機能を使用したすべてのリンクを持つようになります。
- チェックボックスをオフにすると、ゼロ以上のリンクが EVC 機能を使用できるようになります。これは、サービスを配信しながら、1 つ以上のリンクで既存のプラットフォームを引き続き使用できるようにします。これによって、EVC サポートとのリンクを将来追加できるようになります。

  （注）　チェックボックスをオフにすると、サービス要求の作成プロセスで、ユーザは、作成されたリンクが EVC であるか、非 EVC であるかを指定する必要があります。

- リンクが将来も EVC 機能を使用しないことが予期される場合（たとえば、プロバイダーが作成されるサービスの EVC インフラストラクチャにアップグレードする予定がない場合）は、EVC の代わりに、既存の Prime Provisioning ポリシー タイプ（L2VPN または VPLS）を使用できます。

ステップ 3　ドロップダウン リストから [MPLS Core Connectivity Type] を選択します。

（注）　コア オプションでは MPLS だけがサポートされます。このサービスに対する L2TPv3 サポートはありません。

選択できる基準は、次のとおりです。

- [PSEUDOWIRE] : MPLS コアにわたって 2 つの N-PE 間の接続を許可するには、このオプションを選択します。このオプションは、サービスをポイントツーポイント（E-Line）に制限しません。これは、[PSEUDOWIRE] オプションが選択されている場合でも、疑似回線の片側または両方の側のブリッジ ドメインに接続されている CE が引き続き複数存在する可能性があるためです。
- [LOCAL] : MPLS コアにわたる接続が必要ないローカル接続のケースでは、このオプションを選択します。

  ローカル接続では、次のシナリオがサポートされます。

  - N-PE 上のすべてのインターフェイスが EVC 対応で、EVC インフラストラクチャを使用しています。これは、これらのインターフェイス上のカスタマー トラフィックをすべてブリッジ ドメインに関連付けることで設定します。これは、N-PE 上で VLAN ID（ブリッジ ドメイン ID と等しい）を消費します。
  - N-PE 上の一部のインターフェイスは EVC 対応ですが、他はスイッチ ポート ベースです。そのような場合は、EVC インフラストラクチャを使用して設定されたインターフェイス上のカスタマー トラフィックはすべて、ブリッジ ドメインに関連付けられます。非 EVC インターフェイス上のトラフィック（およびこの N-PE 以外のすべてのアクセス ノードまたはインターフェイス）は、サービス プロバイダー VLAN ID を使用して設定されます。この場合、サービス プロバイダー VLAN ID は、EVC ベース サービスのブリッジ ドメイン ID と同じです。
  - N-PE 上の 2 つのインターフェイスだけが使用され、両方とも EVC 対応ラインカードに基づいています。最初のケースでは、オペレータは、ブリッジ ドメイン オプションを設定しないことを選択することがあります。この場合、ローカル接続に使用される **connect** コマンドが使用され、グローバル VLAN がデバイスで保存されます。オペレータがブリッジ ドメイン オプションを使用した設定を選択する場合は、両方のインターフェイスがブリッジ ドメイン ID に関連付けられるため、追加のローカル リンクを将来サービスに追加できます。これは、N-PE で VLAN ID（ブリッジ ドメイン ID）を消費します。
- [VPLS] : MPLS コアにわたって複数の N-PE 間の接続を許可するには、このオプションを選択します。
  - これには MPLS-TP 対応ネットワーク上のマルチセグメント疑似回線のサポートが含まれます。VPLS インスタンスに相互接続する LSP の一部またはすべてが既存の MPLS-TP トンネルでアドミッションできます（Prime Provisioning を使用してプロビジョニングされている場合があります）。LSP は、各ホップを MPLS-TP トンネルでアドミッションできるマルチセグメント疑似回線として設定できます。Prime Provisioning は、ノードやトンネルが含まれているかどうかを考慮して、最短パスに沿ってマルチセグメント疑似回線を自動的にルーティングします。
  - LSP/pseudowire ラベルは Prime Provisioning によって静的に割り当てることができます。これによって、転送されたプロトコルを VPLS 内で実行してラベル交換を行う必要がなくなるため、VPLS 内のエンドポイント間の IP 接続が不要になります。
  - MPLS ラベルのプールは VPLS と MPLS-TP サービスを通じて（デバイスで同じ MPLS スタティック ラベル範囲から取得される場合）共有されます。それ以外の場合、Prime Provisioning はデバイスに設定された別個のトンネルとサービス ラベルの範囲を使用します。MPLS ラベルが一意に割り当てられるように、使用中のラベルが検出され、ラベル プールから削除されます。

  サービス要求内の MPLS コア全体での N-PE の数に制限はありません。ただし、多数のサービス要求が、同じカスタマー関連 VPN を参照することがあります。

（注） ポリシー ワークフローの後続のウィンドウで使用可能な属性は、[MPLS Core Connectivity Type] に選択した項目（[PSEUDOWIRE]、[LOCAL]、または [VPLS]）に基づいて動的に変わります。完全性を確保するため、さまざまなコア タイプに使用できるすべての属性が、次のステップで説明されています。属性は、別途明記されていない限り、すべてのコア タイプに適用されます。

（注）　また、一部の属性は、IOS または IOS XR プラットフォームだけでサポートされます。属性は、別途明記されていない限り、両方のプラットフォームに適用されます。すべてのプラットフォーム固有属性が、ポリシー ワークフロー ウィンドウに表示されます。後で、ポリシーに基づいてサービス要求を作成する（および特定のデバイスがサービス要求に関連付けられる）際に、プラットフォーム固有属性は、デバイス タイプ（IOS または IOS XR）に基づいて、サービス要求ウィンドウからフィルタリングされます。

ステップ 4　ブリッジ ドメインの特性を判別するには、[Configure With Bridge Domain] チェックボックスをオンにします。

[Configure With Bridge-Domain] オプションの動作は、次に示すように、[MPLS Core Connectivity Type] オプションで選択した項目と並行して動作します。

- [MPLS Core Connectivity Type] として [PSEUDOWIRE] を選択。次の 2 つのケースがあります。

  A.EVC の場合

  - [Configure With Bridge Domain] をオンにすると、ポリシーは、ブリッジ ドメインに関連付けられた SVI 下で疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サービス インスタンス下で直接疑似回線を設定します。これによってグローバル VLAN が保存されます。

  B.EVC を使用しない場合

  - [Configure With Bridge Domain] をオンにすると、ポリシーは、L2VPN サービス（SVI を使用）の場合と同様に疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サブインターフェイス下で直接疑似回線を設定します。

  疑似回線だけを、対応する EVC 対応インターフェイスのサービス インスタンス下、またはブリッジ ドメインに関連付けられた SVI の下のいずれかで直接設定できます。

- [MPLS Core Connectivity Type] として [LOCAL] を選択。
  - [Configure With Bridge Domain] をオンにすると、ポリシーでは、ポイントツーポイント ローカル接続サービスまたはマルチポイント ローカル接続サービスのいずれかが許可されます。
  - [Configure With Bridge Domain] がオフの場合、Prime Provisioning はブリッジ ドメインなしのポイントツーポイント ローカル接続のみを許可します。
- [VPLS] : [Configure With Bridge Domain] はデフォルトでオンにされ、編集不可能です。

  VPLS サービス オプションを選択すると、VPLS 固有サービス オプションが表示されます。
  - 自動的にスタティック ラベルを割り当てるには、[Static VPLS (AutoPick MPLS Labels)] チェックボックスをオンにします。
    スタティック ラベルは、サービス要求を保存するときに割り当てられます。
  - [Configure Pseudowire Segment(s)] チェックボックスをオンにすると、VPLS サービスが MPLS-TP トンネルでアドミッションされ、トンネルがともに「切り替え」られ、シミュレートされたエンドツーエンドのパスが形成されます。

ステップ 5　[Next] をクリックします。

EVC の [Attributes] ウィンドウが表示されます。

ステップ 6　次の項である「EVC 属性の設定」（P.3-25）に記載されているステップに進みます。

EVC 属性の設定

この項では、EVC イーサネット ポリシーの EVC 属性を設定する方法について説明します。

EVC 属性は、次のカテゴリに編成されます。

- Service Attributes
- VLAN Match Criteria
- VLAN Rewrite Criteria

次の項では、各カテゴリのオプションの設定方法について説明します。

[Service] 属性の設定

EVC サービス属性は、どの MPLS コア接続タイプが選択された場合でも同じです。

EVC サービス属性を設定するには、次の手順を実行します。

ステップ 1　サービス要求の作成中にサービス インスタンス ID を自動生成し、リンクに割り当てることを指定するには、[AutoPick Service Instance ID] チェックボックスをオンにします。

チェックボックスをオフにすると、サービス要求の作成中に Prime Provisioning リンク属性を設定するときに、Prime Provisioning は、サービス インスタンス ID を指定するようオペレータに求めます。

使用方法に関する注釈：

- サービス インスタンス ID は、EVC インフラストラクチャ内のインターフェイス上の Ethernet Flow Point（EFP; イーサネット フロー ポイント）を表します。サービス インスタンス ID は、インターフェイスに対してローカルで有効です。この ID は、インターフェイス レベルだけで固有でなければなりません。ID は 1 ～ 8000 までの値でなければなりません。
- Prime Provisioning では、サービス インスタンス ID の割り当て元として使用可能なリソース プールはありません。
- サービス要求を作成するオペレータが、インターフェイス レベルで ID の一意性を維持する必要があります。

ステップ 2　ポリシーに基づいたサービス要求の作成時に Prime Provisioning にサービス インスタンス名を自動生成させるには、[AutoPick Service Instance Name] チェックボックスをオンにします。自動生成される値のパターンは、*CustomerName_ServiceRequestJobID* です。

チェックボックスをオフにすると、サービス要求の作成中に値を入力できます。

ステップ 3　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[Enable PseudoWire Redundancy] 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：

- [Enable Pseudo Wire Redundancy] は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- このオプションの使用方法に関する注釈については、付録 C「2 台の N-PE 上でのアクセス リングの終端」、および特に「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）を参照してください。

ステップ 4　サービス要求の作成中に Prime Provisioning に VC ID を自動選択させるには、[AutoPick VC ID] 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フにすると、オペレータは、サービス要求の作成中に VC ID を指定するよう求められます。

使用方法に関する注釈：

- この属性は、[Service Options] ウィンドウで [MPLS Core Connectivity of Type] が [PSEUDOWIRE] または [VPLS] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- [AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。
- [MPLS Core Connectivity of Type] が [VPLS] の場合は、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから VPLS VPN ID を割り当てます。

ステップ 5　サービス要求の作成中に、Prime Provisioning に仮想転送インスタンス（VFI）を自動選択させるには、[AutoPick VFI Name] 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フにすると、オペレータは、サービス要求の作成中に VFI 名を指定するよう求められます。

（注）　[AutoPick VFI Name] 属性は、[MPLS Core Connectivity Type] が [VPLS] に設定されている場合にのみ使用できます。他のコア タイプの場合（PSEUDOWIRE および LOCAL）、この属性は表示されません。

ステップ 6　サービス要求の作成中に Prime Provisioning にサービス要求の VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにすると、オペレータは、サービス要求の作成中に VLAN ID を指定するよう求められます。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメインまたは VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。サービス要求で VLAN ID を割り当てると、Prime Provisioning は、後続のサービス要求では VLAN ID を使用不可にします。
- 手動による VLAN ID の割り当ての場合は、ID が Prime Provisioning によって管理される VLAN プールの範囲外にあると、Prime Provisioning は VLAN ID を管理しません。この場合は、オペレータは、イーサネット アクセス ドメインで ID の一意性を確保する必要があります。オペレータが、Prime Provisioning によって管理される VLAN プールの範囲内にある VLAN ID を指定した場合に、その VLAN ID がアクセス ドメインですでに使用中であるときは、Prime Provisioning は、VLAN ID が使用中であることを示すエラー メッセージを表示します。

アクセス VLAN ID に関する注釈

アクセス VLAN ID は、EVC 対応ポートに対してローカルで有効です。グローバル VLAN と混同しないでください。これは、EVC ポートの向こうにあるイーサネット アクセス ネットワークをいくつかのサブイーサネット アクセス ドメインにパーティション化する（EVC 対応ポートごとに 1 つ）ことで可視化できます。

ただし、EVC ポートの向こうにあるイーサネット アクセス ノード上のすべてのサービス インターフェイスには、リンクのこの同じ VLAN ID が割り当てられます。この ID は、サービス要求の作成中にリンク属性を設定する際にオペレータが手動で指定する必要があります。オペレータは、EVC-demarcated イーサネット アクセス ドメインにわたって ID の一意性を確保する必要があります。

これらの VLAN ID は、ローカルで有効な VLAN プールを使用して Prime Provisioning によって管理されません。ただし、サービス要求でリンクに VLAN ID を割り当てた後で、Prime Provisioning は、EVC によって境界が定められたイーサネット アクセス ドメイン内の後続のサービス要求では VLAN を使用不可にします。同様に、手動で指定した VLAN が、EVC によって区切られたアクセス ドメイ

ンですでに使用中の場合は、Prime Provisioning は、指定された新しい VLAN ID が NPC ですでに使用中であることを示すエラー メッセージを表示します。オペレータは、L2 アクセス ノードでプロビジョニングされる別の VLAN ID を指定するよう求められます。

ステップ 7　サービス要求の作成中に Prime Provisioning にサービス要求のグループ名を自動選択させるには、[AutoPick Bridge Group Name] 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フにすると、オペレータは、サービス要求の作成中にグループ名を指定するよう求められます。チェックボックスをオンにすると、グループ名はデフォルトでカスタマー名に設定されます。

（注）　この属性は、サポートされる IOS XR デバイスだけに適用されます。

ステップ 8　サービス要求の作成中に Prime Provisioning にサービス要求のドメイン名を自動選択させるには、[AutoPick Bridge Domain Name] 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フにすると、オペレータは、サービス要求の作成中にドメイン名を指定するよう求められます。
- チェックボックスをオンにすると、ドメイン名はデフォルトで次の形式に設定されます。
  - 疑似回線とローカル接続コア タイプの場合：*ISC-Job-Job_ID*。ここで、*Job_ID* はサービス要求ジョブ ID です。
  - VPLS コア タイプの場合：*ISC-VPN_Name-VPN_ID*。ここで、*VPN_Name* は、使用されている VPLS VPN の名前で、*VPN_ID* は、サービス要求で使用される VPN ID です。

（注）　この属性は、サポートされる IOS XR デバイスだけに適用されます。

ステップ 9　次の項である「VLAN 一致基準属性の設定」（P.3-27）に記載されているステップに進みます。

VLAN 一致基準属性の設定

EVC 機能を導入する前に、サービス プロバイダーは、単一のポートでサービス多重化サービス（ERS/ERMS または EVPL/EVCS）またはサービス バンドル サービスのいずれかを展開できます。インフラストラクチャの制限が原因で、両方を同時にサポートすることはできません。この制限では、最外部の VLAN タグの照合だけが許可されます。

Prime Provisioning での EVC サポートの主な利点の 1 つは、着信フレームの VLAN タグ（最大 2 つのレベル）を調べて、適切なイーサネット フロー ポイント（EFP）に関連付けるための柔軟な方法が提供されることです。これによって、サービス プロバイダーは、サービス多重化サービスとサービス バンドル サービスの両方を単一のポートに同時に展開できます。

EVC VLAN 一致基準属性を設定するには、次の手順を実行します。

ステップ 1　ポリシーを使用して作成されたサービス要求を、着信フレームの内部 VLAN タグと外部 VLAN タグの両方と一致させるには、[Both Tags] 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しないと、ポリシーを使用して作成されたサービス要求は、着信フレームの外部 VLAN タグだけと一致します。

[Both Tags] 属性をオンにすると、[Inner VLAN Ranges] 属性（次の手順で説明）が [EVC Attribute] ウィンドウに表示されます。

ステップ 2　サービス要求の作成中に内部 VLAN タグの範囲を指定できるようにするには、[Inner VLAN Ranges] チェックボックスをオンにします。

チェックボックスをオフにすると、内部 VLAN タグの範囲は許可されません。この場合は、オペレータは、サービス要求の作成中に別個の VLAN ID を指定する必要があります。

ステップ 3　サービス要求の作成中に外部 VLAN タグの範囲を指定できるようにするには、[Outer VLAN Ranges] チェックボックスをオンにします。

チェックボックスをオフにすると、外部 VLAN タグの範囲は許可されません。この場合は、オペレータは、サービス要求の作成中に別個の VLAN ID を指定する必要があります。

ステップ 4　サービス要求の作成中に、以前に作成した外部 VLAN ID リソース プールから外部 VLAN ID を Prime Provisioning が自動選択するように設定するには、[AutoPick Outer VLAN] 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フにすると、オペレータは、サービス要求の作成中に外部 VLAN ID を指定するよう求められます。

（注）　[AutoPick Outer VLAN] 属性を使用するには、2 つの要素が Prime Provisioning で事前に設定されている必要があります。1 つめの要素はインターフェイス アクセス ドメインであり、これは N-PE デバイスの物理ポートをグループ化する論理要素です。2 つめの要素は EVC 外部 VLAN リソース プールであり、これはインターフェイス アクセス ドメインによって使用されます。これらの要素を設定する方法については、項「リソースの設定」（P.2-42）と「リソース プール」（P.2-46）を参照してください。

使用方法に関する注釈：

- [AutoPick Outer VLAN] は、EVC 機能をサポートするインターフェイスに使用できます。
- [AutoPick Outer VLAN] は、EVC をサポートするインターフェイスで VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 5　次の項である「VLAN 書き換え基準属性の設定」（P.3-28）に記載されているステップに進みます。

VLAN 書き換え基準属性の設定

VLAN 一致基準とともに、VLAN 書き換えは、EVC インフラストラクチャを非常に強力かつ柔軟にします。次の VLAN 書き換えオプションがサポートされています。

- 1 つまたは 2 つのタグをポップする。
- 1 つまたは 2 つのタグをプッシュする。
- 変換（1:1、2:1、1:2、2:2）。

VLAN 書き換え基準属性を設定するときは、次の点に注意してください。

- どの CE-facing EVC リンクでも、行うことができる書き換えは 1 種類だけです。
- すべての VLAN 書き換えは、入力トラフィックで **symmetric** キーワードを使用して行われます（たとえば、**rewrite ingress tag pop 2 symmetric**）。
- すべてのサービス インスタンスで、インスタンスごとに 1 つのタイプの書き換えオプション（ポップ、プッシュ、または変換）だけが許可されます。たとえば、[pop outer] をイネーブルにすると、[push inner]、[push outer]、[translate inner]、および [translate outer] は使用できません。

EVC VLAN 書き換え基準属性を設定するには、次の手順を実行します。

ステップ 1　一致基準を満たす着信フレームの外部 VLAN ID タグをポップするには、[Pop Outer] 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フにすると、着信トラフィックの外部タグはポップされません。

ステップ 2　一致基準を満たす着信フレームの内部 VLAN ID タグをポップするには、[Pop Inner] 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フにすると、内部タグはポップされません。[Pop Inner] をオンにすると、[Pop Outer] が自動的にオンになることに注意してください。

ステップ 3　一致基準を満たす着信フレームの外部 VLAN ID タグをインポーズするには、[Push Outer] 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フにすると、外部タグは着信フレームでインポーズされません。

使用方法に関する注釈：

- [Push Outer] をオンにする場合は、ポリシーを使用して作成されたすべてのサービス要求が、一致基準と一致する着信フレームで dot1q 外部タグをプッシュします。サービスの作成中にリンクを作成する場合は、オペレータは、1 ～ 4096 までの値で外部タグを指定できます。
- この属性は、一致基準で使用されるタグの数に関係なく使用可能です。着信トラフィックがダブルタグ付きであるか、シングルタグ付きであるかに関係なく、[Push Outer] をイネーブルにすると、対応するすべてのサービス要求が外部タグをプッシュします。後続のノードはすべて、最外部の 2 つのタグ（EVC 対応の場合）または 1 つのタグ（EVC 対応ではない場合）だけを考慮し、最内部のタグを透過的にペイロードとして扱います。
- この VLAN ID は、Prime Provisioning 管理の VLAN ID プールからは得られません。

ステップ 4　一致基準を満たす着信フレームの内部 VLAN ID タグをインポーズするには、[Push Inner] チェックボックスをオンにします。

この操作は、内部タグだけでなく、内部タグと外部タグの両方を着信パケットにプッシュします。このチェックボックスをオフにすると、内部タグは着信フレームでインポーズされません。

使用方法に関する注釈：

- [Push Inner] をオンにする場合は、ポリシーを使用して作成されたすべてのサービス要求が、一致基準と一致する着信フレームで dot1q 内部タグをプッシュします。サービスの作成中にリンクを作成する場合は、オペレータは、1 ～ 4096 までの値で内部タグを指定できます。
- [Push Inner] をオンにすると、[Pop Outer] が自動的にオンになります。
- この属性は、一致基準で使用されるタグの数に関係なく使用可能です。着信トラフィックがダブルタグ付きであるか、シングルタグ付きであるかに関係なく、[Push Inner] をイネーブルにすると、対応するすべてのサービス要求が内部タグをプッシュします。後続のノードはすべて、最外部の 2 つのタグ（EVC 対応の場合）または 1 つのタグ（EVC 対応ではない場合）だけを考慮し、最内部のタグを透過的にペイロードとして扱います。
- この VLAN ID は、Prime Provisioning 管理の VLAN ID プールからは得られません。

ステップ 5　サービス要求の作成中にオペレータがターゲットの外部 VLAN ID を指定できるようにするには、[Translate Outer] チェックボックスをオンにします。

一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。チェックボックスをオフにすると、外部タグの変換は実行されません。表 3-2 を参照してください。

ステップ 6　サービス要求の作成中にオペレータがターゲットの内部 VLAN ID を指定できるようにするには、[Translate Inner] チェックボックスをオンにします。

一致基準を満たすすべての着信フレームの内部タグがこの ID に変換されます。チェックボックスをオフにすると、内部タグの変換は実行されません。表 3-2 を参照してください。

（注）　表 3-2 には、EVC インフラストラクチャで使用可能なさまざまな VLAN 変換の実行の要約が示されています。2 番めと 3 番めの列（「外部タグと一致」と「内部タグと一致」）は、ポリシー設定を示しています。最後の 2 つの列（「外部タグの変換」と「内部タグの変換」）は、着信フレームで行われる VLAN 変換を示しています。

表 3-2　VLAN 変換の要約表

タイプ	外部タグと一致	内部タグと一致	外部タグの変換	内部タグの変換	プッシュ外部タグ
1:1	True	N/A	Yes	No	N/A
1:2	True	N/A	N/A	N/A	Yes
2:1	True	True	Yes	No	N/A
2:2	True	True	Yes	Yes	N/A

ステップ 7　[Next] をクリックします。

[Interface Attribute] ウィンドウが表示されます。

ステップ 8　次の項である「インターフェイス属性の設定」（P.3-30）に記載されているステップに進みます。

インターフェイス属性の設定

EVC のイーサネット ポリシー作成のこの手順には、[Interface Attribute] ウィンドウでのインターフェイス属性の設定が含まれます。このウィンドウで設定できる属性は、次のカテゴリにグループ化されます。

- UNI 情報
- VLAN
- 疑似回線
- ACL
- セキュリティ
- UNI ストーム制御
- プロトコル

場合によっては、属性を確認すると、GUI に追加の属性が表示されます。これは、次のステップで説明します。

（注）　CE が N-PE に直接接続されている場合は、速度、デュプレックス、UNI シャットダウン、およびその他の汎用オプションだけが表示されます。この場合は、現在のプラットフォームの制限が原因で、ポート セキュリティ、ストーム制御、L2 プロトコル トンネリング、およびその他の高度な機能はサポートされません。サービスでこれらの機能が必要な場合、サービス プロバイダーは、これらの要件をサポートするためにレイヤ 2 イーサネット アクセス ノードを EVC の外にまで展開する必要があります。

（注）　[Interface Attributes] ウィンドウで使用可能な属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] に選択した項目（[PSEUDOWIRE]、[LOCAL]、または [VPLS]）に基づいて動的に変わります（「サービス オプションの設定」（P.3-22）を参照）。完全性を確保するため、さまざまなコア タイプに使用できるすべての属性が、次のステップで説明されています。属性は、別途明記されていない限り、すべてのコア タイプに適用されます。

EVC インターフェイス属性を設定するには、次の手順を実行します。

ステップ 1　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 2　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 3　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために、編集可能です。

ステップ 4　[Link Media]（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

ステップ 5　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 6　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- [DOT1QTRUNK] : 802.1q カプセル化によって UNI をトランクとして設定します。UNI が直接接続された EVC リンクに属している場合、この設定は、着信フレームが 802.1q カプセル化され、リンクに設定された VLAN ID と一致することを意味します。この固有のトポロジには、トランク UNI 自体は含まれていません。
- [DOT1QTUNNEL] : UNI を 802.1q トンネル（dot1q トンネルまたは Q-in-Q とも呼ばれています）ポートとして設定します。
- [ACCESS] : UNI をアクセス ポートとして設定します。

ステップ 8　適切なオプション ボタンをクリックして、このポリシーの [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No] : VLAN 変換は実行されません （デフォルト）。
- [1:1] : 1:1 VLAN 変換。着信カスタマー VLAN を別のものに変換します。
- [2:1] : 2:1 VLAN 変換。内部および外部の両方の VLAN を単一の VLAN に変換します。
- [1:2] : 1 対 2 VLAN 変換。もう 1 つのプロバイダー VLAN をプッシュします。
- [2:2] : 2 対 2 VLAN 変換。内部および外部の両方の VLAN を別の 2 つの VLAN に変換します。

（注）　EVC イーサネット サービスで VLAN がどのようにサポートされるかについては、「EVC イーサネット サービス要求の管理」（P.3-36）の VLAN 変換属性の対象範囲を参照してください。

ステップ 9　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR デバイスで pw-class コマンドをプロビジョニングするために使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。

ステップ 10　[L2VPN Group Name] では、ドロップダウン リストから次のいずれかを選択します。

- ISC
- VPNSC

使用方法に関する注釈：

- この属性は、IOS XR デバイスで L2VPN グループ名をプロビジョニングするために使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

- [L2VPN Group Name] 属性は、[Service Options] ウィンドウで [MPLS core connectivity type] が [VPLS] に設定されていた場合は使用不可です（「サービス オプションの設定」（P.3-22）を参照）。
- [L2VPN Group Name] は、IOS XR デバイスだけに適用されます。

ステップ 11　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

使用方法に関する注釈：

- ポリシーまたはポリシーに基づくサービス要求のいずれかの [E-Line Name] に何も値が指定されていない場合、Prime Provisioning は次のようにデフォルト名を自動生成します。
  - [PSEUDOWIRE] コア接続タイプの場合は、次の形式になります。

    DeviceName--VC_ID
  - [LOCAL] コア接続タイプの場合は、次の形式になります。

    DeviceName--0--VLAN_ID

  デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。
- [E-Line Name] 属性は、[Service Options] ウィンドウで [MPLS core connectivity type] が [VPLS] に設定されていた場合は使用不可です（「サービス オプションの設定」（P.3-22）を参照）。

- [E-Line Name] は、IOS XR デバイスだけに適用されます。

ステップ 12　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 13　Prime Provisioning に SVI（スイッチ仮想インターフェイス）でフォワーディング コマンドを生成させるには、[N-PE Pseudo-wire on SVI] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフになっています。この場合、Prime Provisioning は、サービス インスタンスでフォワーディング コマンドを生成します。

EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（これは、[EVC Policy Editor - Service Options] ウィンドウのポリシー ワークフローで使用可能です）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

使用方法に関する注釈：

- Prime Provisioning では、EVC サービス要求のハイブリッド設定がサポートされます。ハイブリッド設定では、接続回線のいずれかの側のフォワーディング コマンド（xconnect など）は、サービス インスタンスで設定でき、接続回線のもう一方の側の xconnect 設定は、スイッチ仮想インターフェイス（SVI）で設定できます。
- これらのケースの例については、コンフィグレットの例 「EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）」（P.3-222）と「EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）」（P.3-223）を参照してください。
- [N-PE Pseudo-wire on SVI] は、すべての接続タイプ（[PSEUDOWIRE]、[VPLS]、または [LOCAL]）に適用できますが、ハイブリッド SVI 設定は疑似回線接続だけで可能です。
- [MPLS Core Connectivity Type] が [VPLS] に設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にイネーブルにされます。
- [MPLS Core Connectivity Type] が [LOCAL] 接続タイプに設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にディセーブルにされます。
- [N-PE Pseudo-wire on SVI] 属性は、IOS XR デバイスではサポートされません。サブインターフェイスだけが ASR 9000 デバイスでサポートされます。サービス インスタンスはサポートされません。すべての xconnect コマンドは、L2 サブインターフェイスで設定されます。
- 表 3-3 では、EVC サービス要求のハイブリッド設定のさまざまな使用例を示します。

表 3-3　EVC サービス要求のハイブリッド設定の使用例

ブリッジ ドメインの使用	EVC	SVI 上の N-PE 疑似回線	生成される CLI
True	True	True	• VLAN インターフェイスの xconnect。 • メイン インターフェイスのサービス インスタンス。
True	True	False	• サービス インスタンスの xconnect。 • メイン インターフェイスのサービス インスタンス。
False	True	N/A	• サービス インスタンスの xconnect。 • メイン インターフェイスのサービス インスタンス。
True	False	True	VLAN インターフェイスの xconnect。
True	False	False	サブインターフェイスの xconnect。
False	False	False	サブインターフェイスの xconnect。

ステップ 14　独自の名前付きアクセス リストをポートに割り当てる場合は、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 15　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 16　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 17　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。

- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 18 UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 19 コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

選択したプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Enable cdp] : Cisco Discover Protocol（CDP）でレイヤ 2 トンネリングをイネーブルにします。

b. [cdp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

c. [cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Enable vtp] : VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）でレイヤ 2 トンネリングをイネーブルにします。

e. [vtp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Enable stp] : スパニングツリー プロトコル（STP）でレイヤ 2 トンネリングをイネーブルにします。

h. [stp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 20 [MTU Size] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。デフォルトのサイズは 9216 で、範囲は 1500 ～ 9216 です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。

Cisco Prime Fulfillment 1.0 では、プラットフォームごとに異なる範囲がサポートされます。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- Cisco 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードでは、MTU サイズとして 9216 だけが使用され、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Prime Provisioning は両方のケースで 9216 を使用します。
- Cisco 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21 この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場合は、[Next] ボタンをクリックします。

この機能の詳細については、「テンプレートの関連付けのイネーブル化」（P.3-36）を参照してください。

（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。

ステップ 22　EVC ポリシーを保存するには、[Finish] をクリックします。

EVC ポリシーに基づいてサービス要求を作成するには、「EVC イーサネット サービス要求の管理」（P.3-36）を参照してください。

テンプレートの関連付けのイネーブル化

Prime Provisioning テンプレート機能を使用すると、デバイスにフリーフォーマット CLI をダウンロードできます。テンプレートをイネーブルにする場合は、Prime Provisioning で現在サポートされていないコマンドをダウンロードするために、テンプレートとデータ ファイルを作成できます。

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、（[Finish] をクリックする前に）[Interface Attribute] ウィンドウで [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、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、「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 2　ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

ステップ 3　EVC ポリシーを保存するには、[Finish] をクリックします。

EVC ポリシーに基づいてサービス要求を作成するには、「EVC イーサネット サービス要求の管理」（P.3-36）を参照してください。

EVC イーサネット サービス要求の管理

この項では、EVC イーサネット サービス要求のプロビジョニング方法について説明します。具体的な内容は、次のとおりです。

- 「EVC イーサネット 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」（P.3-57）
- 「EVC サービス要求の保存」（P.3-58）

EVC サービス要求の概要

EVC イーサネット サービス要求では、「EVC イーサネット ポリシーの作成」（P.3-20）で説明した EVC 機能をサポートするために、N-PE でインターフェイスを設定することができます。EVC サービス要求を作成するには、EVC 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。定義済みの EVC ポリシーに基づいて、オペレータは EVC サービス要求を作成してサービスを展開します。サービス要求の一部として、1 つ以上のテンプレートを N-PE に関連付けることもできます。

EVC イーサネット サービス要求の作成では、次を行う必要があります。

- 既存の EVC イーサネット ポリシーを選択します。
- VPN を選択します。

（注）　EVC イーサネット ポリシーとサービス要求のコンテキストで VPN オブジェクトを操作する場合は、VPN 名とカスタマー属性だけが関係します。MPLS と VPLS に関連するその他の VPN 属性は無視されます。

- ブリッジ ドメイン コンフィギュレーションを指定します（該当する場合）。
- サービス要求の説明を指定します。
- VC ID または VPLS VPN ID の自動または手動の割り当てを指定します。
- 直接接続リンクを追加します（該当する場合）。
- L2 アクセス ノードとのリンクを追加します（該当する場合）。
- リンクの N-PE と UNI インターフェイスを選択します。
- L2 アクセス ノードとのリンクでは、N-PE または UNI インターフェイスに複数の NPC が存在する場合は、Named Physical Circuit（NPC; 名前付き物理回線）を選択します。
- リンク属性を編集します。
- サービス要求を変更します。
- サービス要求を保存します。

EVC イーサネット シナリオのサンプル 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.3-186）を参照してください。

EVC サービス要求の作成

EVC イーサネット 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 Request Manager] を選択します。

[Service Request Manager] 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。

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

ステップ 3　ポリシー選択機能を使用して、以前に作成したポリシーから EVC ポリシーを選択します（「EVC イーサネット ポリシーの作成」（P.3-20）を参照）。

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

新しいサービス要求は、すべての編集可能な機能と編集不可能な機能および事前設定されたパラメータなど、選択した EVC ポリシーのプロパティをすべて継承します。

ステップ 4　次の項である「サービス要求の詳細の設定」（P.3-38）に記載されているステップに進みます。

サービス要求の詳細の設定

サービス要求の基礎として使用する EVC イーサネット ポリシーを選択した後で、[EVC Service Request Editor] ウィンドウが表示されます。これは次の 3 つのセクションに分かれています。

- Link Page
- [Direct Connect Links]（NPC なし）
- [Links with L2 Access Nodes]（NPC を使用）

このウィンドウでは、サービス要求のオプションを指定して、直接接続リンクと L2 アクセス ノードとのリンクを設定できます。ウィンドウの最初のセクションに表示されるオプションは、ポリシーで指定された [MPLS Core Connectivity Type]（疑似回線、VPLS、またはローカル）によって変わります。明確にするために、これらの各シナリオは下記では別個のセクションに示されており、さまざまなウィンドウ設定と表示されるオプションの動作が強調されています。

ポリシーの [MPLS Core Connectivity Type] で決定された、該当する項に進みます。

- 「疑似回線コア接続」（P.3-38）
- 「VPLS コア接続」（P.3-40）
- 「ローカル コア接続」（P.3-42）

直接接続リンクと L2 アクセス ノードとのリンクを設定するための指示は、後の項に示されています。

疑似回線コア接続

この項では、EVC イーサネット ポリシーの [MPLS Core Connectivity Type] が [PSEUDOWIRE] であるケースについて説明します。

[Link Page] ウィンドウの最初のセクションで属性を設定します。次の手順を実行します。

（注）　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

（注）　[Policy] フィールドは読み取り専用です。サービス要求の元になっているポリシーの名前が表示されます。読み取り専用のポリシー名をクリックすると、ポリシー内で設定されているすべての属性値のリストが表示されます。

ステップ 1　このサービス要求で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

（注）　コア タイプが LOCAL および PSEUDOWIRE のサービス要求では同じ VPN を使用できます。サービス要求の VPN が VPLS コア タイプで使用される場合は、コア タイプが LOCAL または PSEUDOWIRE のサービス要求には同じ VPN を使用できません。

ステップ 2　[Select] 列で **VPN 名**を選択します。

ステップ 3　[Select] をクリックします。

VPN 名が示された [EVC Service Request Editor] ウィンドウが表示されます。

ステップ 4　Prime Provisioning に VC ID を選択させる場合は、[AutoPick VC ID] 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しない場合は、次のステップで説明されているように、[VC ID] フィールドで ID を指定するよう求めるプロンプトが表示されます。

[AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。この場合は、[VC ID] オプションのテキスト フィールドは編集不可能です。

ステップ 5　[AutoPick VC ID] をオフにした場合は、[VC ID] フィールドに VC ID を入力します。

使用方法に関する注釈：

- [VC ID] 値は、VC ID に対応する整数値でなければなりません。
- VC ID を手動で割り当てると、Prime Provisioning は VC ID を調べて、Prime Provisioning の VC ID プール内にそれがあるかどうかを確認します。VC ID がプール内にあっても割り当てられていない場合は、VC ID はサービス要求に割り当てられます。VC ID がプール内にあって、すでに使用中の場合は、Prime Provisioning は別の VC ID を割り当てるよう求めるプロンプトを表示します。VC ID が Prime Provisioning VC ID プールの外にある場合は、Prime Provisioning は、VC ID が割り当てられているかどうかに関する検査を実行しません。オペレータは、VC ID が使用可能であることを確認する必要があります。
- VC ID は、サービスの作成中に限り入力できます。サービス要求の編集中は、[VC ID] フィールドは編集不可能です。

ステップ 6　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[Enable PseudoWire Redundancy] 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方法に関する注釈については、付録 C「2 台の N-PE 上でのアクセス リングの終端」、および特に「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）を参照してください。

ステップ 7　[AutoPick VC ID] 属性をオフにした場合は、[Backup PW VC ID] フィールドにバックアップ疑似回線の VC ID を入力します。

上のステップ 7 で [AutoPick VC ID] 属性の使用方法に関する注釈を参照してください。バックアップ VC ID の動作は、プライマリ疑似回線の VC ID の動作と同じです。

ステップ 8　ブリッジ ドメインの特性を判別するには、[Configure Bridge Domain] チェックボックスをオンにします。

[Configure Bridge Domain] オプションの動作は、EVC ポリシーの [MPLS Core Connectivity Type] オプションで選択した項目（この場合は、疑似回線コア接続）と並行して動作します。次の 2 つのケースがあります。

- EVC の場合
  - [Configure With Bridge Domain] をオンにすると、ポリシーは、ブリッジ ドメインに関連付けられた SVI の下で疑似回線を設定します。

- [Configure With Bridge Domain] をオフにすると、ポリシーは、サービス インスタンス下で直接疑似回線を設定します。これによって、グローバル VLAN が保存されます。

- EVC を使用しない場合
  - [Configure With Bridge Domain] をオンにすると、ポリシーは、SVI の下で疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サブインターフェイスで直接疑似回線を設定します。

  疑似回線を、対応する EVC 対応インターフェイスのサービス インスタンス下、またはブリッジ ドメインに関連付けられた SVI の下のいずれかで直接設定できます。

ステップ 9　ブリッジ ドメインとのスプリット ホライズンをイネーブルにするには、[Use Split Horizon] 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：

- [Use Split Horizon] 属性はデフォルトでディセーブルになっています。
- [Use Split Horizon] 属性は、[Configure Bridge Domain] チェックボックスがオン（イネーブル）になっている場合にだけ使用できます。
- [Use Split Horizon] がイネーブルになっている場合は、スプリット ホライズンとともに CLI で **bridge domain** コマンドが生成されます。ディセーブルにすると、スプリット ホライズンなしで **bridge domain** コマンドが生成されます。

ステップ 10　サービス要求の説明ラベルを入力するには、[Description] 属性の [Click here] リンクをクリックします。

これは、Prime Provisioning データベースで特定のサービス要求を検索するのに役立ちます。

説明を入力できるダイアログが表示されます。

ステップ 11　ダイレクト接続リンクを設定するには、「直接接続リンクの設定」（P.3-44）の項を参照してください。

ステップ 12　L2 アクセス ノードとのリンクを設定するには、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）の項を参照してください。

VPLS コア接続

この項では、EVC イーサネット ポリシーの [MPLS Core Connectivity Type] が [VPLS] であるケースについて説明します。

[Link Page] ウィンドウの最初のセクションで属性を設定するには、次の手順を実行します。

ステップ 1　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。

初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

ステップ 2　[Policy] フィールドは読み取り専用です。サービス要求の元になっているポリシーの名前が表示されます。

ステップ 3　このサービス要求で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

（注）　コア タイプが LOCAL および PSEUDOWIRE のサービス要求では同じ VPN を使用できます。サービス要求の VPN が VPLS コア タイプで使用される場合は、コア タイプが LOCAL または PSEUDOWIRE のサービス要求には同じ VPN を使用できません。

（注）　複数のサービス要求で同じ VPN を使用して、すべてに VPLS コア タイプを指定する場合は、これらすべてのサービス要求が同じ VPLS サービスに参加します。

ステップ 4　[Select] 列で **VPN 名**を選択します。

ステップ 5　[Select] をクリックします。

VPN 名が示された [EVC Service Request Editor] ウィンドウが表示されます。

ステップ 6　Prime Provisioning に VPLS VPN ID を選択させる場合、[AutoPick VPLS VPN ID] 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しない場合は、次のステップで説明されているように、[VPLS VPN ID] フィールドで VPN ID を指定するよう求めるプロンプトが表示されます。

- [AutoPick VPLS VPN ID] をオンにすると、Prime Provisioning は Prime Provisioning 管理 VC ID リソース プールから VPLS VPN ID を割り当てます。この場合は、[VPLS VPN ID] オプションのテキスト フィールドは編集不可能です。
- [AutoPick VPLS VPN ID] をオンにした場合に、同じ VPN オブジェクトを参照するサービス要求がすでに存在するときは、既存のサービス要求の VPLS VPN ID が新しいサービス要求に割り当てられます。

ステップ 7　[AutoPick VPLS VPN ID] をオフにした場合は、[VPLS VPN ID] フィールドに VPLS VPN ID を入力します。

使用方法に関する注釈：

- [VPLS VPN ID] 値は、VPN ID に対応する整数値でなければなりません。
- [VPLS VPN ID] を手動割り当てする場合、Prime Provisioning は [VPLS VPN ID] が Prime Provisioning の VC ID プール内の値かどうかを確認します。VPLS VPN ID がプール内にあっても、割り当てられていない場合は、VPLS VPN ID がサービス要求に割り当てられます。VPLS VPN ID がプール内にあり、すでに使用されている場合は、Prime Provisioning は、別の VPLS VPN ID を割り当てるよう求めるプロンプトを表示します。[VPLS VPN ID] が VC ID プールの外にある場合、Prime Provisioning はその [VPLS VPN ID] が割り当てられているかについての確認を行いません。オペレータは、VPLS VPN ID が使用可能であることを確認する必要があります。
- VPLS VPN ID は、サービスの作成中に限り入力できます。サービス要求の編集中は、[VPLS VPN ID] フィールドは編集不可能です。

ステップ 8　Prime Provisioning で仮想転送インスタンス（VFI）名を選択する場合は、[AutoPick VFI Name] 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しない場合は、次の手順で説明されているように、[VFI Name] フィールドで VFI 名を指定できます。

使用方法に関する注釈：

- [AutoPick VFI name] をオンにすると、Prime Provisioning は次の形式で VFI 名を生成します。

  VPN name-VC ID

- この属性は、既存のサービスを Prime Provisioning にインポートし、このために作成されたサービス要求にそれをマッピングする場合に便利です。手動でサービス要求に VFI 名を指定すると、VFI 名を既存のサービス名と一致させることができます。

ステップ 9　[AutoPick VFI Name] をオフにした場合、[VFI Name] フィールドに VFI 名を入力します。

ステップ 10　VPLS 自動検出に、[Discovery Mode] タイプを選択します。

選択できる基準は、次のとおりです。

- [Manual]：サービス要求によって設定された VPLS PE デバイスで、VPLS 自動検出をプロビジョニングしません。この場合、VPLS ドメインに対して新しい PE デバイスを追加または削除すると、VPLS ドメインの各ネイバーに対して手動設定が必要になります。
- [Auto Discovery]：サービス要求によって設定された VPLS PE デバイスで、VPLS 自動検出をプロビジョニングします。VPLS 自動検出をイネーブルにすると、VPLS ドメインに対して PE が追加または削除されたときに、ネイバー デバイスが自動的に検出します。

Prime Provisioning でのこの機能のサポート内容、デバイスの事前設定要件、および制限の詳細については、「EVC サービス要求を使用したデバイス上での VPLS 自動検出のプロビジョニング」（P.3-177）を参照してください。

ステップ 11　LSP/疑似回線ラベルの静的割り当てをイネーブルにするには、[Static VPLS] チェックボックスをオンにします。

ステップ 12　[Configure Bridge Domain] チェックボックスはデフォルトでオンになっており、変更できません。

使用方法に関する注釈：

- VPLS では、すべての設定が SVI 下にあります。
- EVC 機能を使用する場合は、すべての設定は SVI 下にあり、ブリッジ ドメインにも関連付けられます。

ステップ 13　サービス要求の説明ラベルを入力するには、[Description] 属性の [Click here] リンクをクリックします。

説明を入力できるダイアログが表示されます。

ステップ 14　ダイレクト接続リンクを設定するには、「直接接続リンクの設定」（P.3-44）の項を参照してください。

ステップ 15　L2 アクセス ノードとのリンクを設定するには、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）の項を参照してください。

ローカル コア接続

この項では、EVC イーサネット ポリシーの [MPLS Core Connectivity Type] が [LOCAL] であるケースについて説明します。

[Link Page] ウィンドウの最初のセクションで属性を設定するには、次の手順を実行します。

ステップ 1　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。

初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

ステップ 2　[Policy] フィールドは読み取り専用です。

サービス要求の元になっているポリシーの名前が表示されます。

ステップ 3　このサービス要求で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

（注）　コア タイプが LOCAL および PSEUDOWIRE のサービス要求では同じ VPN を使用できます。サービス要求の VPN が VPLS コア タイプで使用される場合は、コア タイプが LOCAL または PSEUDOWIRE のサービス要求には同じ VPN を使用できません。

ステップ 4　[Select] 列で **VPN 名**を選択します。

ステップ 5　[Select] をクリックします。

VPN 名が示された [EVC Service Request Editor] ウィンドウが表示されます。

ステップ 6　ブリッジ ドメインの特性を判別するには、[Configure Bridge Domain] 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：

- [Configure Bridge Domain] がオンの場合は、すべてのリンクに、N-PE 上の VLAN プールから同じブリッジ ドメイン ID が割り当てられます。すべての非 EVC リンクには、ブリッジ ドメイン ID としてサービス プロバイダー VLAN が割り当てられます。その一方で、EVC リンクが追加されない場合は、サービス プロバイダー VLAN が最初に割り当てられ、これは、EVC リンクが追加されたときにブリッジ ドメイン ID として使用されます。
- [Configure Bridge Domain] をオフにすると、同じ N-PE で終端するリンクを最大 2 つ追加できます （これは、EVC インフラストラクチャで使用可能な **connect** コマンドを使用します）。

  （注）　Prime Provisioning が接続名を自動生成する方法に関する詳細については、次の補足説明を参照してください。

  デバイスでは、接続名には最大で 15 文字だけが受け入れられるため、接続名は次の形式を使用して生成されます。

  CustomerNameTruncatedToMaxPossibleCharacters_ServiceRequestJobID

  たとえば、カスタマー名が NorthAmericanCustomer で、サービス要求ジョブ ID が 56345 の場合は、自動生成される接続名は NorthAmer_56345 になります。

  生成される CLI は次のとおりです。

  ```
  connect NorthAmer_56345 GigabitEthernet7/0/5 11 GigabitEthernet7/0/4 18
  ```

  この場合は、11 と 18 がサービス インスタンス ID です。
- [Configure Bridge Domain] のポリシー設定が編集不可能な場合は、サービス要求のオプションは読み取り専用です。

ステップ 7　ブリッジ ドメインとのスプリット ホライズンをイネーブルにするには、[Use Split Horizon] 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：

- [Use Split Horizon] 属性はデフォルトでディセーブルになっています。
- [Use Split Horizon] 属性は、[Configure Bridge Domain] チェックボックスがオン（イネーブル）になっている場合にだけ使用できます。
- [Use Split Horizon] がイネーブルになっている場合は、スプリット ホライズンとともに CLI で **bridge domain** コマンドが生成されます。ディセーブルにすると、スプリット ホライズンなしで **bridge domain** コマンドが生成されます。

ステップ 8　サービス要求の説明ラベルを入力するには、[Description] 属性の [Click here] リンクをクリックします。

説明を入力できるダイアログが表示されます。

ステップ 9　ダイレクト接続リンクを設定するには、「直接接続リンクの設定」（P.3-44）の項を参照してください。

ステップ 10　L2 アクセス ノードとのリンクを設定するには、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）の項を参照してください。

N-PE へのリンクの設定

[EVC Service Request Editor] ウィンドウの下部 2 つのセクションでは、N-PE へのリンクを設定できます。直接接続リンクの場合は、CE は、中間 L2 アクセス ノードなしで N-PE に直接接続されます。L2 アクセス ノードとのリンクの場合は、Prime Provisioning で作成する NPC を必要とする CE と NPE の間に中間デバイスが存在します。

ウィンドウの [Direct Connect Links] セクションは、N-PE に直接接続するリンクを設定する場所です。NPC は使用されません。[Links with L2 Access Nodes] セクションは、L2（イーサネット）アクセス ノードとのリンクを設定する場所です。NPC が使用されます。

設定するリンクのタイプに応じて、適切な項を参照してください。

- 「直接接続リンクの設定」（P.3-44）
- 「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）
- 「VPLS ネイバー リンクの設定（VPLS のみ）」（P.3-56）

（注）　2 つのリンク タイプを設定するための手順の多くは同じです。リンクを設定するための基本的なワークフロー、および設定する属性は、「直接接続リンクの設定」（P.3-44）に記載されています。L2 アクセス ノードとのリンクを設定する場合でも、この項に記載されている情報を参照すると役に立ちます。L2 アクセス ノードの項では、そのようなリンクに固有のステップだけが記載されているためです。

直接接続リンクの設定

直接接続リンクを設定するには、次の手順を実行します。これらのステップの多くは、L2 アクセス ノードとのリンクにも適用されます。

ステップ 1　[Add] をクリックして、リンクを追加します。

リンク属性の新たに番号付けされた行が表示されます。

ステップ 2　[N-PE] 列の [Select NPE] をクリックします。

[Select PE Device] ウィンドウが表示されます。このウィンドウには、現在定義されている PE のリストが表示されます。

a.　[Show PEs with] ドロップダウン リストには、[PEs by Provider]、[PE Region Name]、または [by Device Name] が表示されます。

b.　[Find] ボタンを使用すると、特定の PE を検索するか、ウィンドウを更新できます。

c.　[Rows per page] ドロップダウン リストでは、ユーザは画面に一度に表示される項目の数を設定できます。

ステップ 3　[Select] 列で、リンクの PE デバイス名を選択します。

ステップ 4　[Select] をクリックします。

選択した PE の名前が [N-PE] 列に示された [EVC Service Request Editor] ウィンドウが再表示されます。

ステップ 5　[UNI] 列のインターフェイス選択機能から UNI インターフェイスを選択します。

（注） Prime Provisioning には、基盤となるインターフェイスの設定、インターフェイスを使用する可能性がある既存のサービス要求、サービス要求に関連付けられたカスタマーに基づいて、サービスに使用可能なインターフェイスだけが表示されます。[Detail] ボタンをクリックして、インターフェイス名、カスタマー名、VPN 名、ジョブ ID、サービス要求 ID、サービス要求タイプ、変換タイプ、および VLAN ID 情報など、使用可能なインターフェイスに関する情報が示されたポップアップ ウィンドウを表示できます。

（注） IOS XR が実行されている N-PE デバイスで UNI を設定する場合は、[Standard UNI Port] 属性はサポートされません。この場合、[Standard UNI Port] と [UNI Port Security] に関連する CLI はすべて無視されます。

ステップ 6　[EVC] チェックボックスをオンにして、リンクの設定サービス インスタンスのリンクをマークします。

（注） ここで [EVC] チェックボックスについて述べるのは、このチェックボックスの設定によって [Link Attributes] 列内で使用できるリンク編集機能の動作が変わるからです。これは次のステップで説明します。

（注） [EVC] チェックボックスは、デフォルトでオフになっています。このチェックボックスのデフォルト値は、DCPL プロパティ Pr ovisioning\ProvDrv\CheckFlexUniCheckBox の値を設定することによって変更できます。

[Link Attributes] の編集

次のステップでは、[Link Attributes] 列の [Edit] リンクの使用について説明します（リンク属性がすでに設定されている場合は、このリンクが [Edit] から [Change] に変わります）。リンク編集ワークフローは、そのリンクの [EVC] チェックボックスの状態によって変化します。[EVC] チェックボックスがオンの場合、編集ワークフローには、2 セットのリンク属性について、2 つのウィンドウで行う属性設定が含まれます。

- EVC Details
- Standard UNI Details

リンクの [EVC] チェックボックスがオフの場合、[Standard UNI Details] ウィンドウだけが表示されます。

次のステップでは、両方のシナリオについて説明します。

ステップ 7　[UNI] 属性を指定するには、[Link Attributes] 列で [Edit] をクリックします。

[EVC Details] ウィンドウ

[EVC] チェックボックスをオンにすると、[EVC Details] ウィンドウが表示されます。

[EVC Details] 画面のフィールドはすべて、ポリシー設定に基づいてイネーブルになります。たとえば、[Both Tags] がポリシーで選択され、編集可能である場合は、このウィンドウで [Match Inner and Outer Tags] チェックボックスが選択され、編集可能になります。この動作は、[EVC Details] ウィンドウ内の他の属性についても類似しています。

ステップ 8　サービス要求の作成中にサービス インスタンス ID を自動生成し、リンクに割り当てることを指定するには、[AutoPick Service Instance ID] チェックボックスをオンにします。

チェックボックスをオフにする場合は、サービス インスタンス ID を指定する必要があります（次のステップを参照）。

使用方法に関する注釈：

- サービス インスタンス ID は、EVC インフラストラクチャ内のインターフェイス上の Ethernet Flow Point（EFP; イーサネット フロー ポイント）を表します。サービス インスタンス ID は、インターフェイスに対してローカルで有効です。この ID は、インターフェイス レベルだけで固有でなければなりません。ID は 1 ～ 8000 までの値でなければなりません。
- Prime Provisioning では、サービス インスタンス ID の割り当て元として使用可能なリソース プールはありません。
- サービス インスタンス ID を手動で指定する場合は、オペレータが、インターフェイス レベルで ID の一意性を維持する必要があります。
- この属性は IOS XR デバイスでは表示されません。

ステップ 9　[AutoPick Service Instance ID] チェックボックスをオンにしない場合は、[Service Instance ID] フィールドにサービス インスタンス ID に適した値を入力します。

この属性は IOS XR デバイスでは表示されません。

ステップ 10　サービス インスタンス名を自動生成することを指定するには、[AutoPick Service Instance Name] チェックボックスをオンにします。

チェックボックスをオフにすると、サービス インスタンス名を指定できます（次のステップを参照）。

使用方法に関する注釈：

- チェックボックスをオンにすると、[Service Instance Name] テキスト フィールドはディセーブルになります。
- サービス インスタンス名は、*CustomerName_ServiceRequestJobID* というパターンで自動生成されます。
- コングレットの例については、「EVC（AutoPick Service Instance Name）」（P.3-224）、「EVC（ユーザ指定のサービス インスタンス名、疑似回線コア接続）」（P.3-226）、および「EVC（ユーザ指定のサービス インスタンス名、ローカル コア接続）」（P.3-227）を参照してください。
- この属性は IOS XR デバイスでは表示されません。

ステップ 11　[AutoPick Service Instance Name] チェックボックスをオンにしない場合は、[Service Instance Name] フィールドにサービス インスタンス ID に適した値を入力します。

使用方法に関する注釈：

- サービス インスタンス名を表すテキスト ストリングは、40 文字以下で、スペースは使用できません。他の特殊文字は使用できます。
- [AutoPick Service Instance Name] がオフで、テキスト フィールドにサービス インスタンス名が入力されていない場合、Prime Provisioning はサービス要求によって生成されるデバイスの設定中にグローバルな **ethernet evc evcname** コマンドを生成しません。

ステップ 12　サービス要求の作成中に Prime Provisioning にサービス要求の VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにする場合は、ブリッジ ドメイン VLAN ID を指定する必要があります（次のステップを参照）。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。

- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 13　[AutoPick Bridge Domain/VLAN ID] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID] フィールドに適切な値を入力します。

（注）　この設定は、[EVC Service Request Editor] ウィンドウの [Configure Bridge Domain] オプションとともに適用されます。このウィンドウでオプションをイネーブルにしない場合は、[AutoPick Bridge Domain/VLAN ID] チェックボックスは冗長であり、必要ありません。

VLAN ID を手動で割り当てる場合は、Prime Provisioning は、Prime Provisioning の VLAN ID プール内にあるかどうかを確認するために VLAN ID を調べます。VLAN ID がプール内にあっても、割り当てられていない場合は、VLAN ID がサービス要求に割り当てられます。VLAN ID がプール内にあり、すでに使用されている場合、Prime Provisioning は、別の VLAN ID を割り当てるよう求めるプロンプトを表示します。VLAN ID が Prime Provisioning VLAN ID プールの外にある場合は、Prime Provisioning は、VLAN ID が割り当てられているかどうかの確認を実行しません。オペレータは、VLAN ID が使用可能であることを確認する必要があります。

ステップ 14　サービス要求の作成中に、デュアルホーム接続リングのセカンダリ N-PE に対してブリッジ ドメインの VLAN ID を自動選択するように Prime Provisioning を設定するには、[AutoPick Bridge Domain/VLAN ID Secondary N-PE] 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フにする場合は、セカンダリ N-PE のセカンダリ ブリッジ ドメイン VLAN ID を指定する必要があります（次の手順を参照）。

使用方法に関する注釈：

- この属性は、デュアル ホーム接続リング（2 つの異なる N-PE で終端するリング）の場合にのみ適用できます。Prime Provisioning では、セカンダリ N-PE 用に別個のブリッジ ドメイン VLAN ID を使用することがサポートされます。
- デュアル ホーム接続リングでは、2 つの N-PE が異なるアクセス ドメインに存在する場合、Prime Provisioning はプライマリとセカンダリの両方の N-PE アクセス ドメインからブリッジ ドメイン VLAN ID を割り当てます。両方が同一のアクセス ドメイン内にある場合、Prime Provisioning は共通の VLAN ID をこれらが属するアクセス ドメインから割り当てます。
- AutoPick ブリッジ ドメイン/VLAN ID セカンダリ N-PE は、デバイスでグローバル VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。
- この属性は IOS XR デバイスでは表示されません。

ステップ 15　[AutoPick Bridge Domain/VLAN ID Secondary N-PE] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID Secondary N-PE] フィールドに適切な値を入力します。

ステップ 16　サービス インスタンスの詳細を設定します。
次の図に示すように [Match] ドロップダウン リストからカプセル化タイプを選択します。
選択できる基準は、次のとおりです。

- DOT1Q
- Default

一致基準として [Default] を選択すると、ページ内の [Outer VLAN ID] と [Outer VLAN Ranges] フィールドがディセーブルになります。[Default] が CE カプセル化タイプである場合、Prime Provisioning には、UNI ポート タイプに別のフィールドが表示されます。

ステップ 17　ポリシーを使用して作成されたサービス要求を、着信フレームの内部 VLAN タグと外部 VLAN タグの両方と一致させるには、[Match Inner and Outer Tags] 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しないと、ポリシーを使用して作成されたサービス要求は、着信フレームの外部 VLAN タグだけと一致します。

[Match Inner and Outer Tags] 属性をオンにすると、[Inner VLAN ID] フィールドと [Outer VLAN ID] フィールド（次のステップで説明）が表示されます。

ステップ 18　[Match Inner and Outer Tags] チェックボックスをオンにする場合は、[Inner VLAN ID] フィールドと [Outer VLAN ID] フィールドに内部 VLAN タグと外部 VLAN タグを入力します。

使用方法に関する注釈：

- 単一の値、単一の範囲、複数の値、複数の範囲、またはこれらの組み合わせを指定できます。次に、例を示します。
  - 10
  - 10, 15,17
  - 10-15
  - 10-15,17-20
  - 10,20-25
- ポリシーで [Inner VLAN Ranges] 属性を true に設定すると、[Inner VLAN ID] フィールドは、内部 VLAN タグの範囲を使用できます。
- ポリシーで [Outer VLAN Ranges] 属性を true に設定すると、[Outer VLAN ID] フィールドは、外部 VLAN タグの範囲を使用できるようになります。

ステップ 19　[Match Inner and Outer Tags] チェックボックスをオフにする場合は、[Outer VLAN ID] フィールドに外部 VLAN タグを入力します。

（注）　[Outer VLAN ID] で指定した VLAN は、カスタマー側の UNI を含め、残りの L2 アクセス ノード（リンクにある場合）でプロビジョニングされます。

（注）　また、次の手順で説明されているように、Prime Provisioning が外部 VLAN ID を自動選択するように設定することもできます。

ステップ 20　以前に作成した外部 VLAN ID リソース プールから外部 VLAN ID を Prime Provisioning が自動選択するように設定するには、[AutoPick Outer VLAN] 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フにすると、オペレータは外部 VLAN ID を指定するように求められます。

（注）　[AutoPick Outer VLAN] 属性を使用するには、2 つの要素が Prime Provisioning で事前に設定されている必要があります。1 つめの要素はインターフェイス アクセス ドメインであり、これは N-PE デバイスの物理ポートをグループ化する論理要素です。2 つめの要素は EVC 外部 VLAN リソース プールであり、これはインターフェイス アクセス ドメインによって使用されます。これらの要素を設定する方法については、項「リソースの設定」（P.2-42）と「リソース プール」（P.2-46）を参照してください。

使用方法に関する注釈：

- [AutoPick Outer VLAN] は、EVC 機能をサポートするインターフェイスに使用できます。
- [AutoPick Outer VLAN] は、EVC をサポートするインターフェイスで VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 21　ウィンドウの [VLAN Rewrite] セクションで、ドロップダウン リストから [Rewrite Type] を選択します。

選択できる基準は、次のとおりです。

- Pop
- Push
- Translate

GUI の後続の属性は、次のステップで説明するように、[Rewrite Type] の選択によって変わります。

ステップ 22　[Pop] が [Rewrite Type] である場合は、次の 2 つのチェックボックスが表示されます。

a. 一致基準を満たす着信フレームの外部 VLAN ID タグをポップするには、[Pop Outer Tag] 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フにすると、着信トラフィックの外部タグはポップされません。

b. 一致基準を満たす着信フレームの内部 VLAN ID タグをポップするには、[Pop Inner Tag] 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フにすると、内部タグは変更されません。

[Pop Inner Tag] をオンにすると、[Pop Outer Tag] が自動的にオンになることに注意してください。

ステップ 23　[Push] が [Rewrite Type] である場合は、次の 2 つのテキスト ボックスが表示されます。

a. テキスト ボックス [Outer VLAN ID] に、一致基準を満たす着信フレームにインポーズされる外部 VLAN ID タグを入力します。この設定で作成されるサービス要求はすべて、一致基準と一致する着信フレームで dot1q 外部タグをプッシュします。値が指定されていない場合は、プッシュ操作は無視され、デバイスで設定されません。

b. テキスト ボックス [Inner VLAN ID] に、一致基準を満たす着信フレームにインポーズされる内部 VLAN ID タグを入力します。この設定で作成されるサービス要求はすべて、一致基準と一致する着信フレームで dot1q 内部タグをプッシュします。内部 VLAN タグは、外部 VLAN タグなしではプッシュできません。つまり、内部 VLAN タグを適用する場合は、外部 VLAN タグも定義する必要があります。

ステップ 24　[Translate] が [Rewrite Type] である場合は、[Translation Type] ドロップダウン リストが表示されます。

このリストで選択可能な項目は、[Match Inner and Outer Tags] 属性の設定（前のステップで設定）によって異なります。

a. [Match Inner and Outer Tags] チェックボックスをオンにする（true）場合は、[Translation Type] ドロップダウン リストから変換タイプとして [1:1]、[1:2]、[2:1]、または [2:2] を選択します。

- [1:1] または [2:1] を選択する場合は、表示される [Outer VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。
- [1:2] または [2:2] を選択する場合は、表示される [Outer VLAN ID] および [Inner VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグと内部タグがこれらの ID に変換されます。

b. [Match Inner and Outer Tags] チェックボックスをオフにする（false）場合は、[Translation Type] ドロップダウン リストから変換タイプとして [1:1] または [1:2] を選択します。

- [1:1] を選択する場合は、表示される [Outer VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。
- [1:2] を選択する場合は、表示される [Outer VLAN ID] および [Inner VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグと内部タグがこれらの ID に変換されます。

ステップ 25　[Next] をクリックして、[EVC Details] ウィンドウの設定内容を保存します。

[Standard UNI Details] ウィンドウが表示されます。

ステップ 26　次のステップで、標準 UNI リンク属性の設定に進みます。

標準 UNI 属性の編集

次のステップでは、[Standard UNI Details] ウィンドウの属性の設定について説明します。EVC リンクとして設定されていないリンクの場合（[EVC Service Request Editor] ウィンドウで [EVC] チェックボックスをオンにしなかった場合）、リンク属性の編集はこのウィンドウから開始します。

（注）　[Standard UNI Details] ウィンドウに表示される属性は、Prime Provisioning によって動的に設定されます。下記のステップで説明する属性の一部は、ポリシーとサービス要求設定またはリンク タイプによっては、ウィンドウに表示されないことがあります。たとえば、EVC ポリシーの MPLS コア接続タイプが VPLS またはローカルの場合は、疑似回線関連の属性は表示されません。また、リンクを EVC または非 EVC として設定すると、ウィンドウに表示される属性が変わります。さらに、属性は、デバイス タイプ（IOS または IOS XR）に基づいてフィルタリングされます。これらのケースとその他のケースは、参照用としてステップに示されています。

ステップ 27　[N-PE/U-PE Information] フィールドと [Interface Name] フィールドには、前のステップで選択した PE デバイスとインターフェイス名が表示されます。

このフィールドは読み取り専用です。

ステップ 28　ドロップダウン リストから**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- [DOT1QTRUNK] : 802.1q カプセル化によって UNI をトランクとして設定します。UNI が直接接続された EVC リンクに属している場合、この設定は、着信フレームが 802.1q カプセル化され、リンクに設定された VLAN ID と一致することを意味します。この固有のトポロジには、トランク UNI 自体は含まれていません。
- [DOT1QTUNNEL] : UNI を 802.1q トンネル（dot1q トンネルまたは Q-in-Q とも呼ばれています）ポートとして設定します。
- [ACCESS] : UNI をアクセス ポートとして設定します。

この属性では、サービスの異なるリンクにさまざまなタイプの UNI カプセル化を導入できます。

使用方法に関する注釈：

- IOS とともに実行される U-PE を、（N-PE ロールで機能している）ASR 9000 で終端する同じ回線に追加すると、[Encapsulation] 属性のドロップダウン リストで 3 つすべてのカプセル化タイプ値が表示されます。
- [DOT1QTUNNEL] は、ASR 9000 デバイスを直接サポートしていません。
- EVC がイネーブルになっている直接接続リンクの場合（[EVC Service Request Editor] ウィンドウの [EVC] チェックボックスをオンにした場合）、カプセル化タイプとして選択できるのは、[DOT1Q] と [DEFAULT] です。

ステップ 29　必要に応じて、[PE/UNI Interface Description] フィールドにインターフェイスの説明を入力します。

ステップ 30　サービスのアクティブ化中（たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化する場合）に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。

ステップ 31　適切なオプション ボタンをクリックして、サービス要求の [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No] : VLAN 変換は実行されません （デフォルト）。
- [1:1] : 1:1 VLAN 変換。

- [2:1] : 2:1 VLAN 変換。
- [1:2] : 1 対 2 VLAN 変換。
- [2:2] : 2 対 2 VLAN 変換。

使用方法に関する注釈：

- 直接接続リンクの場合、[EVC] チェックボックスがオンになっているときは、[VLAN Translation] 属性は表示されません。これは次の組み合わせの場合は表示されます。
  - 直接接続リンクで、[EVC] チェックボックスがオフになっている場合。
  - L2 アクセス ノードで、[EVC] チェックボックスがオンまたはオフになっている場合。
- [No] 以外の選択肢を選ぶと、他のフィールドが GUI に表示されます。これらは、設定に基づいて指定できます。
  - [CE VLAN] : 1 ～ 4096 までの値を入力します。
  - [Auto Pick] : このチェックボックスをオンにすると、Prime Provisioning は VLAN リソース プールから外部 VLAN を自動選択するようになります。
  - [Outer VLAN] : [Auto Pick] がオフの場合、1 ～ 4096 までの値を指定します。
  - [Select where 2:1 or 2:2 translation takes place] : 2 対 1 または 2 対 2 の VLAN 変換が行われるデバイスを指定します。[Auto] を選択すると、UNI ポートに最も近いデバイスで VLAN 変換が行われます。
- VLAN 変換、すべての標準 UNI、およびポート セキュリティ属性は、L2 アクセスとのリンクに適用できます。UNI が N-PE にある場合は、これらの属性は表示されません。
- VLAN 変換が U-PE または PE-AGG デバイスで行われると、VLAN 変換のコマンドが選択したデバイスの NNI インターフェイスに設定されます。VLAN 変換が NP-E で行われると、VLAN 変換のコマンドがデバイスの UNI インターフェイスに設定されます。
- リング ベースの環境に 2 つの NNI インターフェイスがある場合、VLAN 変換は両方の NNI インターフェイスに適用されます。
- 1 対 1 および 2 対 1 の VLAN 変換は、非 EVC（スイッチポート ベースの N-PE の構文）終端の接続回線と同じ構文でサポートされます。

ステップ 32　Prime Provisioning に SVI（スイッチ仮想インターフェイス）でフォワーディング コマンドを生成させるには、[N-PE Pseudo-wire on SVI] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフになっています。この場合、Prime Provisioning は、サービス インスタンスでフォワーディング コマンドを生成します。

EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（これは、[EVC Service Request Editor] ウィンドウのサービス要求ワークフローで使用可能）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

使用方法に関する注釈：

- EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（[EVC Service Request Editor] ウィンドウ内）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

- Prime Provisioning では、EVC サービス要求のハイブリッド設定がサポートされます。ハイブリッド設定では、接続回線のいずれかの側のフォワーディング コマンド（xconnect など）は、サービス インスタンスで設定でき、接続回線のもう一方の側の xconnect 設定は、スイッチ仮想インターフェイス（SVI）で設定できます。
- [N-PE Pseudo-wire on SVI] は、すべての接続タイプ（[PSEUDOWIRE]、[VPLS]、または [LOCAL]）に適用できますが、ハイブリッド SVI 設定は疑似回線接続だけで可能です。
- [MPLS Core Connectivity Type] が [VPLS] に設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にイネーブルにされます。
- [MPLS Core Connectivity Type] が [LOCAL] 接続タイプに設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にディセーブルにされます。
- これらのケースの例については、コンフィグレットの例 「EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）」（P.3-222）と「EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）」（P.3-223）を参照してください。
- [N-PE Pseudo-wire on SVI] 属性の追加情報については、「インターフェイス属性の設定」（P.3-30）の項にある EVC ポリシーの章で対応するカバレッジを参照してください。
- [N-PE Pseudo-wire on SVI] 属性は、IOS XR デバイスではサポートされません。すべての xconnect コマンドは、L2 サブインターフェイスで設定されます。

ステップ 33　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] 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：

- [PW Tunnel Selection] チェックボックスをオンにすると、[Interface Tunnel] 属性フィールド（次のステップを参照）がアクティブになります。
- この属性は、EVC ポリシーで MPLS コア接続タイプが疑似回線として設定されている場合にのみ表示されます。
- [PW Tunnel Selection] 属性は、IOS XR デバイスではサポートされません。

ステップ 34　[PW Tunnel Selection] チェックボックスをオンにした場合は、[Interface Tunnel] テキスト フィールドに TE トンネル ID を入力します。

使用方法に関する注釈：

- Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。サービス要求の作成中に、Prime Provisioning はトンネル ID 番号の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。
- [Interface Tunnel] 属性は、IOS XR デバイスではサポートされません。

ステップ 35　サービス要求の作成中に、Prime Provisioning にブリッジ グループ名を自動選択させるには、[AutoPick Bridge Group Name] 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フにすると、サービス要求の作成中にブリッジ グループ名を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- この属性は、IOS XR デバイスだけで表示されます。
- [AutoPick Bridge Group Name] チェックボックスをオフにする場合は、[Bridge Group Name] テキスト フィールドにブリッジ グループ名を入力します。

- [AutoPick Bridge Group Name] 属性と [Bridge Group Name] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていた場合に限り表示されます。

ステップ 36　サービス要求の作成中に Prime Provisioning に VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにすると、サービス要求の作成中に VLAN ID を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。
- [AutoPick Bridge Domain/VLAN ID] 属性は、Cisco 7600 と ASR 9000 の両方のデバイスで表示されます。これは、非 EVC リンクについてのみ表示されます。

ステップ 37　[AutoPick Bridge Domain/VLAN ID] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID] テキスト フィールドに ID 番号を入力します。

使用方法に関する注釈：

- [AutoPick Bridge Domain/VLAN ID] をオンにすると、このフィールドは編集できません。
- VLAN ID を手動で割り当てる場合は、Prime Provisioning は、Prime Provisioning の VLAN ID プール内にあるかどうかを確認するために VLAN ID を調べます。VLAN ID がプール内にあっても、割り当てられていない場合は、VLAN ID がサービス要求に割り当てられます。VLAN ID がプール内にあり、すでに使用されている場合、Prime Provisioning は、別の VLAN ID を割り当てるよう求めるプロンプトを表示します。VLAN ID が Prime Provisioning VLAN ID プールの外にある場合は、Prime Provisioning は、VLAN ID が割り当てられているかどうかの確認を実行しません。オペレータは、VLAN ID が使用可能であることを確認する必要があります。
- [Bridge Domain/VLAN ID] テキスト フィールドは、Cisco 7600 と ASR 9000 の両方のデバイスで表示されます。これは、非 EVC リンクについてのみ表示されます。

ステップ 38　サービス要求の作成中に、Prime Provisioning にブリッジ ドメイン名を自動選択させるには、[AutoPick Bridge Domain Name] 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フにすると、サービス要求の作成中にブリッジ ドメイン名を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- [AutoPick Bridge Domain Name] 属性は、Cisco ASR 9000 デバイスだけで表示されます。
- [AutoPick Bridge Domain Name] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていた場合に限り表示されます。

ステップ 39　[AutoPick Bridge Domain Name] チェックボックスをオフにする場合は、[Bridge Domain Name] テキスト フィールドにブリッジ ドメイン名を入力します。

使用方法に関する注釈：

- [Bridge Domain Name] フィールドは、Cisco ASR 9000 デバイスだけで表示されます。
- [Bridge Domain Name] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていた場合に限り表示されます。

ステップ 40　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR デバイスで pw-class コマンドをプロビジョニングするために使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。
- [Use PseudoWireClass] 属性と [PseudoWireClass] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていなかった場合に限り表示されます。

ステップ 41　[L2VPN Group Name] では、ドロップダウン リストから次のいずれかを選択します。

- ISC
- VPNSC

使用方法に関する注釈：

- この属性は、IOS XR デバイスで L2VPN グループ名をプロビジョニングするために使用されます。

（注） ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

- [L2VPN Group Name] 属性は、[Service Options] ウィンドウで [MPLS core connectivity type] が [VPLS] に設定されていた場合は使用不可です（「サービス オプションの設定」（P.3-22）を参照）。
- [L2VPN Group Name] は、IOS XR デバイスだけに適用されます。
- [L2VPN Group Name] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていなかった場合に限り表示されます。

ステップ 42　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

使用方法に関する注釈：

- [E-Line Name] に値を指定しない場合は、Prime Provisioning は、次のようにデフォルト名を自動生成します。
  - [PSEUDOWIRE] コア接続タイプの場合は、次の形式になります。

    DeviceName--VC_ID
  - [LOCAL] コア接続タイプの場合は、次の形式になります。

    DeviceName--VLAN_ID

  デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。
- [E-Line Name] 属性は、[Service Options] ウィンドウで [MPLS core connectivity type] が [VPLS] に設定されていた場合は使用不可です（「サービス オプションの設定」（P.3-22）を参照）。
- [E-Line Name] は、IOS XR デバイスだけに適用されます。

- [E-Line Name] 属性は、サービス要求ワークフローの前半の [EVC Service Request Editor] ウィンドウで [Configure Bridge Domain] がイネーブルになっていなかった場合に限り表示されます。

ステップ 43　標準 UNI 設定を保存し、[EVC SR] ウィンドウに戻るには、[OK] をクリックします。

[Link Attributes] 列の値は、リンク設定が更新されたことを意味する [Changed] と表示されるようになります。[Changed] リンクをクリックして、[Standard UNI Details] ウィンドウの設定を変更することで、今後リンク属性を編集できるようになります。

リンク属性の編集に関する詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

ステップ 44　別のリンクを追加するには、[Add] ボタンをクリックして、この項の前のステップと同様に新しいリンクの属性を設定します。

ステップ 45　リンクを削除するには、そのリンクの行の最初の列でチェックボックスをオンにして、[Delete] ボタンをクリックします。

ステップ 46　このサービス要求の L2 アクセス ノードとのリンクを設定する場合は、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）を参照してください。

ステップ 47　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、EVC サービス要求を作成します。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）

[EVC Service Request Editor] ウィンドウの [Links with L2 Access Nodes] セクションでは、L2（イーサネット）アクセス ノードとのリンクを設定できます。これらは、（CE に向かった）N-PE 以外に L2/イーサネット アクセス ノードがある点を除き、直接接続リンクと類似しています。そのため、NPC が必要です。L2 アクセス ノードとのリンクを設定するためのステップは、「直接接続リンクの設定」（P.3-44）の項に記載されているステップと似ています。次の共通する操作の詳細なステップについては、この項を参照してください。

- リンクの追加と削除。
- N-PE の選択。
- UNI インターフェイスの選択。
- EVC リンクとしてのリンクの設定。
- 標準および EVC リンク属性の編集。

L2 アクセスとのリンクの設定における主な違いは、NPC の詳細の指定です。

L2 アクセス ノードとのリンクに NPC 詳細を設定するには、次の手順を実行します。

ステップ 1　NPC を使用してリンクを追加するプロセスの最初のステップは、N-PE ではなく U-PE/PE-AGG デバイスを選択することです。

選択したインターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Details] 列に自動入力される場合は、明示的に選択する必要はありません。

複数の NPC が使用可能な場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。[NPC] ウィンドウが表示され、適切な NPC を選択できます。

ステップ 2　[OK] をクリックします。

PE とインターフェイスを選択するたびに、この PE とインターフェイスから設定した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。[NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

ステップ 3　リンク属性の編集、リンクの追加と削除、[EVC] チェックボックスの使用については、「直接接続リンクの設定」（P.3-44）の項の対応する手順を参照してください。

ステップ 4　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、EVC サービス要求を作成します。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

VPLS ネイバー リンクの設定（VPLS のみ）

VPLS ポリシーを選択した場合、下部のウィンドウに VPLS ネイバーのリンクが表示されます。N-PE を直接接続リンクで複数選択すると、VPLS 対応ネイバーを検出できます。

マルチセグメント疑似回線トポロジで必要のないパスを選択するには、次の手順を実行します。

ステップ 1　VPLS ネイバー リンクで [Configure Pseudowire] リンクをクリックして疑似回線を設定します。

ステップ 2　ポップ アップ ウィンドウで、[Calculate Path] ボタンをクリックします。

これは以前に指定された N-PE 間の最短パスを使用してパスの図を表示します。それらの間の既存の MPLS-TP トンネルが優先されます。

ステップ 3　右のプラス（またはマイナス）アイコンをクリックして、パス制約を追加（または削除）します。

- [Required NE/Link] : パス用にパス スルーする必要があるトラフィックの要素またはリンクを指定します。
- [Required NE/Link] : パス用にパス スルーしてはならないトラフィックの要素またはリンクを指定します。

ステップ 4　どのパスを使用するかを決定したら、[Save] をクリックして、サービス要求の作成操作を完了します。

[Service Request Manager] ウィンドウが開きます。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。Service Request Manager の要素と操作については、第 8 章「サービス要求の管理」を参照してください。

EVC サービス要求の変更

リンクまたはサービス要求の他の設定を変更する必要がある場合は、EVC サービス要求を変更できます。

EVC サービス要求を変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

[Service Request Manager] ウィンドウが表示され、Prime Provisioning で使用可能なサービス要求が示されます。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

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

ステップ 4　必要に応じて、属性を変更します。

このウィンドウでの属性の設定に関する詳細なカバレッジについては、「サービス要求の詳細の設定」（P.3-38）で始まる項を参照してください。

（注）　VC ID、VPLS VPN ID、および VLAN ID は、サービス要求で設定した後は変更できません。

ステップ 5　テンプレートまたはデータ ファイルを接続回線に追加するには、「EVC イーサネット 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」（P.3-57）の項を参照してください。

ステップ 6　EVC サービス要求の編集が終了したら、[Save] をクリックします。

EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

EVC イーサネット 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

Prime Provisioning では、アプリケーションによって管理されるデバイスで使用可能なすべての CLI コマンドの設定はサポートされません。そのようなコマンドをデバイス上で設定するために、Prime Provisioning Template Manager 機能を使用できます。テンプレートは、デバイス ロール単位でポリシー レベルで関連付けることができます。サービス要求レベルでのテンプレートの上書きは、ポリシーレベルの設定でオペレータに許可されている場合は行うことができます。

サービス要求でテンプレートとデータ ファイルを関連付けるには、[Service Request Editor] ウィンドウで任意のリンクを選択して、ウィンドウの下部にある [Template] ボタンをクリックします。

（注）　関連付けられたポリシーでテンプレート機能が使用可能になっていない場合は、[Template] ボタンは選択できません。

[SR Template Association] ウィンドウが表示されます。このウィンドウでは、デバイス単位レベルでテンプレートを関連付けることができます。[SR Template Association] ウィンドウには、リンクを構成するデバイス、デバイス ロール、およびデバイスに関連付けられているテンプレートとデータ ファイルが一覧表示されます。この場合は、テンプレートまたはデータ ファイルはまだ設定されていません。

テンプレートとデータ ファイルをサービス要求に関連付ける方法に関する詳細については、「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。

EVC サービス要求の保存

EVC イーサネット サービス要求を保存するには、次の手順を実行します。

ステップ 1　EVC イーサネット サービス要求の属性の設定が終了したら、[Save] をクリックして、サービス要求を作成します。

EVC サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウが表示されます新しく作成された EVC のイーサネット サービス要求が [REQUESTED] の状態で追加されます。

ステップ 2　ただし、何らかの理由で（たとえば、選択した値が範囲外である）EVC イーサネット サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。

そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

ステップ 3　EVC イーサネット サービス要求を展開する準備ができたら、「サービス要求の展開」（P.8-10）を参照してください。

EVC ATM-Ethernet インターワーキング ポリシーの作成

この項は、Prime Provisioning の EVC ATM-Ethernet インターワーキング サポートの概要および EVC ATM-Ethernet インターワーキング ポリシー作成の基本的な手順で構成されています。具体的な内容は、次のとおりです。

- 「EVC イーサネット ポリシーの定義」（P.3-20）
- 「サービス オプションの設定」（P.3-22）
- 「ATM インターフェイス属性の設定」（P.3-62）
- 「EVC 属性の設定」（P.3-25）
- 「インターフェイス属性の設定」（P.3-30）
- 「テンプレートの関連付けのイネーブル化」（P.3-36）

EVC ATM-Ethernet サービス要求の作成については、「EVC ATM-Ethernet インターワーキング サービス要求の管理」（P.3-74）を参照してください。

（注）　Prime Provisioning での EVC サポートの一般的な概要については、*『Cisco Prime Provisioning 6.3 Administration Guide』* の「Layer 2 Concepts」の章を参照してください。

EVC ATM-Ethernet インターワーキング ポリシーの定義

サービスをプロビジョニングするには、EVC ATM-Ethernet インターワーキング ポリシーを定義する必要があります。ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。

ポリシーは、EVC サービス要求の定義に必要な大部分のパラメータのテンプレートです。定義後に、共通する一連の特性を共有するすべての EVC サービス要求で EVC ポリシーを使用できます。新しいタイプのサービスまたは異なるパラメータを持つサービスを作成する場合は、常に新しい EVC ポリシーを作成します。EVC ポリシーの作成は通常、経験のあるネットワーク エンジニアが実行します。

EVC ATM-Ethernet インターワーキング ポリシーを定義するには、最初にサービス タイプ属性を設定します。これを行うには、次のステップを実行します。

ステップ 1　[Service Design] > [Create Policy] 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　[Policy Type] ドロップダウン リストから [EVC] 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　EVC ATM-Ethernet インターワーキング ポリシーの [Policy Name] を入力します。

ステップ 4　EVC ポリシーの [Policy Owner] を選択します。

EVC 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：すべてのサービス オペレータがこの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 EVC 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。

ステップ 5　EVC ポリシーの所有者を選択するには、[Select] をクリックします。

ポリシー所有者は、Prime Provisioning の設定中にカスタマーまたはプロバイダーを作成した際に設定しました。所有権がグローバルの場合は、[Select] 機能は表示されません。

ステップ 6　[Policy Type] を選択します。

選択できる基準は、次のとおりです。

- [ETHERNET]：「EVC イーサネット ポリシーの作成」（P.3-20）を参照してください。
- [ATM]：「ATM ポリシーの作成」（P.4-19）を参照してください。
- [ATM-Ethernet Interworking]：この項です。
- [TDM Circuit Emulation]：「CEM TDM ポリシーの作成」（P.4-6）を参照してください。

（注）　この項では、FlexUNI/EVC ATM-Ethernet インターワーキング ポリシー タイプの作成について説明します。EVC ETHERNET ポリシー タイプの使用については、「EVC イーサネット ポリシーの作成」（P.3-20）を参照してください。

ステップ 7　[Next] をクリックします。

[Service Options] ウィンドウが表示されます。

ステップ 8　次の項である「サービス オプションの設定」（P.3-22）に記載されているステップに進みます。

サービス オプションの設定

この項では、EVC ポリシーのサービス オプションの設定方法について説明します。

EVC サービス オプションを設定するには、次の手順を実行します。

ステップ 1　CE が N-PE に直接接続されている場合は、[CE Directly Connected to EVC] 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は、デフォルトでオフになっています。

（注）　[Editable] チェックボックスを使用すると、フィールドを編集可能にするオプションを使用できます。[Editable] チェックボックスをオンにすると、この EVC ポリシーを使用しているサービス オペレータは、EVC サービス要求の作成中に編集可能パラメータを変更できます。

使用方法に関する注釈：

- チェックボックスをオンにすると、このポリシーを使用して作成されたサービス要求は、直接接続リンクだけを持つことができます。イーサネット アクセス ノードは含められません。
- チェックボックスをオフにすると、このポリシーを使用して作成されたサービス要求は、リンクにイーサネット アクセス ノードを持つ場合と、持たない場合があります。
- CE が N-PE に直接接続されている場合は、NPC は、サービス要求の作成中にリンクには適用されません。
- CE が N-PE に直接接続されていない場合は、NPC は、Prime Provisioning の標準の動作に従って、サービス要求の作成中に使用されます。EVC 機能をサポートするための NPC の実装への変更はありません。

ステップ 2　EVC 機能を使用してすべてのリンクを設定する必要がある場合は、[All Links Terminate on EVC] 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は、デフォルトでオフになっています。使用方法に関する注釈：

- チェックボックスをオンにすると、そのようなポリシーを使用して作成されたサービス要求は、EVC 機能を使用したすべてのリンクを持つようになります。
- チェックボックスをオフにすると、ゼロ以上のリンクが EVC 機能を使用できるようになります。これは、サービスを配信しながら、1 つ以上のリンクで既存のプラットフォームを引き続き使用できるようにします。これによって、EVC サポートとのリンクを将来追加できるようになります。

（注）　チェックボックスをオフにすると、サービス要求の作成プロセスで、ユーザは、作成されたリンクが EVC であるか、非 EVC であるかを指定する必要があります。

- リンクが将来も EVC 機能を使用しないことが予期される場合（たとえば、プロバイダーが作成されるサービスの EVC インフラストラクチャにアップグレードする予定がない場合）は、EVC の代わりに、既存の Prime Provisioning ポリシー タイプ（L2VPN または VPLS）を使用できます。

ステップ 3　ドロップダウン リストから [MPLS Core Connectivity Type] を選択します。

（注）　コア オプションでは MPLS だけがサポートされます。このサービスに対する L2TPv3 サポートはありません。

選択できる基準は、次のとおりです。

- [PSEUDOWIRE] : MPLS コアにわたって 2 つの N-PE 間の接続を許可するには、このオプションを選択します。このオプションは、サービスをポイントツーポイント（E-Line）に制限しません。これは、[PSEUDOWIRE] オプションが選択されている場合でも、疑似回線の片側または両方の側のブリッジ ドメインに接続されている CE が引き続き複数存在する可能性があるためです。
- [LOCAL] : MPLS コアにわたる接続が必要ないローカル接続のケースでは、このオプションを選択します。

  ローカル接続では、次のシナリオがサポートされます。

  - N-PE 上のすべてのインターフェイスが EVC 対応で、EVC インフラストラクチャを使用しています。これは、これらのインターフェイス上のカスタマー トラフィックをすべてブリッジ ドメインに関連付けることで設定します。これは、N-PE 上で VLAN ID（ブリッジ ドメイン ID と等しい）を消費します。
  - N-PE 上の一部のインターフェイスは EVC 対応ですが、他はスイッチ ポート ベースです。そのような場合は、EVC インフラストラクチャを使用して設定されたインターフェイス上のカスタマー トラフィックはすべて、ブリッジ ドメインに関連付けられます。非 EVC インターフェイス上のトラフィック（およびこの N-PE 以外のすべてのアクセス ノードまたはインターフェイス）は、サービス プロバイダー VLAN ID を使用して設定されます。この場合、サービス プロバイダー VLAN ID は、EVC ベース サービスのブリッジ ドメイン ID と同じです。
  - N-PE 上の 2 つのインターフェイスだけが使用され、両方とも EVC 対応ラインカードに基づいています。最初のケースでは、オペレータは、ブリッジ ドメイン オプションを設定しないことを選択することがあります。この場合、ローカル接続に使用される **connect** コマンドが使用され、グローバル VLAN がデバイスで保存されます。オペレータがブリッジ ドメイン オプションを使用した設定を選択する場合は、両方のインターフェイスがブリッジ ドメイン ID に関連付けられるため、追加のローカル リンクを将来サービスに追加できます。これは、N-PE で VLAN ID（ブリッジ ドメイン ID）を消費します。
- [VPLS] : このオプションは、EVC ATM-Ethernet インターワーキング ポリシーとサービス要求ではサポートされません。

（注）　ポリシー ワークフローの後続のウィンドウで使用可能な属性は、[MPLS Core Connectivity Type] に選択した項目（[PSEUDOWIRE] または [LOCAL]）に基づいて動的に変わります。完全性を確保するため、さまざまなコア タイプに使用できるすべての属性が、次のステップで説明されています。属性は、別途明記されていない限り、すべてのコア タイプに適用されます。

（注）　また、一部の属性は、IOS または IOS XR プラットフォームだけでサポートされます。属性は、別途明記されていない限り、両方のプラットフォームに適用されます。すべてのプラットフォーム固有属性が、ポリシー ワークフロー ウィンドウに表示されます。後で、ポリシーに基づいてサービス要求を作成する（および特定のデバイスがサービス要求に関連付けられる）際に、プラットフォーム固有属性は、デバイス タイプ（IOS または IOS XR）に基づいて、サービス要求ウィンドウからフィルタリングされます。

ステップ 4　ブリッジ ドメインの特性を判別するには、[Configure With Bridge Domain] チェックボックスをオンにします。

[Configure With Bridge-Domain] オプションの動作は、次に示すように、[MPLS Core Connectivity Type] オプションで選択した項目と並行して動作します。

- [MPLS Core Connectivity Type] として [PSEUDOWIRE] を選択。次の 2 つのケースがあります。

  A.EVC の場合

  - [Configure With Bridge Domain] をオンにすると、ポリシーは、ブリッジ ドメインに関連付けられた SVI 下で疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サービス インスタンス下で直接疑似回線を設定します。これによってグローバル VLAN が保存されます。

  B.EVC を使用しない場合

  - [Configure With Bridge Domain] をオンにすると、ポリシーは、L2VPN サービス（SVI を使用）の場合と同様に疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サブインターフェイス下で直接疑似回線を設定します。

  疑似回線だけを、対応する EVC 対応インターフェイスのサービス インスタンス下、またはブリッジ ドメインに関連付けられた SVI の下のいずれかで直接設定できます。

- [MPLS Core Connectivity Type] として [LOCAL] を選択。
  - [Configure With Bridge Domain] をオンにすると、ポリシーでは、ポイントツーポイント ローカル接続サービスまたはマルチポイント ローカル接続サービスのいずれかが許可されます。
  - [Configure With Bridge Domain] がオフの場合、Prime Provisioning はブリッジ ドメインなしのポイントツーポイント ローカル接続のみを許可します。

ステップ 5　[Next] をクリックします。

[ATM Interface Attribute] ウィンドウが表示されます。

ステップ 6　次の項である「ATM インターフェイス属性の設定」（P.3-62）に記載されているステップに進みます。

ATM インターフェイス属性の設定

この項では、EVC ATM-Ethernet インターワーキング ポリシーの ATM インターフェイス属性を設定する方法について説明します。

ATM インターフェイス属性を設定するには、次のステップを実行します。

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

選択できる基準は、次のとおりです。

- [VP]：仮想パス モード。これはデフォルトです。
- [VC]：仮想回線モード。

ステップ 2　ドロップダウン リストから [ATM Encapsulation] を選択します。

- AAL5SNAP

ステップ 3　[Next] をクリックします。

[EVC Attribute] ウィンドウが表示されます。

ステップ 4　次の項である「EVC 属性の設定」（P.3-25）に記載されているステップに進みます。

EVC 属性の設定

この項では、EVC ATM-Ethernet ポリシーの EVC 属性を設定する方法について説明します。

EVC 属性は、次のカテゴリに編成されます。

- Service Attributes
- VLAN Match Criteria
- VLAN Rewrite Criteria

次の項では、各カテゴリのオプションの設定方法について説明します。

[Service] 属性の設定

EVC サービス属性を設定するには、次の手順を実行します。

ステップ 1　サービス要求の作成中にサービス インスタンス ID を自動生成し、リンクに割り当てることを指定するには、[AutoPick Service Instance ID] チェックボックスをオンにします。

チェックボックスをオフにすると、サービス要求の作成中に Prime Provisioning リンク属性を設定するときに、Prime Provisioning は、サービス インスタンス ID を指定するようオペレータに求めます。

使用方法に関する注釈：

- サービス インスタンス ID は、EVC インフラストラクチャ内のインターフェイス上の Ethernet Flow Point（EFP; イーサネット フロー ポイント）を表します。サービス インスタンス ID は、インターフェイスに対してローカルで有効です。この ID は、インターフェイス レベルだけで固有でなければなりません。ID は 1 ～ 8000 までの値でなければなりません。
- Prime Provisioning では、サービス インスタンス ID の割り当て元として使用可能なリソース プールはありません。
- サービス要求を作成するオペレータが、インターフェイス レベルで ID の一意性を維持する必要があります。

ステップ 2　ポリシーに基づいたサービス要求の作成時に Prime Provisioning にサービス インスタンス名を自動生成させるには、[AutoPick Service Instance Name] チェックボックスをオンにします。自動生成される値のパターンは、*CustomerName_ServiceRequestJobID* です。

チェックボックスをオフにすると、サービス要求の作成中に値を入力できます。

ステップ 3　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[Enable PseudoWire Redundancy] 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：

- [Enable Pseudo Wire Redundancy] は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。

ステップ 4　サービス要求の作成中に Prime Provisioning に VC ID を自動選択させるには、[AutoPick VC ID] 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フにすると、オペレータは、サービス要求の作成中に VC ID を指定するよう求められます。

使用方法に関する注釈：

- [AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。

ステップ 5　サービス要求の作成中に Prime Provisioning にサービス要求の VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにすると、オペレータは、サービス要求の作成中に VLAN ID を指定するよう求められます。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメインまたは VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。サービス要求で VLAN ID を割り当てると、Prime Provisioning は、後続のサービス要求では VLAN ID を使用不可にします。
- 手動による VLAN ID の割り当ての場合は、ID が Prime Provisioning によって管理される VLAN プールの範囲外にあると、Prime Provisioning は VLAN ID を管理しません。この場合は、オペレータは、イーサネット アクセス ドメインで ID の一意性を確保する必要があります。オペレータが、Prime Provisioning によって管理される VLAN プールの範囲内にある VLAN ID を指定した場合に、その VLAN ID がアクセス ドメインですでに使用中であるときは、Prime Provisioning は、VLAN ID が使用中であることを示すエラー メッセージを表示します。

アクセス VLAN ID に関する注釈

アクセス VLAN ID は、EVC 対応ポートに対してローカルで有効です。グローバル VLAN と混同しないでください。これは、EVC ポートの向こうにあるイーサネット アクセス ネットワークをいくつかのサブイーサネット アクセス ドメインにパーティション化する（EVC 対応ポートごとに 1 つ）ことで可視化できます。

ただし、EVC ポートの向こうにあるイーサネット アクセス ノード上のすべてのサービス インターフェイスには、リンクのこの同じ VLAN ID が割り当てられます。この ID は、サービス要求の作成中にリンク属性を設定する際にオペレータが手動で指定する必要があります。オペレータは、EVC-demarcated イーサネット アクセス ドメインにわたって ID の一意性を確保する必要があります。

これらの VLAN ID は、ローカルで有効な VLAN プールを使用して Prime Provisioning によって管理されません。ただし、サービス要求でリンクに VLAN ID を割り当てた後で、Prime Provisioning は、EVC によって境界が定められたイーサネット アクセス ドメイン内の後続のサービス要求では VLAN を使用不可にします。同様に、手動で指定した VLAN が、EVC によって区切られたアクセス ドメインですでに使用中の場合は、Prime Provisioning は、指定された新しい VLAN ID が NPC ですでに使用中であることを示すエラー メッセージを表示します。オペレータは、L2 アクセス ノードでプロビジョニングされる別の VLAN ID を指定するよう求められます。

ステップ 6　次の項である「VLAN 一致基準属性の設定」（P.3-27）に記載されているステップに進みます。

VLAN 一致基準属性の設定

EVC 機能を導入する前に、サービス プロバイダーは、単一のポートでサービス多重化サービス（ERS/ERMS または EVPL/EVCS）またはサービス バンドル サービスのいずれかを展開できます。インフラストラクチャの制限が原因で、両方を同時にサポートすることはできません。この制限では、最外部の VLAN タグの照合だけが許可されます。

Prime Provisioning での EVC サポートの主な利点の 1 つは、着信フレームの VLAN タグ（最大 2 つのレベル）を調べて、適切なイーサネット フロー ポイント（EFP）に関連付けるための柔軟な方法が提供されることです。これによって、サービス プロバイダーは、サービス多重化サービスとサービス バンドル サービスの両方を単一のポートに同時に展開できます。

EVC VLAN 一致基準属性を設定するには、次の手順を実行します。

ステップ 1　ポリシーを使用して作成されたサービス要求を、着信フレームの内部 VLAN タグと外部 VLAN タグの両方と一致させるには、[Both Tags] 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しないと、ポリシーを使用して作成されたサービス要求は、着信フレームの外部 VLAN タグだけと一致します。

[Both Tags] 属性をオンにすると、[Inner VLAN Ranges] 属性（次の手順で説明）が [EVC Attribute] ウィンドウに表示されます。

ステップ 2　サービス要求の作成中に内部 VLAN タグの範囲を指定できるようにするには、[Inner VLAN Ranges] チェックボックスをオンにします。

チェックボックスをオフにすると、内部 VLAN タグの範囲は許可されません。この場合は、オペレータは、サービス要求の作成中に別個の VLAN ID を指定する必要があります。

ステップ 3　サービス要求の作成中に外部 VLAN タグの範囲を指定できるようにするには、[Outer VLAN Ranges] チェックボックスをオンにします。

チェックボックスをオフにすると、外部 VLAN タグの範囲は許可されません。この場合は、オペレータは、サービス要求の作成中に別個の VLAN ID を指定する必要があります。

ステップ 4　サービス要求の作成中に、以前に作成した外部 VLAN ID リソース プールから外部 VLAN ID を Prime Provisioning が自動選択するように設定するには、[AutoPick Outer VLAN] 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フにすると、オペレータは、サービス要求の作成中に外部 VLAN ID を指定するよう求められます。

（注）　[AutoPick Outer VLAN] 属性を使用するには、2 つの要素が Prime Provisioning で事前に設定されている必要があります。1 つめの要素はインターフェイス アクセス ドメインであり、これは N-PE デバイスの物理ポートをグループ化する論理要素です。2 つめの要素は EVC 外部 VLAN リソース プールであり、これはインターフェイス アクセス ドメインによって使用されます。これらの要素を設定する方法については、項「リソースの設定」（P.2-42）と「リソース プール」（P.2-46）を参照してください。

使用方法に関する注釈：

- [AutoPick Outer VLAN] は、EVC 機能をサポートするインターフェイスに使用できます。
- [AutoPick Outer VLAN] は、EVC をサポートするインターフェイスで VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 5　次の項である「VLAN 書き換え基準属性の設定」（P.3-28）に記載されているステップに進みます。

VLAN 書き換え基準属性の設定

VLAN 一致基準とともに、VLAN 書き換えは、EVC インフラストラクチャを非常に強力かつ柔軟にします。次の VLAN 書き換えオプションがサポートされています。

- 1 つまたは 2 つのタグをポップする。
- 1 つまたは 2 つのタグをプッシュする。
- 変換（1:1、2:1、1:2、2:2）。

VLAN 書き換え基準属性を設定するときは、次の点に注意してください。

- どの CE-facing EVC リンクでも、行うことができる書き換えは 1 種類だけです。
- すべての VLAN 書き換えは、入力トラフィックで **symmetric** キーワードを使用して行われます（たとえば、**rewrite ingress tag pop 2 symmetric**）。
- すべてのサービス インスタンスで、インスタンスごとに 1 つのタイプの書き換えオプション（ポップ、プッシュ、または変換）だけが許可されます。たとえば、[pop outer] をイネーブルにすると、[push inner]、[push outer]、[translate inner]、および [translate outer] は使用できません。

EVC VLAN 書き換え基準属性を設定するには、次の手順を実行します。

ステップ 1　一致基準を満たす着信フレームの外部 VLAN ID タグをポップするには、[Pop Outer] 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フにすると、着信トラフィックの外部タグはポップされません。

ステップ 2　一致基準を満たす着信フレームの内部 VLAN ID タグをポップするには、[Pop Inner] 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フにすると、内部タグはポップされません。[Pop Inner] をオンにすると、[Pop Outer] が自動的にオンになることに注意してください。

ステップ 3　一致基準を満たす着信フレームの外部 VLAN ID タグをインポーズするには、[Push Outer] 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フにすると、外部タグは着信フレームでインポーズされません。

使用方法に関する注釈：

- [Push Outer] をオンにする場合は、ポリシーを使用して作成されたすべてのサービス要求が、一致基準と一致する着信フレームで dot1q 外部タグをプッシュします。サービスの作成中にリンクを作成する場合は、オペレータは、1 ～ 4096 までの値で外部タグを指定できます。
- この属性は、一致基準で使用されるタグの数に関係なく使用可能です。着信トラフィックがダブルタグ付きであるか、シングルタグ付きであるかに関係なく、[Push Outer] をイネーブルにすると、対応するすべてのサービス要求が外部タグをプッシュします。後続のノードはすべて、最外部の 2 つのタグ（EVC 対応の場合）または 1 つのタグ（EVC 対応ではない場合）だけを考慮し、最内部のタグを透過的にペイロードとして扱います。
- この VLAN ID は、Prime Provisioning 管理の VLAN ID プールからは得られません。

ステップ 4　一致基準を満たす着信フレームの内部 VLAN ID タグをインポーズするには、[Push Inner] チェックボックスをオンにします。

この操作は、内部タグだけでなく、内部タグと外部タグの両方を着信パケットにプッシュします。このチェックボックスをオフにすると、内部タグは着信フレームでインポーズされません。

使用方法に関する注釈：

- [Push Inner] をオンにする場合は、ポリシーを使用して作成されたすべてのサービス要求が、一致基準と一致する着信フレームで dot1q 内部タグをプッシュします。サービスの作成中にリンクを作成する場合は、オペレータは、1 ～ 4096 までの値で内部タグを指定できます。

- [Push Inner] をオンにすると、[Pop Outer] が自動的にオンになります。
- この属性は、一致基準で使用されるタグの数に関係なく使用可能です。着信トラフィックがダブルタグ付きであるか、シングルタグ付きであるかに関係なく、[Push Inner] をイネーブルにすると、対応するすべてのサービス要求が内部タグをプッシュします。後続のノードはすべて、最外部の 2 つのタグ（EVC 対応の場合）または 1 つのタグ（EVC 対応ではない場合）だけを考慮し、最内部のタグを透過的にペイロードとして扱います。
- この VLAN ID は、Prime Provisioning 管理の VLAN ID プールからは得られません。

ステップ 5　サービス要求の作成中にオペレータがターゲットの外部 VLAN ID を指定できるようにするには、[Translate Outer] チェックボックスをオンにします。

一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。チェックボックスをオフにすると、外部タグの変換は実行されません。表 3-4 を参照してください。

ステップ 6　サービス要求の作成中にオペレータがターゲットの内部 VLAN ID を指定できるようにするには、[Translate Inner] チェックボックスをオンにします。

一致基準を満たすすべての着信フレームの内部タグがこの ID に変換されます。チェックボックスをオフにすると、内部タグの変換は実行されません。表 3-4 を参照してください。

（注）　表 3-4 には、EVC インフラストラクチャで使用可能なさまざまな VLAN 変換の実行の要約が示されています。2 番めと 3 番めの列（「外部タグと一致」と「内部タグと一致」）は、ポリシー設定を示しています。最後の 2 つの列（「外部タグの変換」と「内部タグの変換」）は、着信フレームで行われる VLAN 変換を示しています。

表 3-4　VLAN 変換の要約表

タイプ	外部タグと一致	内部タグと一致	外部タグの変換	内部タグの変換	プッシュ外部タグ
1:1	True	N/A	Yes	No	N/A
1:2	True	N/A	N/A	N/A	Yes
2:1	True	True	Yes	No	N/A
2:2	True	True	Yes	Yes	N/A

ステップ 7　[Next] をクリックします。

[Interface Attribute] ウィンドウが表示されます。

ステップ 8　次の項である「インターフェイス属性の設定」（P.3-30）に記載されているステップに進みます。

インターフェイス属性の設定

EVC ATM-Ethernet インターワーキング ポリシー作成のこの手順には、[Interface Attribute] ウィンドウに示されているように、インターフェイス属性の設定が含まれます。このウィンドウで設定できる属性は、次のカテゴリにグループ化されます。

- UNI 情報
- VLAN
- 疑似回線

- ACL
- セキュリティ
- UNI ストーム制御
- プロトコル

場合によっては、属性を確認すると、GUI に追加の属性が表示されます。これは、次のステップで説明します。

（注） CE が N-PE に直接接続されている場合は、速度、デュプレックス、UNI シャットダウン、およびその他の汎用オプションだけが表示されます。この場合は、現在のプラットフォームの制限が原因で、ポート セキュリティ、ストーム制御、L2 プロトコル トンネリング、およびその他の高度な機能はサポートされません。サービスでこれらの機能が必要な場合、サービス プロバイダーは、これらの要件をサポートするためにレイヤ 2 イーサネット アクセス ノードを EVC の外にまで展開する必要があります。

（注） [Interface Attributes] ウィンドウで使用可能な属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] に選択した項目（[PSEUDOWIRE] または [LOCAL]）に基づいて動的に変わります（「サービス オプションの設定」（P.3-22）を参照）。完全性を確保するため、さまざまなコア タイプに使用できるすべての属性が、次のステップで説明されています。属性は、別途明記されていない限り、すべてのコア タイプに適用されます。

EVC インターフェイス属性を設定するには、次の手順を実行します。

ステップ 1　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

（注） IOS XR が実行されている N-PE デバイスで UNI を設定する場合は、[Standard UNI Port] 属性はサポートされません。この場合、[Standard UNI Port] と [UNI Port Security] に関連する CLI はすべて無視されます。

ステップ 2　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 3　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために、編集可能です。

ステップ 4　[Link Media]（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

ステップ 5　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 6　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- [DOT1QTRUNK] : 802.1q カプセル化によって UNI をトランクとして設定します。UNI が直接接続された EVC リンクに属している場合、この設定は、着信フレームが 802.1q カプセル化され、リンクに設定された VLAN ID と一致することを意味します。この固有のトポロジには、トランク UNI 自体は含まれていません。
- [DOT1QTUNNEL] : UNI を 802.1q トンネル（dot1q トンネルまたは Q-in-Q とも呼ばれています）ポートとして設定します。
- [ACCESS] : UNI をアクセス ポートとして設定します。

ステップ 8　適切なオプション ボタンをクリックして、このポリシーの [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No] : VLAN 変換は実行されません （デフォルト）。
- [1:1] : 1:1 VLAN 変換。着信カスタマー VLAN を別のものに変換します。
- [2:1] : 2:1 VLAN 変換。内部および外部の両方の VLAN を単一の VLAN に変換します。
- [1:2] : 1 対 2 VLAN 変換。もう 1 つのプロバイダー VLAN をプッシュします。
- [2:2] : 2 対 2 VLAN 変換。内部および外部の両方の VLAN を別の 2 つの VLAN に変換します。

（注）　EVC ATM-Ethernet サービスで VLAN がどのようにサポートされるかについては、「EVC ATM-Ethernet インターワーキング サービス要求の管理」（P.3-74）の VLAN 変換属性の対象範囲を参照してください。

ステップ 9　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR デバイスで pw-class コマンドをプロビジョニングするために使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。

ステップ 10　[L2VPN Group Name] では、ドロップダウン リストから次のいずれかを選択します。

- ISC
- VPNSC

使用方法に関する注釈：

- この属性は、IOS XR デバイスで L2VPN グループ名をプロビジョニングするために使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

- [L2VPN Group Name] は、IOS XR デバイスだけに適用されます。

ステップ 11　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

使用方法に関する注釈：

- ポリシーまたはポリシーに基づくサービス要求のいずれかの [E-Line Name] に何も値が指定されていない場合、Prime Provisioning は次のようにデフォルト名を自動生成します。
  - [PSEUDOWIRE] コア接続タイプの場合は、次の形式になります。
    DeviceName--VC_ID
  - [LOCAL] コア接続タイプの場合は、次の形式になります。
    DeviceName--VLAN_ID

  デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。
- [E-Line Name] は、IOS XR デバイスだけに適用されます。

ステップ 12　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 13　Prime Provisioning に SVI（スイッチ仮想インターフェイス）でフォワーディング コマンドを生成させるには、[N-PE Pseudo-wire on SVI] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフになっています。この場合、Prime Provisioning は、サービス インスタンスでフォワーディング コマンドを生成します。

EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（これは、[EVC Policy Editor - Service Options] ウィンドウのポリシー ワークフローで使用可能です）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

使用方法に関する注釈：

- Prime Provisioning では、EVC サービス要求のハイブリッド設定がサポートされます。ハイブリッド設定では、接続回線のいずれかの側のフォワーディング コマンド（xconnect など）は、サービス インスタンスで設定でき、接続回線のもう一方の側の xconnect 設定は、スイッチ仮想インターフェイス（SVI）で設定できます。
- これらのケースの例については、コンフィグレットの例 「EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）」（P.3-222）と「EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）」（P.3-223）を参照してください。

- [N-PE Pseudo-wire on SVI] は、すべての接続タイプに適用できますが、ハイブリッド SVI 設定は疑似回線接続だけで可能です。
- [MPLS Core Connectivity Type] が [LOCAL] 接続タイプに設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にディセーブルにされます。
- [N-PE Pseudo-wire on SVI] 属性は、IOS XR デバイスではサポートされません。すべての xconnect コマンドは、L2 サブインターフェイスまたはサービス インスタンスで設定されます。
- 表 3-5 では、EVC サービス要求のハイブリッド設定のさまざまな使用例を示します。

表 3-5　EVC サービス要求のハイブリッド設定の使用例

ブリッジ ドメインの使用	EVC	SVI 上の N-PE 疑似回線	生成される CLI
True	True	True	• VLAN インターフェイスの xconnect。 • メイン インターフェイスのサービス インスタンス。
True	True	False	• サービス インスタンスの xconnect。 • メイン インターフェイスのサービス インスタンス。
False	True	N/A	• サービス インスタンスの xconnect。 • メイン インターフェイスのサービス インスタンス。
True	False	True	VLAN インターフェイスの xconnect。
True	False	False	サブインターフェイスの xconnect。
False	False	False	サブインターフェイスの xconnect。

ステップ 14　独自の名前付きアクセス リストをポートに割り当てる場合は、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 15　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 16　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 17　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b. [Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c. [Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 18 UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 19 コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

選択したプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Enable cdp] : Cisco Discover Protocol（CDP）でレイヤ 2 トンネリングをイネーブルにします。

b. [cdp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

c. [cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Enable vtp] : VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）でレイヤ 2 トンネリングをイネーブルにします。

e. [vtp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Enable stp] : スパニングツリー プロトコル（STP）でレイヤ 2 トンネリングをイネーブルにします。

h. [stp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 20 [MTU Size] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。デフォルトのサイズは 9216 で、範囲は 1500 ～ 9216 です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。

Cisco Prime Provisioning 6.3 では、異なるプラットフォームによって異なる範囲をサポートします。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- Cisco 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードでは、MTU サイズとして 9216 だけが使用され、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Cisco Prime Provisioning 6.3 は両方のケースで 9216 を使用します。
- Cisco 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21　この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場合は、[Next] ボタンをクリックします。

この機能の詳細については、「テンプレートの関連付けのイネーブル化」（P.3-36）を参照してください。

（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。

ステップ 22　EVC ポリシーを保存するには、[Finish] をクリックします。

EVC ATM-Ethernet インターワーキング ポリシーに基づいてサービス要求を作成するには、「EVC ATM-Ethernet インターワーキング サービス要求の管理」（P.3-74）を参照してください。

テンプレートの関連付けのイネーブル化

Prime Provisioning テンプレート機能を使用すると、デバイスにフリーフォーマット CLI をダウンロードできます。テンプレートをイネーブルにする場合は、Prime Provisioning で現在サポートされていないコマンドをダウンロードするために、テンプレートとデータ ファイルを作成できます。

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、（[Finish] をクリックする前に）[Interface Attribute] ウィンドウで [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、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、「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 2　ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

ステップ 3　EVC ATM インターワーキング ポリシーを保存するには、[Finish] をクリックします。

EVC ATM-Ethernet インターワーキング ポリシーに基づいてサービス要求を作成するには、「EVC ATM-Ethernet インターワーキング サービス要求の管理」（P.3-74）を参照してください。

EVC ATM-Ethernet インターワーキング サービス要求の管理

この項では、EVC ATM-Ethernet インターワーキング サービス要求のプロビジョニング方法について説明します。具体的な内容は、次のとおりです。

概要

EVC ATM-Ethernet インターワーキング サービス要求では、「EVC ATM-Ethernet インターワーキング ポリシーの作成」（P.3-58）で説明した EVC 機能をサポートするために、N-PE でインターフェイスを設定することができます。EVC ATM-Ethernet インターワーキング サービス要求を作成するには、「EVC ATM-Ethernet インターワーキング ポリシーの作成」（P.3-58）で説明されているように、EVC ATM-Ethernet インターワーキング 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。定義済みの EVC ポリシーに基づいて、オペレータは、EVC ポリシーに変更を行うか、変更を行わずにサービス要求を作成してサービスを展開します。サービス要求の一部として、1 つ以上のテンプレートを N-PE に関連付けることもできます。

ATM-Ethernet インターワーキングは、次の設定によってサポートされます。

- ATM トランスポート モード（VC）
  - ATM-Ethernet 疑似回線
  - ATM-ATM ローカル接続
  - ATM-Ethernet ローカル接続
- ATM トランスポート モード（VP）
  - ATM-ATM ローカル接続

EVC ATM-Ethernet インターワーキング サービス要求を作成する際に、次の手順を実行する必要があります。

- 既存の EVC ATM-Ethernet インターワーキング ポリシーを選択します。
- VPN を選択します。

（注）　EVC ポリシーとサービス要求のコンテキストで VPN オブジェクトを操作する場合は、VPN 名とカスタマー属性だけが関係します。MPLS と VPLS に関連するその他の VPN 属性は無視されます。

- ブリッジ ドメイン コンフィギュレーションを指定します（該当する場合）。
- サービス要求の説明を指定します。
- VC ID または VPLS VPN ID の自動または手動の割り当てを指定します。

- 直接接続リンクを追加します（該当する場合）。
- L2 アクセス ノードとのリンクを追加します（該当する場合）。
- リンクの N-PE と UNI インターフェイスを選択します。
- L2 アクセス ノードとのリンクでは、N-PE または UNI インターフェイスに複数の NPC が存在する場合は、Named Physical Circuit（NPC; 名前付き物理回線）を選択します。
- リンク属性を編集します。
- サービス要求を変更します。
- サービス要求を保存します。

EVC ATM-Ethernet インターワーキング シナリオのサンプル 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.3-186）を参照してください。

EVC ATM-Ethernet インターワーキング サービス要求の作成

EVC ATM-Ethernet インターワーキング 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 Request Manager] を選択します。

[Service Request Manager] 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。

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

ステップ 3　ポリシー選択機能を使用して、以前に作成したポリシーから EVC ATM-Ethernet インターワーキング ポリシーを選択します（「EVC ATM-Ethernet インターワーキング ポリシーの作成」（P.3-58）を参照）。

[EVC Service Request Editor] ウィンドウが表示されます。新しいサービス要求は、すべての編集可能な機能と編集不可能な機能および事前設定されたパラメータなど、選択した EVC ATM-Ethernet インターワーキング ポリシーのプロパティをすべて継承します。

ステップ 4　次の項である「サービス要求の詳細の設定」（P.3-38）に記載されているステップに進みます。

サービス要求の詳細の設定

サービス要求の基礎として使用する EVC ポリシーを選択した後で、[EVC Service Request Editor] ウィンドウが表示されます。これは次の 3 つのセクションに分かれています。

- Link Page
- [Direct Connect Links]（NPC なし）
- [Links with L2 Access Nodes]（NPC を使用）

このウィンドウでは、サービス要求のオプションを指定して、直接接続リンクと L2 アクセス ノードとのリンクを設定できます。ウィンドウの最初のセクションに表示されるオプションは、ポリシーで指定された [MPLS Core Connectivity Type]（疑似回線またはローカル）によって変わります。明確にするために、これらの各シナリオは下記では別個のセクションに示されており、さまざまなウィンドウ設定と表示されるオプションの動作が強調されています。

ポリシーの [MPLS Core Connectivity Type] で決定された、該当する項に進みます。

- 「疑似回線コア接続」（P.3-38）
- 「ローカル コア接続」（P.3-42）

直接接続リンクと L2 アクセス ノードとのリンクを設定するための指示は、後の項に示されています。

疑似回線コア接続

この項では、EVC ATM-Ethernet インターワーキング ポリシーの [MPLS Core Connectivity Type] が [PSEUDOWIRE] であるケースについて説明します。

[EVC Service Request Editor] ウィンドウの最初のセクションで属性を設定するには、次の手順を実行します。

（注）　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

（注）　[Policy] フィールドは読み取り専用です。サービス要求の元になっているポリシーの名前が表示されます。読み取り専用のポリシー名をクリックすると、ポリシー内で設定されているすべての属性値のリストが表示されます。

ステップ 1　このサービス要求で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

（注）　コア タイプが LOCAL および PSEUDOWIRE のサービス要求では同じ VPN を使用できます。サービス要求の VPN が VPLS コア タイプで使用される場合は、コア タイプが LOCAL または PSEUDOWIRE のサービス要求には同じ VPN を使用できません。

ステップ 2　[Select] 列で **VPN 名**を選択します。

ステップ 3　[Select] をクリックします。

VPN 名が示された [EVC Service Request Editor] ウィンドウが表示されます。

ステップ 4　Prime Provisioning に VC ID を選択させる場合は、[AutoPick VC ID] 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しない場合は、次のステップで説明されているように、[VC ID] フィールドで ID を指定するよう求めるプロンプトが表示されます。

[AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。この場合は、[VC ID] オプションのテキスト フィールドは編集不可能です。

ステップ 5　[AutoPick VC ID] をオフにした場合は、[VC ID] フィールドに VC ID を入力します。

使用方法に関する注釈：

- [AutoPick VC ID] 属性は、EVC 疑似回線サービス要求の作成中に表示されます。
- [VC ID] 値は、VC ID に対応する整数値でなければなりません。

- VC ID を手動で割り当てると、Prime Provisioning は VC ID を調べて、Prime Provisioning の VC ID プール内にそれがあるかどうかを確認します。VC ID がプール内にあっても割り当てられていない場合は、VC ID はサービス要求に割り当てられます。VC ID がプール内にあって、すでに使用中の場合は、Prime Provisioning は別の VC ID を割り当てるよう求めるプロンプトを表示します。VC ID が Prime Provisioning VC ID プールの外にある場合は、Prime Provisioning は、VC ID が割り当てられているかどうかに関する検査を実行しません。オペレータは、VC ID が使用可能であることを確認する必要があります。
- VC ID は、サービスの作成中に限り入力できます。サービス要求の編集中は、[VC ID] フィールドは編集不可能です。

ステップ 6　ブリッジ ドメインの特性を判別するには、[Configure Bridge Domain] チェックボックスをオンにします。

[Configure Bridge Domain] オプションの動作は、EVC ポリシーの [MPLS Core Connectivity Type] オプションで選択した項目（この場合は、疑似回線コア接続）と並行して動作します。次の 2 つのケースがあります。

- EVC の場合
  - [Configure With Bridge Domain] をオンにすると、ポリシーは、ブリッジ ドメインに関連付けられた SVI の下で疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サービス インスタンス下で直接疑似回線を設定します。これによって、グローバル VLAN が保存されます。
- EVC を使用しない場合
  - [Configure With Bridge Domain] をオンにすると、ポリシーは、SVI の下で疑似回線を設定します。
  - [Configure With Bridge Domain] をオフにすると、ポリシーは、サブインターフェイスで直接疑似回線を設定します。

  疑似回線を、対応する EVC 対応インターフェイスのサービス インスタンス下、またはブリッジ ドメインに関連付けられた SVI の下のいずれかで直接設定できます。

ステップ 7　ブリッジ ドメインとのスプリット ホライズンをイネーブルにするには、[Use Split Horizon] 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：

- [Use Split Horizon] 属性はデフォルトでディセーブルになっています。
- [Use Split Horizon] 属性は、[Configure Bridge Domain] チェックボックスがオン（イネーブル）になっている場合にだけ使用できます。
- [Use Split Horizon] がイネーブルになっている場合は、スプリット ホライズンとともに CLI で **bridge domain** コマンドが生成されます。ディセーブルにすると、スプリット ホライズンなしで **bridge domain** コマンドが生成されます。

ステップ 8　サービス要求の説明ラベルを入力するには、[Description] 属性の [Click here] リンクをクリックします。

これは、Prime Provisioning データベースで特定のサービス要求を検索するのに役立ちます。

説明を入力できるダイアログが表示されます。

ステップ 9　ダイレクト接続リンクを設定するには、「直接接続リンクの設定」（P.3-44）の項を参照してください。

ステップ 10　L2 アクセス ノードとのリンクを設定するには、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）の項を参照してください。

ローカル コア接続

この項では、EVC ATM-Ethernet インターワーキング ポリシーの [MPLS Core Connectivity Type] が [LOCAL] であるケースについて説明します。

[EVC Service Request Editor] ウィンドウの最初のセクションで属性を設定するには、次の手順を実行します。

ステップ 1　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。

初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

ステップ 2　[Policy] フィールドは読み取り専用です。

サービス要求の元になっているポリシーの名前が表示されます。

ステップ 3　このサービス要求で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

（注）　コア タイプが LOCAL および PSEUDOWIRE のサービス要求では同じ VPN を使用できます。サービス要求の VPN が VPLS コア タイプで使用される場合は、コア タイプが LOCAL または PSEUDOWIRE のサービス要求には同じ VPN を使用できません。

ステップ 4　[Select] 列で **VPN 名**を選択します。

ステップ 5　[Select] をクリックします。

VPN 名が示された [EVC Service Request Editor] ウィンドウが表示されます。

ステップ 6　ブリッジ ドメインの特性を判別するには、[Configure Bridge Domain] 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：

- [Configure Bridge Domain] がオンの場合は、すべてのリンクに、N-PE 上の VLAN プールから同じブリッジ ドメイン ID が割り当てられます。すべての非 EVC リンクには、ブリッジ ドメイン ID としてサービス プロバイダー VLAN が割り当てられます。その一方で、EVC リンクが追加されない場合は、サービス プロバイダー VLAN が最初に割り当てられ、これは、EVC リンクが追加されたときにブリッジ ドメイン ID として使用されます。
- [Configure Bridge Domain] をオフにすると、同じ N-PE で終端するリンクを最大 2 つ追加できます （これは、EVC インフラストラクチャで使用可能な **connect** コマンドを使用します）。これは、ATM-ATM ローカル接続だけでサポートされます。

（注）　Prime Provisioning が接続名を自動生成する方法に関する詳細については、次の補足説明を参照してください。

デバイスでは、接続名には最大で 15 文字だけが受け入れられるため、接続名は次の形式を使用して生成されます。

CustomerNameTruncatedToMaxPossibleCharacters_ServiceRequestJobID

たとえば、カスタマー名が NorthAmericanCustomer で、サービス要求ジョブ ID が 56345 の場合は、自動生成される接続名は NorthAmer_56345 になります。

生成される CLI は次のとおりです。

```
connect NorthAmer_56345 ATM7/0/5 11 ATM7/0/4 18
```

この場合は、11 と 18 がサービス インスタンス VPI です。

- [Configure Bridge Domain] のポリシー設定が編集不可能な場合は、サービス要求のオプションは読み取り専用です。

ステップ 7　ブリッジ ドメインとのスプリット ホライズンをイネーブルにするには、[Use Split Horizon] 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：

- [Use Split Horizon] 属性はデフォルトでディセーブルになっています。
- [Use Split Horizon] 属性は、[Configure Bridge Domain] チェックボックスがオン（イネーブル）になっている場合にだけ使用できます。
- [Use Split Horizon] がイネーブルになっている場合は、スプリット ホライズンとともに CLI で **bridge domain** コマンドが生成されます。ディセーブルにすると、スプリット ホライズンなしで **bridge domain** コマンドが生成されます。

ステップ 8　サービス要求の説明ラベルを入力するには、[Description] 属性の [Click here] リンクをクリックします。

説明を入力できるダイアログが表示されます。

ステップ 9　ダイレクト接続リンクを設定するには、「直接接続リンクの設定」（P.3-44）の項を参照してください。

ステップ 10　L2 アクセス ノードとのリンクを設定するには、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）の項を参照してください。

N-PE へのリンクの設定

[EVC Service Request Editor] ウィンドウの下部 2 つのセクションでは、N-PE へのリンクを設定できます。直接接続リンクの場合は、CE は、中間 L2 アクセス ノードなしで N-PE に直接接続されます。L2 アクセス ノードとのリンクの場合は、Prime Provisioning で作成する NPC を必要とする CE と NPE の間に中間デバイスが存在します。

ウィンドウの [Direct Connect Links] セクションは、N-PE に直接接続するリンクを設定する場所です。NPC は使用されません。直接接続リンクでは ATM リンクがサポートされます。

[Links with L2 Access Nodes] セクションは、L2（イーサネット）アクセス ノードとのリンクを設定する場所です。NPC が使用されます。

（注）　ATM インターフェイスは、L2 アクセス ノード内には存在できません。

設定するリンクのタイプに応じて、適切な項を参照してください。

- 「直接接続リンクの設定」（P.3-44）
- 「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）

（注）　2 つのリンク タイプを設定するためのステップの多くは同じです。リンクを設定するための基本的なワークフロー、および設定する属性は、次の項である「直接接続リンクの設定」（P.3-44）に記載されています。L2 アクセス ノードとのリンクを設定する場合でも、この項に記載されている情報を参照すると役に立ちます。L2 アクセス ノードの項では、そのようなリンクに固有のステップだけが記載されているためです。

直接接続リンクの設定

直接接続リンクを設定するには、次の手順を実行します。これらのステップの多くは、L2 アクセス ノードとのリンクにも適用されます。

ステップ 1　[Add] をクリックして、リンクを追加します。

リンク属性の新たに番号付けされた行が表示されます。

ステップ 2　[N-PE] 列の [Select N-PE] をクリックします。

[Select PE Device] ウィンドウが表示されます。このウィンドウには、現在定義されている PE のリストが表示されます。

a. [Show PEs with] ドロップダウン リストには、[PEs by Provider]、[PE Region Name]、または [by Device Name] が表示されます。

b. [Find] ボタンを使用すると、特定の PE を検索するか、ウィンドウを更新できます。

c. [Rows per page] ドロップダウン リストでは、ユーザは画面に一度に表示される項目の数を設定できます。

ステップ 3　[Select] 列で、リンクの PE デバイス名を選択します。

ステップ 4　[Select] をクリックします。

選択した PE の名前が [NPE] 列に示された [EVC Service Request Editor] ウィンドウが再表示されます。

ステップ 5　[UNI] 列のインターフェイス選択機能から UNI インターフェイスを選択します。

（注） Prime Provisioning には、基盤となるインターフェイスの設定、インターフェイスを使用する可能性がある既存のサービス要求、サービス要求に関連付けられたカスタマーに基づいて、サービスに使用可能なインターフェイスだけが表示されます。[Details] ボタンをクリックして、インターフェイス名、カスタマー名、VPN 名、ジョブ ID、サービス要求 ID、サービス要求タイプ、変換タイプ、および VLAN ID 情報など、使用可能なインターフェイスに関する情報が示されたポップアップ ウィンドウを表示できます。

（注） IOS XR が実行されている N-PE デバイスで UNI を設定する場合は、[Standard UNI Port] 属性はサポートされません。この場合、[Standard UNI Port] と [UNI Port Security] に関連する CLI はすべて無視されます。

ステップ 6　[EVC] チェックボックスをオンにして、リンクの設定サービス インスタンスのリンクをマークします。

（注） ここで [EVC] チェックボックスについて述べるのは、このチェックボックスの設定によって [Link Attributes] 列内で使用できるリンク編集機能の動作が変わるからです。これは次のステップで説明します。

（注） [EVC] チェックボックスは、デフォルトでオフになっています。このチェックボックスのデフォルト値は、DCPL プロパティ Pr ovisioning\ProvDrv\CheckFlexUniCheckBox の値を設定することによって変更できます。

[Link Attributes] の編集

次のステップでは、[Link Attributes] 列の [Edit] リンクの使用について説明します（リンク属性がすでに設定されている場合は、このリンクが [Edit] から [Change] に変わります）。リンク編集ワークフローは、そのリンクの [EVC] チェックボックスの状態によって変化します。[EVC] チェックボックスがオンの場合、編集ワークフローには、2 セットのリンク属性について、2 つのウィンドウで行う属性設定が含まれます。

- EVC Details
- Standard UNI Details

リンクの [EVC] チェックボックスがオフの場合、[Standard UNI Details] ウィンドウだけが表示されます。

次のステップでは、両方のシナリオについて説明します。

（注）（N-PE デバイスで ATM インターフェイスを UNI として選択することによって）ATM リンクを設定している場合は、別のワークフローが存在します。[EVC] 列のチェックボックスは動的に非表示になり、[link attributes] 列で [Edit] リンクをクリックすると、[ATM-Ethernet Attributes] ウィンドウが表示されます。このウィンドウを使用した ATM リンクの設定については、「ATM リンク属性の設定」（P.3-90）を参照してください。

ステップ 7　[UNI] 属性を指定するには、[Link Attributes] 列で [Edit] をクリックします。

[EVC Details] ウィンドウ

[EVC] チェックボックスをオンにすると、[EVC Details] ウィンドウが表示されます。

[EVC Details] ウィンドウのフィールドはすべて、ポリシー設定に基づいてイネーブルになります。たとえば、[Both Tags] がポリシーで選択され、編集可能である場合は、このウィンドウで [Match Inner and Outer Tags] チェックボックスが選択され、編集可能になります。この動作は、[EVC Details] ウィンドウ内の他の属性についても類似しています。

ステップ 8　サービス要求の作成中にサービス インスタンス ID を自動生成し、リンクに割り当てることを指定するには、[AutoPick Service Instance ID] チェックボックスをオンにします。

チェックボックスをオフにする場合は、サービス インスタンス ID を指定する必要があります（次のステップを参照）。

使用方法に関する注釈：

- サービス インスタンス ID は、EVC インフラストラクチャ内のインターフェイス上の Ethernet Flow Point（EFP; イーサネット フロー ポイント）を表します。サービス インスタンス ID は、インターフェイスに対してローカルで有効です。この ID は、インターフェイス レベルだけで固有でなければなりません。ID は 1 ～ 8000 までの値でなければなりません。
- Prime Provisioning では、サービス インスタンス ID の割り当て元として使用可能なリソース プールはありません。
- サービス インスタンス ID を手動で指定する場合は、オペレータが、インターフェイス レベルで ID の一意性を維持する必要があります。
- この属性は IOS XR デバイスでは表示されません。

ステップ 9　[AutoPick Service Instance ID] チェックボックスをオンにしない場合は、[Service Instance ID] フィールドにサービス インスタンス ID に適した値を入力します。

ステップ 10　サービス インスタンス名を自動生成することを指定するには、[AutoPick Service Instance Name] チェックボックスをオンにします。

チェックボックスをオフにすると、サービス インスタンス名を指定できます（次のステップを参照）。

使用方法に関する注釈：

- チェックボックスをオンにすると、[Service Instance Name] テキスト フィールドはディセーブルになります。
- サービス インスタンス名は、*CustomerName_ServiceRequestJobID* というパターンで自動生成されます。
- コングレットの例については、「EVC（AutoPick サービス インスタンス名なし、サービス インスタンス名なし）」（P.3-225）、「EVC（ユーザ指定のサービス インスタンス名、疑似回線コア接続）」（P.3-226）、および「EVC（ユーザ指定のサービス インスタンス名、ローカル コア接続）」（P.3-227）を参照してください。
- この属性は IOS XR デバイスでは表示されません。

ステップ 11　[AutoPick Service Instance Name] チェックボックスをオンにしない場合は、[Service Instance Name] フィールドにサービス インスタンス ID に適した値を入力します。

使用方法に関する注釈：

- サービス インスタンス名を表すテキスト ストリングは、40 文字以下で、スペースは使用できません。他の特殊文字は使用できます。
- [AutoPick Service Instance Name] がオフで、テキスト フィールドにサービス インスタンス名が入力されていない場合、Prime Provisioning はサービス要求によって生成されるデバイスの設定中にグローバルな **ethernet evc evcname** コマンドを生成しません。

ステップ 12　サービス要求の作成中に Prime Provisioning にサービス要求の VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにする場合は、ブリッジ ドメイン VLAN ID を指定する必要があります（次のステップを参照）。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。
- この属性は IOS XR デバイスでは表示されません。

ステップ 13　[AutoPick Bridge Domain/VLAN ID] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID] フィールドに適切な値を入力します。

（注）　この設定は、[EVC Service Request Editor] ウィンドウの [Configure Bridge Domain] オプションとともに適用されます。このウィンドウでオプションをイネーブルにしない場合は、[AutoPick Bridge Domain/VLAN ID] チェックボックスは冗長であり、必要ありません。

VLAN ID を手動で割り当てる場合は、Prime Provisioning は、Prime Provisioning の VLAN ID プール内にあるかどうかを確認するために VLAN ID を調べます。VLAN ID がプール内にあっても、割り当てられていない場合は、VLAN ID がサービス要求に割り当てられます。VLAN ID がプール内にあり、すでに使用されている場合、Prime Provisioning は、別の VLAN ID を割り当てるよう求めるプロンプトを表示します。VLAN ID が Prime Provisioning VLAN ID プールの外にある場合は、Prime Provisioning は、VLAN ID が割り当てられているかどうかの確認を実行しません。オペレータは、VLAN ID が使用可能であることを確認する必要があります。

ステップ 14　サービス要求の作成中に、デュアルホーム接続リングのセカンダリ N-PE に対してブリッジ ドメインの VLAN ID を自動選択するように Prime Provisioning を設定するには、[AutoPick Bridge Domain/VLAN ID Secondary N-PE] 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フにする場合は、セカンダリ N-PE のセカンダリ ブリッジ ドメイン VLAN ID を指定する必要があります（次の手順を参照）。

使用方法に関する注釈：

- この属性は、デュアル ホーム接続リング（2 つの異なる N-PE で終端するリング）の場合にのみ適用できます。Prime Provisioning では、セカンダリ N-PE 用に別個のブリッジ ドメイン VLAN ID を使用することがサポートされます。
- デュアル ホーム接続リングでは、2 つの N-PE が異なるアクセス ドメインに存在する場合、Prime Provisioning はプライマリとセカンダリの両方の N-PE アクセス ドメインからブリッジ ドメイン VLAN ID を割り当てます。両方が同一のアクセス ドメイン内にある場合、Prime Provisioning は共通の VLAN ID をこれらが属するアクセス ドメインから割り当てます。
- AutoPick ブリッジ ドメイン/VLAN ID セカンダリ N-PE は、デバイスでグローバル VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。
- この属性は IOS XR デバイスでは表示されません。

ステップ 15　[AutoPick Bridge Domain/VLAN ID Secondary N-PE] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID Secondary N-PE] フィールドに適切な値を入力します。

ステップ 16　ポリシーを使用して作成されたサービス要求を、着信フレームの内部 VLAN タグと外部 VLAN タグの両方と一致させるには、[Match Inner and Outer Tags] 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しないと、ポリシーを使用して作成されたサービス要求は、着信フレームの外部 VLAN タグだけと一致します。

[Match Inner and Outer Tags] 属性をオンにすると、[Inner VLAN ID] フィールドと [Outer VLAN ID] フィールド（次のステップで説明）が表示されます。

ステップ 17　[Match Inner and Outer Tags] チェックボックスをオンにする場合は、[Inner VLAN ID] フィールドと [Outer VLAN ID] フィールドに内部 VLAN タグと外部 VLAN タグを入力します。

使用方法に関する注釈：

- 単一の値、単一の範囲、複数の値、複数の範囲、またはこれらの組み合わせを指定できます。次に、例を示します。
  - 10
  - 10, 15,17
  - 10-15
  - 10-15,17-20
  - 10,20-25
- ポリシーで [Inner VLAN Ranges] 属性を true に設定すると、[Inner VLAN ID] フィールドは、内部 VLAN タグの範囲を使用できます。
- ポリシーで [Outer VLAN Ranges] 属性を true に設定すると、[Outer VLAN ID] フィールドは、外部 VLAN タグの範囲を使用できるようになります。

ステップ 18　[Match Inner and Outer Tags] チェックボックスをオフにする場合は、[Outer VLAN ID] フィールドに外部 VLAN タグを入力します。

（注）　[Outer VLAN ID] で指定した VLAN は、カスタマー側の UNI を含め、残りの L2 アクセス ノード（リンクにある場合）でプロビジョニングされます。

（注）　また、次の手順で説明されているように、Prime Provisioning が外部 VLAN ID を自動選択するように設定することもできます。

ステップ 19　以前に作成した外部 VLAN ID リソース プールから外部 VLAN ID を Prime Provisioning が自動選択するように設定するには、[AutoPick Outer VLAN] 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フにすると、オペレータは外部 VLAN ID を指定するように求められます。

（注）　[AutoPick Outer VLAN] 属性を使用するには、2 つの要素が Prime Provisioning で事前に設定されている必要があります。1 つめの要素はインターフェイス アクセス ドメインであり、これは N-PE デバイスの物理ポートをグループ化する論理要素です。2 つめの要素は EVC 外部 VLAN リソース プールであり、これはインターフェイス アクセス ドメインによって使用されます。これらの要素を設定する方法については、項「リソースの設定」（P.2-42）と「リソース プール」（P.2-46）を参照してください。

使用方法に関する注釈：

- [AutoPick Outer VLAN] は、EVC 機能をサポートするインターフェイスに使用できます。
- [AutoPick Outer VLAN] は、EVC をサポートするインターフェイスで VLAN ID をコンシュームします。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 20　ウィンドウの [VLAN Rewrite] セクションで、ドロップダウン リストから [Rewrite Type] を選択します。

選択できる基準は、次のとおりです。

- Pop
- Push
- Translate

GUI の後続の属性は、次のステップで説明するように、[Rewrite Type] の選択によって変わります。

ステップ 21　[Pop] が [Rewrite Type] である場合は、次の 2 つのチェックボックスが表示されます。

a.　一致基準を満たす着信フレームの外部 VLAN ID タグをポップするには、[Pop Outer Tag] 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フにすると、着信トラフィックの外部タグはポップされません。

b.　一致基準を満たす着信フレームの内部 VLAN ID タグをポップするには、[Pop Inner Tag] 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フにすると、内部タグは変更されません。

[Pop Inner Tag] をオンにすると、[Pop Outer Tag] が自動的にオンになることに注意してください。

ステップ 22　[Push] が [Rewrite Type] である場合は、次の 2 つのテキスト ボックスが表示されます。

a.　テキスト ボックス [Outer VLAN ID] に、一致基準を満たす着信フレームにインポーズされる外部 VLAN ID タグを入力します。この設定で作成されるサービス要求はすべて、一致基準と一致する着信フレームで dot1q 外部タグをプッシュします。値が指定されていない場合は、プッシュ操作は無視され、デバイスで設定されません。

b.　テキスト ボックス [Inner VLAN ID] に、一致基準を満たす着信フレームにインポーズされる内部 VLAN ID タグを入力します。この設定で作成されるサービス要求はすべて、一致基準と一致する着信フレームで dot1q 内部タグをプッシュします。内部 VLAN タグは、外部 VLAN タグなしではプッシュできません。つまり、内部 VLAN タグを適用する場合は、外部 VLAN タグも定義する必要があります。

ステップ 23　[Translate] が [Rewrite Type] である場合は、[Translation Type] ドロップダウン リストが表示されます。

このリストで選択可能な項目は、[Match Inner and Outer Tags] 属性の設定（前のステップで設定）によって異なります。

a. [Match Inner and Outer Tags] チェックボックスをオンにする（true）場合は、[Translation Type] ドロップダウン リストから変換タイプとして [1:1]、[1:2]、[2:1]、または [2:2] を選択します。

- [1:1] または [2:1] を選択する場合は、表示される [Outer VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。
- [1:2] または [2:2] を選択する場合は、表示される [Outer VLAN ID] および [Inner VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグと内部タグがこれらの ID に変換されます。

b. [Match Inner and Outer Tags] チェックボックスをオフにする（false）場合は、[Translation Type] ドロップダウン リストから変換タイプとして [1:1] または [1:2] を選択します。

- [1:1] を選択する場合は、表示される [Outer VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグがこの ID に変換されます。
- [1:2] を選択する場合は､表示される [Outer VLAN ID] および [Inner VLAN ID] テキスト ボックスに値を入力します。一致基準を満たすすべての着信フレームの外部タグと内部タグがこれらの ID に変換されます。

ステップ 24　[Next] をクリックして、[EVC Details] ウィンドウの設定内容を保存します。

[Standard UNI Details] ウィンドウが表示されます。

ステップ 25　次のステップで、標準 UNI リンク属性の設定に進みます。

標準 UNI 属性の編集

次のステップでは、[Standard UNI Details] ウィンドウの属性の設定について説明します。EVC リンクとして設定されていないリンクの場合（[Service Request Details] ウィンドウで [EVC] チェックボックスをオンにしなかった場合）、リンク属性の編集はこのウィンドウから開始します。

（注）　[Standard UNI Details] ウィンドウに表示される属性は、Prime Provisioning によって動的に設定されます。下記のステップで説明する属性の一部は、ポリシーとサービス要求設定またはリンク タイプによっては、ウィンドウに表示されないことがあります。たとえば、EVC ポリシーの MPLS コア接続タイプがローカルの場合は、疑似回線関連の属性は表示されません。また、リンクを EVC または非 EVC として設定すると、ウィンドウに表示される属性が変わります。さらに、属性は、デバイス タイプ（IOS または IOS XR）に基づいてフィルタリングされます。これらのケースは、参照用としてステップに示されています。

ステップ 26　[N-PE/U-PE Information] フィールドと [Interface Name] フィールドには、前のステップで選択した PE デバイスとインターフェイス名が表示されます。

このフィールドは読み取り専用です。

ステップ 27　ドロップダウン リストから**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- [DOT1QTRUNK] : 802.1q カプセル化によって UNI をトランクとして設定します。UNI が直接接続された EVC リンクに属している場合、この設定は、着信フレームが 802.1q カプセル化され、リンクに設定された VLAN ID と一致することを意味します。この固有のトポロジには、トランク UNI 自体は含まれていません。
- [DOT1QTUNNEL] : UNI を 802.1q トンネル（dot1q トンネルまたは Q-in-Q とも呼ばれています）ポートとして設定します。
- [ACCESS] : UNI をアクセス ポートとして設定します。

この属性では、サービスの異なるリンクにさまざまなタイプの UNI カプセル化を導入できます。

使用方法に関する注釈：

- EVC がイネーブルになっている直接接続リンクの場合（[EVC Service Request Editor] ウィンドウの [EVC] チェックボックスをオンにした場合）、カプセル化タイプとして選択できるのは、[DOT1Q] と [DEFAULT] です。

ステップ 28　必要に応じて、[PE/UNI Interface Description] フィールドにインターフェイスの説明を入力します。

ステップ 29　サービスのアクティブ化中（たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化する場合）に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。

ステップ 30　適切なオプション ボタンをクリックして、サービス要求の [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No] : VLAN 変換は実行されません （デフォルト）。
- [1:1] : 1:1 VLAN 変換。
- [2:1] : 2:1 VLAN 変換。
- [1:2] : 1 対 2 VLAN 変換。
- [2:2] : 2 対 2 VLAN 変換。

使用方法に関する注釈：

- 直接接続リンクの場合、[EVC] チェックボックスがオンになっているときは、[VLAN Translation] 属性は表示されません。これは次の組み合わせの場合は表示されます。
  - 直接接続リンクで、[EVC] チェックボックスがオフになっている場合。
  - L2 アクセス ノードで、[EVC] チェックボックスがオンまたはオフになっている場合。
- [No] 以外の選択肢を選ぶと、他のフィールドが GUI に表示されます。これらは、設定に基づいて指定できます。
  - [CE VLAN] : 1 ～ 4096 までの値を入力します。
  - [Auto Pick] : このチェックボックスをオンにすると、Prime Provisioning は VLAN リソース プールから外部 VLAN を自動選択するようになります。
  - [Outer VLAN] : [Auto Pick] がオフの場合、1 ～ 4096 までの値を指定します。
  - [Select where 2:1 or 2:2 translation takes place] : 2 対 1 または 2 対 2 の VLAN 変換が行われるデバイスを指定します。[Auto] を選択すると、UNI ポートに最も近いデバイスで VLAN 変換が行われます。
- VLAN 変換、すべての標準 UNI、およびポート セキュリティ属性は、L2 アクセスとのリンクに適用できます。UNI が N-PE にある場合は、これらの属性は表示されません。
- VLAN 変換が U-PE または PE-AGG デバイスで行われると、VLAN 変換のコマンドが選択したデバイスの NNI インターフェイスに設定されます。VLAN 変換が NP-E で行われると、VLAN 変換のコマンドがデバイスの UNI インターフェイスに設定されます。
- リング ベースの環境に 2 つの NNI インターフェイスがある場合、VLAN 変換は両方の NNI インターフェイスに適用されます。
- 1 対 1 および 2 対 1 の VLAN 変換は、非 EVC（スイッチポート ベースの N-PE の構文）終端の接続回線と同じ構文でサポートされます。

ステップ 31　Prime Provisioning に SVI（スイッチ仮想インターフェイス）でフォワーディング コマンドを生成させるには、[N-PE Pseudo-wire on SVI] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフになっています。この場合、Prime Provisioning は、サービス インスタンスでフォワーディング コマンドを生成します。

EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（これは、[EVC Service Request Editor] ウィンドウのサービス要求ワークフローで使用可能）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

使用方法に関する注釈：

- EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（[EVC Service Request Editor] ウィンドウ内）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で scanned を使用して作成されません。
- Prime Provisioning では、EVC サービス要求のハイブリッド設定がサポートされます。ハイブリッド設定では、接続回線のいずれかの側のフォワーディング コマンド（scanned など）は、サービス インスタンスで設定でき、接続回線のもう一方の側の xconnect 設定は、スイッチ仮想インターフェイス（SVI）で設定できます。
- [N-PE Pseudo-wire on SVI] は、すべての接続タイプ（[PSEUDOWIRE] または [LOCAL]）に適用できますが、ハイブリッド SVI 設定は疑似回線接続だけで可能です。
- [MPLS Core Connectivity Type] が [LOCAL] 接続タイプに設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にディセーブルにされます。
- これらのケースの例については、コンフィグレットの例 「EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）」（P.3-222）と「EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）」（P.3-223）を参照してください。
- [N-PE Pseudo-wire on SVI] 属性の追加情報については、「インターフェイス属性の設定」（P.3-30）の項にある EVC ポリシーの章で対応するカバレッジを参照してください。
- [N-PE Pseudo-wire on SVI] 属性は、IOS XR デバイスではサポートされません。すべての xconnect コマンドは、L2 サブインターフェイスまたはサービス インスタンスで設定されます。

ステップ 32　疑似回線クラスの選択を可能にするには、[Use Existing PW Class] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- [Use Existing PW Class] をオンにすると、追加の属性 [Existing PW Class Name] が GUI に表示されます。デバイスにすでに存在する疑似回線クラスの名前を入力します。
- [Use Existing PW Class] をオンにすると、[PW Tunnel Selection] および [Interface Tunnel] 属性はウィンドウで非表示になります。これは、Prime Provisioning が疑似回線クラスを生成しないようにするためです。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「疑似回線コア接続」（P.3-38）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。

ステップ 33　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] 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：

- [PW Tunnel Selection] チェックボックスをオンにすると、[Interface Tunnel] 属性フィールド（次のステップを参照）がアクティブになります。

- この属性は、EVC ポリシーで MPLS コア接続タイプが疑似回線として設定されている場合にのみ表示されます。

ステップ 34　[PW Tunnel Selection] チェックボックスをオンにした場合は、[Interface Tunnel] テキスト フィールドに TE トンネル ID を入力します。

Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。サービス要求の作成中に、Prime Provisioning はトンネル ID 番号の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 35　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR デバイスで pw-class コマンドをプロビジョニングするために使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「サービス オプションの設定」（P.3-22）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。

ステップ 36　サービス要求の作成中に、Prime Provisioning にブリッジ グループ名を自動選択させるには、[AutoPick Bridge Group Name] 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フにすると、サービス要求の作成中にブリッジ グループ名を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- この属性は、IOS XR デバイスだけで表示されます。
- [AutoPick Bridge Group Name] チェックボックスをオフにする場合は、[Bridge Group Name] テキスト フィールドにブリッジ グループ名を入力します。

ステップ 37　サービス要求の作成中に Prime Provisioning に VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにすると、サービス要求の作成中に VLAN ID を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。
- [AutoPick Bridge Domain/VLAN ID] 属性は、Cisco 7600 と ASR 9000 の両方のデバイスで表示されます。これは、非 EVC リンクについてのみ表示されます。

ステップ 38　[AutoPick Bridge Domain/VLAN ID] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID] テキスト フィールドに ID 番号を入力します。

使用方法に関する注釈：

- [AutoPick Bridge Domain/VLAN ID] をオンにすると、このフィールドは編集できません。
- VLAN ID を手動で割り当てる場合は、Prime Provisioning は、Prime Provisioning の VLAN ID プール内にあるかどうかを確認するために VLAN ID を調べます。VLAN ID がプール内にあっても、割り当てられていない場合は、VLAN ID がサービス要求に割り当てられます。VLAN ID がプール内にあり、すでに使用されている場合、Prime Provisioning は、別の VLAN ID を割り当てるよう求めるプロンプトを表示します。VLAN ID が Prime Provisioning VLAN ID プールの外にある場合は、Prime Provisioning は、VLAN ID が割り当てられているかどうかの確認を実行しません。オペレータは、VLAN ID が使用可能であることを確認する必要があります。
- [Bridge Domain/VLAN ID] テキスト フィールドは、Cisco 7600 と ASR 9000 の両方のデバイスで表示されます。これは、非 EVC リンクについてのみ表示されます。

ステップ 39　[L2VPN Group Name] では、ドロップダウン リストから次のいずれかを選択します。

- ISC
- VPNSC

使用方法に関する注釈：

- この属性は、IOS XR デバイスで L2VPN グループ名をプロビジョニングするために使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

- [L2VPN Group Name] は、IOS XR デバイスだけに適用されます。

ステップ 40　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

使用方法に関する注釈：

- [E-Line Name] に値を指定しない場合は、Prime Provisioning は、次のようにデフォルト名を自動生成します。
  - [PSEUDOWIRE] コア接続タイプの場合は、次の形式になります。
    DeviceName--VC_ID
  - [LOCAL] コア接続タイプの場合は、次の形式になります。
    DeviceName--VLAN_ID

  デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。
- [E-Line Name] は、IOS XR デバイスだけに適用されます。

ステップ 41　標準 UNI 設定を保存し、[EVC SR] ウィンドウに戻るには、[OK] をクリックします。

[Link Attributes] 列の値は、リンク設定が更新されたことを意味する [Changed] と表示されるようになります。[Changed] リンクをクリックして、[Standard UNI Details] ウィンドウの設定を変更することで、今後リンク属性を編集できるようになります。

リンク属性の編集に関する詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

ステップ 42　別のリンクを追加するには、[Add] ボタンをクリックして、この項の前のステップと同様に新しいリンクの属性を設定します。

ステップ 43　リンクを削除するには、そのリンクの行の最初の列でチェックボックスをオンにして、[Delete] ボタンをクリックします。

ステップ 44　このサービス要求の L2 アクセス ノードとのリンクを設定する場合は、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）を参照してください。

ステップ 45　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、EVC サービス要求を作成します。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

ATM リンク属性の設定

ここでは、直接接続リンクを ATM リンクとして設定する方法について説明します。

ATM リンクを設定するには、次の手順を実行します。

ステップ 1　[EVC Service Request Editor] ウィンドウの [Direct Connect Links] セクションで、ATM リンクを設定するデバイスを指定します。

ステップ 2　UNI の ATM インターフェイスを選択します。

（注）　ATM インターフェイスは、EVC サービス要求が ATM-Ethernet インターワーキング ポリシー タイプに基づいている場合に限り、[UNI] 列のインターフェイス選択機能に表示されます。

ATM インターフェイスを選択すると、[EVC] 列のチェックボックスは動的に GUI から非表示になります。

ステップ 3　[Link Attributes] 列で、ATM リンクを追加するデバイスの [Edit] リンクをクリックします。

[ATM UNI Details] ウィンドウが表示されます。

[ATM UNI Details] ウィンドウのフィールドはすべて、ポリシー設定に基づいてイネーブルにされます。

ステップ 4　ドロップダウン リストから [Transport Mode] を選択します。

選択できる基準は、次のとおりです。

- [VP]：仮想パス モード。これはデフォルトです。
- [VC]：仮想回線モード。

ステップ 5　ドロップダウン リストから [ATM Encapsulation] を選択します。

- AAL5SNAP

ステップ 6　ATM Virtual Channel Descriptor（VCD; 仮想チャネル記述子）またはサブインターフェイス番号を指定するには、[ATM VCD/Sub-Interface #] フィールドに値を入力します。

指定できる値は 1 ～ 2147483647 です。

ステップ 7　ATM Virtual Path Identifier（VPI; 仮想パス識別子）を指定するには、[ATM VPI] フィールドに値を入力します。

指定できる値は 0 ～ 255 です。

ステップ 8　ATM Virtual Channel Identifier（VCI; 仮想チャネル識別子）を指定するには、[ATM VCI] フィールドに値を入力します。

指定できる値は 32 ～ 65535 です。

ステップ 9　サービスのアクティブ化中（たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化する場合）に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。

ステップ 10　疑似回線クラスの選択を可能にするには、[Use Existing PW Class] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- [Use Existing PW Class] をオンにすると、追加の属性 [Existing PW Class Name] が GUI に表示されます。デバイスにすでに存在する疑似回線クラスの名前を入力します。
- [Use Existing PW Class] をオンにすると、[PW Tunnel Selection] および [Interface Tunnel] 属性はウィンドウで非表示になります。これは、Prime Provisioning が疑似回線クラスを生成しないようにするためです。
- [Use PseudoWireClass] 属性は、[Service Options] ウィンドウで [MPLS Core Connectivity Type] が [PSEUDOWIRE] に設定されていた場合だけ使用可能です（「疑似回線コア接続」（P.3-38）を参照）。
- [Use PseudoWireClass] は、IOS XR デバイスだけで適用可能です。

ステップ 11　Prime Provisioning に SVI（スイッチ仮想インターフェイス）でフォワーディング コマンドを生成させるには、[N-PE Pseudo-wire on SVI] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフになっています。この場合、Prime Provisioning は、サービス インスタンスでフォワーディング コマンドを生成します。

EVC リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（これは、[EVC Service Request Editor] ウィンドウのサービス要求ワークフローで使用可能）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE Pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。

使用方法に関する注釈：

- ATM リンクでは、属性 [N-PE Pseudo-wire on SVI] は、属性 [Configure with Bridge Domain]（[EVC Service Request Editor] ウィンドウ内）の値によって決まります。[N-PE Pseudo-wire on SVI] は、イネーブルにすると、[Configure with Bridge Domain] が [true] に設定されている場合にだけ反映されます。それ以外の場合は、[N-PE pseudo-wire on SVI] がイネーブルになっていても、サービス要求は SVI で xconnect を使用して作成されません。
- Prime Provisioning では、EVC サービス要求のハイブリッド設定がサポートされます。ハイブリッド設定では、接続回線のいずれかの側のフォワーディング コマンド（xconnect など）は、サービス インスタンスで設定でき、接続回線のもう一方の側の xconnect 設定は、スイッチ仮想インターフェイス（SVI）で設定できます。
- [N-PE Pseudo-wire on SVI] は、すべての接続タイプ（[PSEUDOWIRE] または [LOCAL]）に適用できますが、ハイブリッド SVI 設定は疑似回線接続だけで可能です。
- [MPLS Core Connectivity Type] が [LOCAL] 接続タイプに設定されている場合は、[N-PE Pseudo-wire on SVI] 属性は、ポリシーとサービス要求で常にディセーブルにされます。
- これらのケースの例については、コンフィグレットの例 「EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）」（P.3-222）と「EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）」（P.3-223）を参照してください。
- [N-PE Pseudo-wire on SVI] 属性の追加情報については、「インターフェイス属性の設定」（P.3-30）の項にある EVC ポリシーの章で対応するカバレッジを参照してください。

- [N-PE Pseudo-wire on SVI] 属性は、IOS XR デバイスではサポートされません。すべての xconnect コマンドは、L2 サブインターフェイスまたはサービス インスタンスで設定されます。

ステップ 12　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] 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：

- [PW Tunnel Selection] チェックボックスをオンにすると、[Interface Tunnel] 属性フィールド（次のステップを参照）がアクティブになります。
- この属性は、EVC ポリシーで MPLS コア接続タイプが疑似回線として設定されている場合にのみ表示されます。

ステップ 13　[PW Tunnel Selection] チェックボックスをオンにした場合は、[Interface Tunnel] テキスト フィールドに TE トンネル ID を入力します。

Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。サービス要求の作成中に、Prime Provisioning はトンネル ID 番号の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 14　サービス要求の作成中に Prime Provisioning に VLAN ID を自動選択させるには、[AutoPick Bridge Domain/VLAN ID] 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フにすると、サービス要求の作成中に VLAN ID を指定するようプロンプトが表示されます（次のステップを参照）。

使用方法に関する注釈：

- AutoPick ブリッジ ドメインまたは VLAN ID は、デバイスでグローバル VLAN ID を消費します。
- ブリッジ ドメイン VLAN ID は既存の Prime Provisioning VLAN プールから選択されます。

ステップ 15　[AutoPick Bridge Domain/VLAN ID] チェックボックスをオフにする場合は、[Bridge Domain/VLAN ID] テキスト フィールドに ID 番号を入力します。

使用方法に関する注釈：

- [AutoPick Bridge Domain/VLAN ID] をオンにすると、このフィールドは編集できません。
- VLAN ID を手動で割り当てる場合は、Prime Provisioning は、Prime Provisioning の VLAN ID プール内にあるかどうかを確認するために VLAN ID を調べます。VLAN ID がプール内にあっても、割り当てられていない場合は、VLAN ID がサービス要求に割り当てられます。VLAN ID がプール内にあり、すでに使用されている場合、Prime Provisioning は、別の VLAN ID を割り当てるよう求めるプロンプトを表示します。VLAN ID が Prime Provisioning VLAN ID プールの外にある場合は、Prime Provisioning は、VLAN ID が割り当てられているかどうかの確認を実行しません。オペレータは、VLAN ID が使用可能であることを確認する必要があります。

ステップ 16　[ATM UNI Details] 設定を保存し、[EVC Service Request Editor] ウィンドウに戻るには、[OK] をクリックします。

[Link Attributes] 列の値は、リンク設定が更新されたことを意味する [Changed] と表示されるようになります。[Changed] リンクをクリックして、[Standard UNI Details] ウィンドウの設定を変更することで、今後リンク属性を編集できるようになります。

リンク属性の編集に関する詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

ステップ 17　別のリンクを追加するには、[Add] ボタンをクリックして、この項の前のステップと同様に新しいリンクの属性を設定します。

ステップ 18　リンクを削除するには、そのリンクの行の最初の列でチェックボックスをオンにして、[Delete] ボタンをクリックします。

ステップ 19　このサービス要求の L2 アクセス ノードとのリンクを設定する場合は、「L2 アクセス ノードとのリンクの設定（疑似回線とローカル接続のみ）」（P.3-55）を参照してください。

ステップ 20　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、EVC サービス要求を作成します。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

L2 アクセス ノードとのリンクの設定

[EVC Service Request Editor] ウィンドウの [Links with L2 Access Nodes] セクションでは、L2（イーサネット）アクセス ノードとのリンクを設定できます。これらは、（CE に向かった）N-PE 以外に L2/イーサネット アクセス ノードがある点を除き、直接接続リンクと類似しています。そのため、NPC が必要です。

（注）　ATM リンクは、L2 アクセス ノードではサポートされません。ATM リンクは、直接接続リンクとして設定する必要があります。詳細については、「ATM リンク属性の設定」（P.3-90）を参照してください。

L2 アクセス ノードとのリンクを設定するためのステップは、「直接接続リンクの設定」（P.3-44）の項に記載されているステップと似ています。次の共通する操作の詳細なステップについては、この項を参照してください。

- リンクの追加と削除。
- N-PE の選択。
- UNI インターフェイスの選択。
- EVC リンクとしてのリンクの設定。
- 標準および EVC リンク属性の編集。

L2 アクセスとのリンクの設定における主な違いは、NPC の詳細の指定です。

L2 アクセス ノードとのリンクに NPC 詳細を設定するには、次の手順を実行します。

ステップ 1　NPC を使用してリンクを追加するプロセスの最初のステップは、N-PE ではなく U-PE/PE-AGG デバイスを選択することです。

選択したインターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Details] 列に自動入力される場合は、明示的に選択する必要はありません。

複数の NPC が使用可能な場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。[NPC] ウィンドウが表示され、適切な NPC を選択できます。

ステップ 2　[OK] をクリックします。

PE とインターフェイスを選択するたびに、この PE とインターフェイスから設定した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。[NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

ステップ 3　リンク属性の編集、リンクの追加と削除、[EVC] チェックボックスの使用については、「直接接続リンクの設定」（P.3-44）の項の対応する手順を参照してください。

ステップ 4　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、EVC サービス要求を作成します。

属性が欠落しているか、誤って設定されていると、Prime Provisioning は、ウィンドウの左下に警告を表示します。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「EVC サービス要求の変更」（P.3-57）の項を参照してください。EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

EVC サービス要求の変更

リンクまたはサービス要求の他の設定を変更する必要がある場合は、EVC サービス要求を変更できます。

EVC サービス要求を変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

[Service Request Manager] ウィンドウが表示され、Prime Provisioning で使用可能なサービス要求が示されます。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

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

ステップ 4　必要に応じて、属性を変更します。

このウィンドウでの属性の設定に関する詳細なカバレッジについては、「サービス要求の詳細の設定」（P.3-38）で始まる項を参照してください。

（注）　VC ID、VPLS VPN ID、および VLAN ID は、サービス要求で設定した後は変更できません。

ステップ 5　テンプレートまたはデータ ファイルを接続回線に追加するには、「EVC イーサネット 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」（P.3-57）の項を参照してください。

ステップ 6　EVC サービス要求の編集が終了したら、[Save] をクリックします。

EVC サービス要求の保存に関する追加情報については、「EVC サービス要求の保存」（P.3-58）を参照してください。

EVC 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

Prime Provisioning では、アプリケーションによって管理されるデバイスで使用可能なすべての CLI コマンドの設定はサポートされません。そのようなコマンドをデバイス上で設定するために、Prime Provisioning Template Manager 機能を使用できます。テンプレートは、デバイス ロール単位でポリシー レベルで関連付けることができます。サービス要求レベルでのテンプレートの上書きは、ポリシーレベルの設定でオペレータに許可されている場合は行うことができます。

サービス要求でテンプレートとデータ ファイルを関連付けるには、[EVC Service Request Editor] ウィンドウで任意のリンクを選択して、ウィンドウの下部にある [Template] ボタンをクリックします。

（注）　関連付けられたポリシーでテンプレート機能が使用可能になっていない場合は、[Template] ボタンは選択できません。

[SR Template Association] ウィンドウが表示されます。このウィンドウでは、デバイス単位レベルでテンプレートを関連付けることができます。

[Template Association] ウィンドウには、リンクを構成するデバイス、デバイス ロール、およびデバイスに関連付けられている 1 つ以上のテンプレートとデータ ファイルが一覧表示されます。この場合は、テンプレートまたはデータ ファイルはまだ設定されていません。

テンプレートとデータ ファイルをサービス要求に関連付ける方法に関する詳細については、「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。

EVC サービス要求の保存

EVC サービス要求を保存するには、次の手順を実行します。

ステップ 1　EVC サービス要求の属性の設定が終了したら、[Save] をクリックして、サービス要求を作成します。

EVC サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウが表示されます

新しく作成された EVC サービス要求が [REQUESTED] の状態で追加されます。

ステップ 2　ただし、何らかの理由で（たとえば、選択した値が範囲外である）EVC サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。

そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

ステップ 3　EVC サービス要求を展開する準備ができたら、「サービス要求の展開」（P.8-10）を参照してください。

L2VPN ポリシーの作成

この項では、L2VPN ポリシーの基本的な作成手順について説明します。具体的な内容は、次のとおりです。

- 「CE が存在しないイーサネット EWS（EPL）ポリシーの定義」（P.3-112）
- 「CE が存在するフレーム リレー ポリシーの定義」（P.3-117）
- 「CE が存在しないフレーム リレー ポリシーの定義」（P.3-119）
- 「CE が存在する ATM ポリシーの定義」（P.3-121）
- 「CE が存在しない ATM ポリシーの定義」（P.3-123）

L2VPN ポリシーの定義

Prime Provisioning サービスをプロビジョニングするには、L2VPN ポリシーを定義する必要があります。L2VPN ポリシーは、エンドツーエンド ワイヤ属性と Attachment Circuit（AC; 接続回線）属性で共有される共通特性を定義します。

ポリシーは、L2VPN サービス要求の定義に必要な大部分のパラメータのテンプレートです。定義後に、共通する一連の特性を共有するすべての L2VPN サービス要求で L2VPN ポリシーを使用できます。新しいタイプのサービスまたは異なるパラメータを持つサービスを作成する場合は、常に新しい L2VPN ポリシーを作成します。L2VPN ポリシーの作成は通常、経験のあるネットワーク エンジニアが実行します。

ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。[Editable] チェックボックスを使用すると、ネットワーク オペレータはフィールドを編集可能にできます。値が [editable] に設定されている場合は、サービス要求の作成者は、特定のポリシー項目のその他の有効値を変更できます。値が [editable] に設定*されていない*場合、サービス要求作成者は、ポリシー項目を変更できません。

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 ファイルの使用方法の詳細については、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。

L2VPN ポリシーの 4 つの主要カテゴリは、L2VPN が提供する次の 4 つの主要サービスに対応します。

- ポイントツーポイント Ethernet Relay Service（ERS）。このサービスの Metro Ethernet Forum（MEF）名は、Ethernet Virtual Private Line（EVPL）です。このマニュアルで L2VPN サービスを示すために使用される用語の詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* の「L2VPN Concepts」の章にある「Layer 2 Terminology Conventions」を参照してください。
- ポイントツーポイント Ethernet Wire Service（EWS）。このサービスの MEF 名は、Ethernet Private Line（EPL）です。
- Frame Relay over MPLS（FRoMPLS）
- ATM over MPLS（ATMoMPLS）

Prime Provisioning で L2VPN ポリシーを定義するには、次のステップを実行します。

ステップ 1　[Service Design] > [Create Policy] 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　[Policy Type] ドロップダウン リストから [L2VPN] 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　L2VPN ポリシーの [Policy Name] を入力します。

ステップ 4　L2VPN ポリシーの [Policy Owner] を選択します。

L2VPN 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：すべてのサービス オペレータがこの L2VPN 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 L2VPN ポリシーは、このカスタマー所有ポリシーでの作業を許可されるオペレータだけが表示できます。

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。

ステップ 5　L2VPN ポリシーの所有者を選択するには、[Select] をクリックします

([Global ownership] を選択した場合は、[Select] 機能は使用不可です)。[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 6　L2VPN ポリシーの [Service Type] を選択できます。

L2VPN ポリシーには 4 つのサービス タイプがあります。

- L2VPN ERS（EVPL）
- L2VPN EWS（EPL）
- フレーム リレー
- ATM

後続の項では、これらの各サービスのポリシーの設定について説明します。

ステップ 7　Prime Provisioning に、サービスのアクティブ化中に CE ルータとインターフェイスを提供するよう、この L2VPN ポリシーを使用するサービス オペレータに求めさせる場合は、[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は、Prime Provisioning は、サービスのアクティブ化中に、U-PE または N-PE ルータとカスタマー側インターフェイスだけをサービス オペレータに求めます。

ステップ 8　[Next] をクリックします。

次に、CE が存在する場合と存在しない場合のサービス タイプのポリシーの設定例を示します。

CE が存在するイーサネット ERS（EVPL）ポリシーの定義

ここでは、CE が存在するイーサネット ERS（EVPL）ポリシーの定義について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [L2VPN ERS] を選択します。

ステップ 2　[CE Present] チェックボックスをオンにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

（注）　[Standard UNI Port] 属性は、IOS XR が実行されている N-PE デバイス上に UNI がある場合は、このポリシーに基づくサービス要求内では使用不可です。

ステップ 5　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、U-PE または N-PE インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、L2VPN サービス要求の作成中にオペレータが表示できるインターフェイス タイプを制限するためのフィルタとして機能します。

ステップ 6　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 10　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 11　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 12　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 13　Prime Provisioning に VC ID を選択させる場合は、[VC ID AutoPick] 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しない場合は、サービスのアクティブ化中に [VC ID] フィールドで VC ID を指定するよう求めるプロンプトが表示されます。

ステップ 14　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。

ステップ 15　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 16　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 17　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。**p2p** 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 18　[Link Media] タイプ（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

使用方法に関する注釈：

- デフォルトは [None] です。
- この属性の使用時に、新しい CLI が、メディア タイプを定義するために UNI インターフェイスで生成されます。
- [Link Media] 属性は、ME3400 プラットフォームだけでサポートされます。

ステップ 19　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 20　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 24　**UNI ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

（注）　カプセル化タイプが [DEFAULT] の場合に限り、[UNI Port Type] に入力します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　OSM カードのスイッチ仮想インターフェイスで疑似回線接続を設定するには、[N-PE Pseudo-wire On SVI] 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は、デフォルトでオンになっています。チェックボックスをオフにすると、疑似回線は、PFC カードのサブインターフェイス（使用可能な場合）でプロビジョニングされます。このオプションは、C76xx デバイスだけで使用可能です。

（注）　[N-PE Pseudo-wire on SVI] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 28　適切なオプション ボタンをクリックして、このポリシーの [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No]：VLAN 変換は実行されません （デフォルト）。
- [1:1]：1:1 VLAN 変換。
- [2:1]：2:1 VLAN 変換。

（注）　VLAN 変換の設定の詳細なカバレッジについては、「L2VPN ERS（EVPL）サービスの VLAN 変換の設定」（P.3-180）を参照してください。

ステップ 29　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

（注）　[PW Tunnel Selection] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 30　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 31　[Finish] をクリックします。

CE が存在しないイーサネット ERS（EVPL）ポリシーの定義

ここでは、CE が存在しないイーサネット ERS（EVPL）ポリシーの定義について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [L2VPN ERS] を選択します。

ステップ 2　[CE Present] チェックボックスをオフにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ドロップダウン リストから N-PE/U-PE **インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、または U-PE インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、L2VPN サービス要求の作成中にオペレータが表示できるインターフェイス タイプを制限するためのフィルタとして機能します。

ステップ 5　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

（注）　[Standard UNI Port] 属性は、IOS XR が実行されている N-PE デバイス上に UNI がある場合は、このポリシーに基づくサービス要求内では使用不可です。

ステップ 6　PE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 10　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 11　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 12　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 13　Prime Provisioning に VC ID を選択させる場合は、[VC ID AutoPick] 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しない場合は、サービスのアクティブ化中に [VC ID] フィールドで VC ID を指定するよう求めるプロンプトが表示されます。

ステップ 14　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 15　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 16　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 17　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。

ステップ 18　[Link Media] タイプ（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

使用方法に関する注釈：

- デフォルトは [None] です。
- この属性の使用時に、新しい CLI が、メディア タイプを定義するために UNI インターフェイスで生成されます。
- [Link Media] 属性は、ME3400 プラットフォームだけでサポートされます。

ステップ 19　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 20　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフであり、[UNI MAC addresses]（下記を参照）に入力した値に基づいて、Prime Provisioning は MAC ベースの ACL を自動的にカスタマー向きの UNI ポートに割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 24　**UNI ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

（注）　カプセル化タイプが [DEFAULT] の場合に限り、[UNI Port Type] に入力します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　OSM カードのスイッチ仮想インターフェイスで疑似回線接続を設定するには、[N-PE Pseudo-wire On SVI] 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は、デフォルトでオンになっています。チェックボックスをオフにすると、疑似回線は、PFC カードのサブインターフェイス（使用可能な場合）でプロビジョニングされます。このオプションは、C76xx デバイスだけで使用可能です。

（注）　[N-PE Pseudo-wire On SVI] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 28　適切なオプション ボタンをクリックして、このポリシーの [VLAN Translation] のタイプを指定します。

選択できる基準は、次のとおりです。

- [No] : VLAN 変換は実行されません （デフォルト）。
- [1:1] : 1:1 VLAN 変換。
- [2:1] : 2:1 VLAN 変換。

（注）　VLAN 変換の設定の詳細なカバレッジについては、「L2VPN ERS（EVPL）サービスの VLAN 変換の設定」（P.3-180）を参照してください。

ステップ 29　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

（注）　[PW Tunnel Selection] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 30　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 31　[Finish] をクリックします。

CE が存在するイーサネット EWS（EPL）ポリシーの定義

ここでは、CE が存在するイーサネット EWS（EPL）ポリシーの定義について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [L2VPN EWS] を選択します。

ステップ 2　[CE Present] チェックボックスをオンにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

（注）　[Standard UNI Port] 属性は、IOS XR が実行されている N-PE デバイス上に UNI がある場合は、このポリシーに基づくサービス要求内では使用不可です。

（注）　以前のリリースでは、EWS（EPL）に対する唯一のレイヤ 2 VPN サポートは、EWS（EPL）から EWS（EPL）でした。ISC 4.1.2 以降では、トランク ポートとしての EWS（EPL）から Network to Network Interface（NNI; ネットワーク間インターフェイス）もサポートされます。この新しいタイプのサービス要求を作成するには、標準の UNI フラグをオフにして、EWS（EPL）「ハイブリッド」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に EWS（EPL）ハイブリッド ポリシーを使用する場合は、接続の EWS（EPL）側の [Standard UNI Port flag] をオンにして、接続の NNI 側の標準の UNI フラグをオフにします。

（注）　ハイブリッド サービスの場合は、IOS XR が実行されている N-PE 上の UNI はサポートされません。

ステップ 5　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、U-PE または N-PE インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、L2VPN サービス要求の作成中にオペレータが表示できるインターフェイス タイプを制限するためのフィルタとして機能します。

ステップ 6　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 10　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 11　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 12　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 13　Prime Provisioning に VC ID を選択させる場合は、[VC ID AutoPick] 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しない場合は、サービスのアクティブ化中に [VC ID] フィールドで VC ID を指定するよう求めるプロンプトが表示されます。

ステップ 14　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 15　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 16　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 17　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。

ステップ 18　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 19　[Link Media] タイプ（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

使用方法に関する注釈：

- デフォルトは [None] です。
- この属性の使用時に、新しい CLI が、メディア タイプを定義するために UNI インターフェイスで生成されます。
- [Link Media] 属性は、ME3400 プラットフォームだけでサポートされます。

ステップ 20　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 21　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 22　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 23　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 24　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。トラフィックのタイプごとにしきい値を入力します。

2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

選択したプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a.　[Enable cdp]：Cisco Discover Protocol（CDP）でレイヤ 2 トンネリングをイネーブルにします。

b.　[cdp shutdown threshold]：インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

c.　[cdp drop threshold]：インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d.　[Enable vtp]：VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）でレイヤ 2 トンネリングをイネーブルにします。

e.　[vtp shutdown threshold]：インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Enable stp] : スパニングツリー プロトコル（STP）でレイヤ 2 トンネリングをイネーブルにします。

h. [stp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 28 OSM カードのスイッチ仮想インターフェイスで疑似回線接続を設定するには、[N-PE Pseudo-wire On SVI] 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は、デフォルトでオンになっています。チェックボックスをオフにすると、疑似回線は、PFC カードのサブインターフェイス（使用可能な場合）でプロビジョニングされます。このオプションは、C76xx デバイスだけで使用可能です。

（注） [N-PE Pseudo-wire On SVI] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 29 [MTU Size] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。デフォルトのサイズは 9216 で、範囲は 1500 ～ 9216 です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。

Cisco Prime Provisioning 6.3 では、異なるプラットフォームによって異なる範囲をサポートします。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Cisco Prime Provisioning 6.3 は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 30 ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

（注） [PW Tunnel Selection] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 31 ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 32　[Finish] をクリックします。

CE が存在しないイーサネット EWS（EPL）ポリシーの定義

ここでは、CE が存在しないイーサネット EWS（EPL）ポリシーの定義方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [L2VPN EWS] を選択します。

ステップ 2　[CE Present] チェックボックスをオフにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ドロップダウン リストから N-PE/U-PE **インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、または U-PE インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、L2VPN サービス要求の作成中にオペレータが表示できるインターフェイス タイプを制限するためのフィルタとして機能します。

ステップ 5　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

（注）　[Standard UNI Port] 属性は、IOS XR が実行されている N-PE デバイス上に UNI がある場合は、このポリシーに基づくサービス要求内では使用不可です。

（注）　以前のリリースでは、EWS（EPL）に対する唯一のレイヤ 2 VPN サポートは、EWS（EPL）から EWS（EPL）でした。ISC 4.1.2 以降では、トランク ポートとしての EWS（EPL）から Network to Network Interface（NNI; ネットワーク間インターフェイス）もサポートされます。この新しいタイプのサービス要求を作成するには、標準の UNI フラグをオフにして、EWS（EPL）「ハイブリッド」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に EWS（EPL）ハイブリッド ポリシーを使用する場合は、接続の EWS（EPL）側の [Standard UNI Port flag] をオンにして、接続の NNI 側の標準の UNI フラグをオフにします。

（注）　ハイブリッド サービスの場合は、IOS XR が実行されている N-PE 上の UNI はサポートされません。

ステップ 6　PE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 10　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオフになっています。

ステップ 11　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオフになっています。

ステップ 12　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 13　Prime Provisioning に VC ID を選択させる場合は、[VC ID AutoPick] 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しない場合は、サービスのアクティブ化中に [VC ID] フィールドで VC ID を指定するよう求めるプロンプトが表示されます。

ステップ 14　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 15　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 16　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 17　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。

ステップ 18　[Link Media] タイプ（任意）に [None]、[auto-select]、[rj45]、または [sfp] を入力します。

使用方法に関する注釈：

- デフォルトは [None] です。
- この属性の使用時に、新しい CLI が、メディア タイプを定義するために UNI インターフェイスで生成されます。

- [Link Media] 属性は、ME3400 プラットフォームだけでサポートされます。

ステップ 19　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 20　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 24　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 25　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 26　コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

検査するプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Enable cdp] : Cisco Discover Protocol（CDP）でレイヤ 2 トンネリングをイネーブルにします。

b. [cdp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

c. [cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Enable vtp] : VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）でレイヤ 2 トンネリングをイネーブルにします。

e. [vtp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Enable stp] : スパニングツリー プロトコル（STP）でレイヤ 2 トンネリングをイネーブルにします。

h. [stp shutdown threshold] : インターフェイスをシャットダウンするまでに受信する、1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 27　OSM カードのスイッチ仮想インターフェイスで疑似回線接続を設定するには、[N-PE Pseudo-wire On SVI] 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は、デフォルトでオンになっています。チェックボックスをオフにすると、疑似回線は、PFC カードのサブインターフェイス（使用可能な場合）でプロビジョニングされます。このオプションは、C76xx デバイスだけで使用可能です。

（注）　[N-PE Pseudo-wire On SVI] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 28　[MTU Size] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。デフォルトのサイズは 9216 で、範囲は 1500 ～ 9216 です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。

Cisco Prime Provisioning 6.3 では、異なるプラットフォームによって異なる範囲をサポートします。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Cisco Prime Provisioning 6.3 は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 29　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

（注）　[PW Tunnel Selection] 属性は、IOS XR が実行されているデバイスのこのポリシーに基づくサービス要求内では使用不可です。

ステップ 30　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 31　[Finish] をクリックします。

CE が存在するフレーム リレー ポリシーの定義

ここでは、CE が存在するフレーム リレー ポリシーの定義方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [Frame Relay] を選択します。

ステップ 2　[CE Present] チェックボックスをオンにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 5　ドロップダウン リストから **CE** の [Interface Type] を選択します。

選択できる基準は、次のとおりです。

- ANY

- Serial
- MFR
- POS
- Hssi
- BRI

ステップ 6　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　[CE Encapsulation] タイプを選択します。

選択できる基準は、次のとおりです。

- FRAME RELAY
- FRAME RELAY IETF

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 9　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 10　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 11　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 12　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 13　[Finish] をクリックします。

CE が存在しないフレーム リレー ポリシーの定義

ここでは、CE が存在しないフレーム リレー ポリシーの定義方法について説明します。次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [Frame Relay] を選択します。

ステップ 2　[CE Present] チェックボックスをオフにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 5　ドロップダウン リストから **CE** の [N-PE/U-PE Interface Type] を選択します。

選択できる基準は、次のとおりです。

- ANY
- Serial
- MFR

- POS
- Hssi
- BRI

ステップ 6　PE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　N-PE/U-PE の [Encapsulation] タイプを選択します。

選択できる基準は、次のとおりです。

- FRAME RELAY
- FRAME RELAY IETF

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 9　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 10　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 11　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 12　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 13　[Finish] をクリックします。

CE が存在する ATM ポリシーの定義

ここでは、CE が存在する ATM ポリシーの定義方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [ATM] を選択します。

ステップ 2　[CE Present] チェックボックスをオンにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ドロップダウン リストから [Transport Mode] を選択します。

選択できる基準は、次のとおりです。

- [VP]：仮想パス モード。これはデフォルトです。
- [VC]：仮想回線モード。
- [PORT]：ポート モード （IOS XR 3.7 プラットフォームだけでサポートされます）。使用方法に関する注釈：
  - トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで属性 [ATM VCD/Sub-interface #] と [ATM VPI] はディセーブルにされます。

- トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで、タイマー値を設定するための 3 つの属性が表示されます。これらの属性は、[Timer1]、[Timer2]、および 、[Timer3] です。これはタイマー値を追加するために使用します。これらの値の暗黙的範囲は 50 ～ 4095 です。この機能は、UNI デバイスとしての N-PE だけでサポートされます。
- トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで、セル パッキングを設定するための 2 つの属性が表示されます。これらの属性は、[Maximum no. of cells to be packed] と [Cell packing timer] です。この機能は、UNI デバイスとしての N-PE だけでサポートされます。

ステップ 5　ドロップダウン リストから、[CE Interface Type] を選択します。

選択できる基準は、次のとおりです。

- ANY
- ATM
- Switch

ステップ 6　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**CE カプセル化**を選択します。

選択できる基準は、次のとおりです。

- AAL5SNAP
- AAL5MUX
- AAL5NLPID
- AAL2

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 10　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC

- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 11　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 12　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 13　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 14　[Finish] をクリックします。

CE が存在しない ATM ポリシーの定義

ここでは、CE が存在しない ATM ポリシーの定義方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [ATM] を選択します。

ステップ 2　[CE Present] チェックボックスをオフにします。

ステップ 3　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 4　ドロップダウン リストから [Transport Mode] を選択します。

選択できる基準は、次のとおりです。

- [VP]：仮想パス モード。これはデフォルトです。
- [VC]：仮想回線モード。
- [PORT]：ポート モード （IOS XR 3.7 プラットフォームだけでサポートされます）。使用方法に関する注釈：
  - トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで属性 [ATM VCD/Sub-interface #] と [ATM VPI] はディセーブルにされます。
  - トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで、タイマー値を設定するための 3 つの属性が表示されます。これらの属性は、[Timer1]、[Timer2]、および、[Timer3] です。 これはタイマー値を追加するために使用します。これらの値の暗黙的範囲は 50 ～ 4095 です。この機能は、UNI デバイスとしての N-PE だけでサポートされます。
  - トランスポート モードとして [PORT] を選択すると、このポリシーに基づくサービス要求の [Link Attributes] ウィンドウで、セル パッキングを設定するための 2 つの属性が表示されます。これらの属性は、[Maximum no. of cells to be packed] と [Cell packing timer] です。この機能は、UNI デバイスとしての N-PE だけでサポートされます。

ステップ 5　ドロップダウン リストから [N-PE/U-PE Interface Type] を選択します。

選択できる基準は、次のとおりです。

- ANY
- ATM
- Switch

ステップ 6　PE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 7　**PE カプセル化**を選択します。

選択できる基準は、次のとおりです。

- AAL5SNAP
- AAL5MUX
- AAL5NLPID
- AAL5
- AAL0

（注）　[Interface Type] が [ANY] の場合は、Prime Provisioning は、ポリシーで [Encapsulation] タイプを尋ねません。

ステップ 8　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 9　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

この属性は IOS XR デバイスだけで適用可能です。チェックボックスをオンにすると、追加の属性である **PseudoWireClass** が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[PseudoWireClass] 属性の [Select] ボタンをクリックします。疑似回線クラス名は、IOS XR デバイスでの pw-class コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラスのサポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ステップ 10　ドロップダウン リストから **L2VPN グループ名**を選択します。

選択できる基準は、次のとおりです。

- ISC
- VPNSC

この属性は、IOS XR デバイスでの L2VPN グループ名のプロビジョニングに使用されます。

（注）　ドロップダウン リストの選択項目は、設定可能な DCPL プロパティから取得されます。ドロップダウン リストで使用可能な [L2VPN Group Name] 選択項目を定義する方法については、「IOS XR デバイスの L2VPN グループ名の定義」（P.3-19）を参照してください。

ステップ 11　Point-to-Point（p2p; ポイントツーポイント）E-line 名を指定するには、[E-Line Name] に入力します。

この属性は IOS XR デバイスだけで適用可能です。p2p 名に値を指定しないと、Prime Provisioning は、疑似回線を形成する 2 つの PE の名前をハイフンで区切って構成したデフォルトの名前を生成します（たとえば、6503-A----6503-B）。デフォルトの名前が 32 文字を超える場合は、デバイス名は切り捨てられます。

ステップ 12　ポイントツーポイント N-PE を接続する疑似回線にトラフィック エンジニアリング（TE）トンネルを手動で選択できるようにするには、[PW Tunnel Selection] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

その後に、このポリシーに基づいてサービス要求を作成するときに、表示されるフィールドに TE トンネル ID を指定する必要があります。Prime Provisioning は、トンネル情報を使用して、2 つの N-PE 間の疑似回線接続を記述する疑似回線クラスを作成してプロビジョニングします。この疑似回線クラスは、疑似回線が同じトンネル ID とリモート ループバック アドレスを共有する限り、複数の疑似回線によって共有可能です。トンネル インターフェイスと関連する ID が設定されていることを確認する必要があります。サービス要求の作成中にトンネル ID 番号を指定するときに、Prime Provisioning は値の有効性を確認しません。つまり、Prime Provisioning は、トンネルの存在を検査しません。

ステップ 13　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、

「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 14　[Finish] をクリックします。

L2VPN サービス要求の管理

この項では、ERS（EVPL）、EWS（EPL）、ATM、またはフレーム リレー L2VPN サービスの基本的なプロビジョニング手順について説明します。具体的な内容は、次のとおりです。

- 「Prime Provisioning をサポートするためのデバイス設定」（P.3-7）
- 「EVC サービス要求の作成」（P.3-37）
- 「CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-128）
- 「CE が存在する EWS（EPL）L2VPN サービス要求の作成」（P.3-130）
- 「CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-132）
- 「CE が存在しない EWS（EPL）L2VPN サービス要求の作成」（P.3-134）
- 「EVC サービス要求の変更」（P.3-57）
- 「L2VPN サービス要求の保存」（P.3-137）

L2VPN サービス要求の概要

L2VPN サービス要求は、ポイントツーポイント トポロジ内のさまざまなサイトを接続する 1 つ以上のエンドツーエンド ワイヤからなります。サービス要求の作成時に、CE および PE ルータ上の特定のインターフェイスを含め、いくつかのパラメータを入力します。

また、Prime Provisioning テンプレートおよびデータ ファイルをサービス要求と関連付けることもできます。サービス要求でのテンプレートおよびデータ ファイルの使用について詳しくは、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。

サービス要求を作成するには、「VPLS ポリシーの作成」（P.3-138）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。

定義済みの L2VPN ポリシーに基づいて、オペレータは、L2VPN ポリシーに変更を行うか、変更を行わずに、L2VPN サービス要求を作成してサービスを展開します。サービスの作成と展開は一般に、ネットワーク プロビジョニングの毎日の操作として、担当のネットワーク技術者が実行します。

（注）　L2VPN ポリシーで定義したすべての属性がサービス要求に適用されるわけではないことがあります。詳しくは、「L2VPN ポリシーの作成」（P.3-95）にある、L2VPN ポリシー属性の説明を参照してください。

カスタマー サイト間のレイヤ 2 接続のためにサービス要求を作成する際に、次のステップを実行する必要があります。

- ERS（EVPL）/フレーム リレー /ATM サービスの CE トポロジを選択します。
- 接続する必要があるエンドポイント（CE と PE）を選択します。エンドツーエンド レイヤ 2 接続ごとに、Prime Provisioning は、サービス要求のリポジトリにエンドツーエンド ワイヤ オブジェクトを作成します。
- CE または PE インターフェイスを選択します。
- CE または PE の Named Physical Circuit（NPC; 名前付き物理回線）を選択します。
- エンドツーエンド接続を編集します。
- リンク属性を編集します。
- （任意）サービス要求でテンプレートとデータ ファイルをデバイスに関連付けます。

L2VPN シナリオのサンプル コングレットについては、「サンプル コンフィグレット」（P.3-186）を参照してください。

L2VPN サービス要求の作成

L2VPN サービス要求を作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Create Service Request] 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　ポリシー選択機能を使用して、以前に作成したポリシーから L2VPN ポリシーを選択します（「L2VPN ポリシーの作成」（P.3-95）を参照）。

[L2VPN Service Request Editor] ウィンドウが表示されます。

新しいサービス要求は、すべての編集可能な機能と編集不可能な機能および事前設定されたパラメータなど、選択した L2VPN ポリシーのプロパティをすべて継承します。

ステップ 3　L2VPN サービス要求の作成を続行するには、次のいずれかの項に移動します。

- 「CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-128）。
- 「CE が存在する EWS（EPL）L2VPN サービス要求の作成」（P.3-130）。
- 「CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-132）。
- 「CE が存在しない EWS（EPL）L2VPN サービス要求の作成」（P.3-134）。

CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成

ここでは、ERS（EVPL）、ATM、およびフレーム リレー ポリシーについて CE が存在する L2VPN サービス要求を作成するための詳細なステップについて説明します。EWS（EPL）ポリシーの L2VPN サービス要求を作成する場合は、「CE が存在する EWS（EPL）L2VPN サービス要求の作成」（P.3-130）に進みます。

L2VPN ポリシーの選択後に、[L2VPN Service Request Editor] ウィンドウが表示されます。

次のステップを実行します。

ステップ 1　ポリシーの L2VPN サービス要求を作成します。

[L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 2　ドロップダウン リストから**トポロジ**を選択します。

[Full Mesh] を選択すると、各 CE は接続をその他すべての CE に転送します。

[Hub and Spoke] を選択すると、ハブ CE だけが各スポーク CE に接続され、スポーク CE は相互に直接接続されません。

（注）　フル メッシュおよびハブ アンド スポーク トポロジは、3 つ以上のエンドポイントを選択した場合に限り異なります。たとえば、Prime Provisioning は、4 つのエンドポイントを使用して、フル メッシュ トポロジで 6 個のリンクを自動的に作成します。それに対し、ハブ & スポーク トポロジでは Prime Provisioning が作成するリンクは 3 つだけです。

ステップ 3　[Add Link] をクリックします。

[Attachment Tunnel Editor] を使用して CE エンドポイントを指定します。

（注）　ポイントツーポイント接続を導入するすべてのサービス（ERS/EVPL、EWS/EPL、ATMoMPLS、および FRoMPLS）で、少なくとも 2 つの CE を指定する必要があります。

ステップ 4　[CE] 列の [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。このウィンドウには、現在定義されている CE のリストが表示されます。

a. [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。
b. [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。
c. [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

ステップ 5　[Select] 列で、L2VPN リンクに対する CE を選択します。

ステップ 6　[Select] をクリックします。

[CE] 列で選択した CE の名前が示された [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。

（注）　L2VPN ERS（EVPL）サービスをプロビジョニングする場合、あるデバイスに UNI を選択すると、同じ UNI を使用する他のサービスが存在するかどうかを Prime Provisioning が判定します。ある場合は、警告メッセージが表示されます。メッセージを無視して、サービス要求を保存すると、同じ UNI に依存する、基礎となるサービス要求はすべて、最新のサービス要求の変更された共有属性と同期されます。さらに、既存のサービス要求の状態は、[Requested] 状態に変更されます。

（注）　Prime Provisioning には、基盤となるインターフェイスの設定、インターフェイスを使用する可能性がある既存のサービス要求、サービス要求に関連付けられたカスタマーに基づいて、サービスに使用可能なインターフェイスだけが表示されます。[Details] ボタンをクリックして、インターフェイス名、カスタマー名、VPN 名、サービス要求 ID、サービス要求タイプ、VLAN 変換タイプ、および VLAN ID 情報など、使用可能なインターフェイスに関する情報が示されたポップアップ ウィンドウを表示できます。

ステップ 8　選択した CE と CE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動入力される場合は、明示的に選択する必要はありません。複数の NPC が使用可能な場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。

[Select NPC] ウィンドウが表示され、適切な NPC を選択できます。

ステップ 9　[OK] をクリックします。

CE とインターフェイスを選択するたびに、この CE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。[NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

ステップ 10　前のステップと同様に、追加の CE の指定を続けます。

Prime Provisioning は、選択したトポロジに基づいて CE 間のリンクを作成します。

ステップ 11　[OK] をクリックします。

ERS（EVPL）、ATM、およびフレーム リレーでは、[EndToEndWire] ウィンドウが表示されます。

ステップ 12　このサービス要求の VPN が [VPN] フィールドに表示されます。

複数の VPN がある場合は、[Select VPN] 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 13　**VPN 名**を選択して、[Select] をクリックします。

VPN 名が示された [L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 14　必要に応じて、[Attachment Circuit2 (AC2)] 列で [Add AC] をクリックして、AC2 でステップ 3 ～ 10 を繰り返します。

[EndToEndWire] ウィンドウに、エンドツーエンド配線全体が表示されます

ステップ 15　設定の必要に応じて、[EndToEndWire] ウィンドウで残りの項目を指定します。

- エンドツーエンド ワイヤを編集するには、青色で強調表示された値を選択します。
- デフォルトのポリシー設定を変更するには、AC リンク属性を編集できます。これらのフィールドの編集後に、青色のリンクは [Default] から [Changed] に変更されます。詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。
- ワイヤごとに表示される [Description] フィールドに各エンドツーエンド ワイヤの説明を入力できます。説明はこのウィンドウだけに表示されます。このフィールドのデータはデバイスには送信されません。このフィールドの最大長は 256 文字です。
- ID 番号は、システムによって生成される、回線の ID 番号です。
- サービスに基づいて、回線 ID が自動的に作成されます。たとえば、イーサネットの場合は VLAN 番号、フレーム リレーの場合は DLCI、ATM の場合は VPI/VCI に基づいています。
- VC ID を手動で定義するようポリシーを設定した場合は、空の [VC ID] フィールドに入力します。VC ID を「自動選択」するようポリシーを設定した場合は、Prime Provisioning が VC ID を指定し、このフィールドは編集不可能になります。[VC ID] を手動で入力する場合、入力した値がプロバイダーの範囲内であれば、Prime Provisioning は入力値が使用可能か割り当て済みかを確認します。入力した値がすでに割り当てられている場合は、Prime Provisioning は、入力した値が使用不可であることを示すエラー メッセージを生成し、値を再度入力するよう求めます。入力した値がプロバイダーの範囲内にあり、使用可能な場合は、その値が割り当てられ、VC ID プールから削除されます。入力した値がプロバイダーの範囲外にある場合は、Prime Provisioning は、この値が使用可能であるか割り当て済みであるかを調べるための検証を実行できなかったことを示す警告を表示します。
- エンドツーエンド ワイヤを追加するには、[Add Link] をクリックします。
- エンドツーエンド ワイヤを削除するには、[Delete Link] をクリックします。

ステップ 16　エンドツーエンド ワイヤの編集が終了したら、[Save] をクリックします。

サービス要求が作成され、Prime Provisioning に保存されます。

CE が存在する EWS（EPL）L2VPN サービス要求の作成

ここでは、EWS（EPL）について CE が存在する L2VPN サービス要求を作成するための詳細なステップについて説明します。ERS（EVPL）、ATM、フレーム リレー ポリシーの L2VPN サービス要求を作成する場合は、「CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-128）に進みます。

次のステップを実行します。

ステップ 1　CE が存在する EWS（EPL）の L2VPN サービス要求を作成します。

[L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 2　この CE で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

ステップ 3　[Select] 列で **VPN 名**を選択します。

ステップ 4　[Select] をクリックします。

VPN 名が示された [L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 5　[Add Link] をクリックします。

- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Request Editor] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。

- ワイヤごとに表示される [Description] フィールドに各エンドツーエンド ワイヤの説明を入力できます。説明はこのウィンドウだけに表示されます。このフィールドのデータはデバイスには送信されません。このフィールドの最大長は 256 文字です。
- ID 番号は、システムによって生成される、回線の ID 番号です。
- サービスに基づいて、回線 ID が自動的に作成されます。たとえば、イーサネットの場合は VLAN 番号、フレーム リレーの場合は DLCI、ATM の場合は VPI/VCI に基づいています。

ステップ 6　[Attachment Circuit1 (AC1)] 列の [Add AC] をクリックします。

[Customer and Link Selection] ウィンドウが表示されます。

ステップ 7　[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。

このウィンドウには、現在定義されている CE のリストが表示されます。

a. [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。

b. [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。

c. [Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

ステップ 8　[Select] 列で、L2VPN リンクに対する CE を選択します。

ステップ 9　[Select] をクリックします。

ステップ 10　[Customer and Link Selection] ウィンドウで、インターネット選択機能から CE インターフェイスを選択します。

ステップ 11　選択した CE と CE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動入力される場合は、明示的に選択する必要はありません。

複数の NPC が使用可能な場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。[Select NPC] ウィンドウが表示され、適切な NPC を選択できます。CE とインターフェイスを選択するたびに、この CE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

ステップ 12　[OK] をクリックします。

[AC1] 列で選択した CE の名前が示された [EndToEndWire] ウィンドウが表示されます。

ステップ 13　必要に応じて、接続回線の属性を編集するには、[AC1 Attributes] 列の [Edit] リンクをクリックします。

[Link Attributes] ウィンドウが表示されます。必要に応じて属性を編集します。詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

ステップ 14　[OK] をクリックします。

ステップ 15　**AC2** でステップ 6 ～ 14 を繰り返します。

ステップ 16　[L2VPN Service Request Editor] で、[Save] をクリックします。

EWS（EPL）サービス要求が作成され、Prime Provisioning に保存されます。

CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成

ここでは、ERS（EVPL）、ATM、およびフレーム リレー ポリシーについて CE が存在しない L2VPN サービス要求を作成するための詳細なステップについて説明します。EWS（EPL）ポリシーの L2VPN サービス要求を作成する場合は、「CE が存在しない EWS（EPL）L2VPN サービス要求の作成」（P.3-134）に進みます。

次のステップを実行します。

ステップ 1　CE が存在しない ERS（EVPL）の L2VPN サービス要求を作成します。

[L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 2　ドロップダウン リストから**トポロジ**を選択します。

[Full Mesh] を選択すると、各 CE は接続をその他すべての CE に転送します。[Hub and Spoke] を選択すると、ハブ CE だけが各スポーク CE に接続され、スポーク CE は相互に直接接続されません。

（注）　フル メッシュおよびハブ アンド スポーク トポロジは、3 つ以上のエンドポイントを選択した場合に限り異なります。たとえば、Prime Provisioning は、4 つのエンドポイントを使用して、フル メッシュ トポロジで 6 個のリンクを自動的に作成します。それに対し、ハブ & スポーク トポロジでは Prime Provisioning が作成するリンクは 3 つだけです。

ステップ 3　[Add Link] をクリックします。

ステップ 4　次の手順で説明されているように、N-PE/PE-AGG/U-PE エンドポイントを指定します。

ステップ 5　[U-PE/PE-AGG/N-PE] 列で [Select U-PE/PE-AGG/N-PE] をクリックします。

[Select PE Device] ウィンドウが表示されます。

このウィンドウには、現在定義されている PE のリストが表示されます。

a.　[Show PEs with] ドロップダウン リストには、カスタマー名、サイト、またはデバイス名別に PE が表示されます。

b.　[Find] ボタンを使用すると、特定の PE を検索するか、ウィンドウを更新できます。

c.　[Rows per page] ドロップダウン リストを使用すると、ページを [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

ステップ 6　[Select] 列で、L2VPN リンクの PE デバイス名を選択します。

ステップ 7　[Select] をクリックします。

選択した PE の名前が [N-PE/PE-AGG/U-PE] 列に示された [L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 8　インターフェイス選択機能から [UNI Interface] を選択します。

（注）　L2VPN ERS（EVPL）サービスをプロビジョニングする場合、あるデバイスに UNI を選択すると、同じ UNI を使用する他のサービスが存在するかどうかを Prime Provisioning が判定します。ある場合は、警告メッセージが表示されます。メッセージを無視して、サービス要求を保存すると、同じ UNI に依存する、基礎となるサービス要求はすべて、最新のサービス要求の変更された共有属性と同期されます。さらに、既存のサービス要求の状態は、[Requested] 状態に変更されます。

（注）　Prime Provisioning には、基盤となるインターフェイスの設定、インターフェイスを使用する可能性がある既存のサービス要求、サービス要求に関連付けられたカスタマーに基づいて、サービスに使用可能なインターフェイスだけが表示されます。[Details] ボタンをクリックして、インターフェイス名、カスタマー名、VPN 名、サービス要求 ID、サービス要求タイプ、VLAN 変換タイプ、および VLAN ID 情報など、使用可能なインターフェイスに関する情報が示されたポップアップ ウィンドウを表示できます。

ステップ 9　PE ロール タイプが U-PE の場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。

[Select NPC] ウィンドウが表示されます。

選択した PE と PE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動入力される場合は、明示的に選択する必要はありません。

（注）　PE ロール タイプが N-PE の場合は、列 [Circuit Selection] と [Circuit Details] はディセーブルです。

ステップ 10　[Select] 列から NPC の名前を選択します。

ステップ 11　[OK] をクリックします。

PE とインターフェイスを選択するたびに、この PE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

ステップ 12　この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。

[Select NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

ステップ 13　PE をすべて指定した後、選択されたトポロジに基づいて Prime Provisioning が PE 間のリンクを作成します。

ステップ 14　[OK] をクリックします。

ERS（EVPL）、ATM、およびフレーム リレーでは、[EndToEndWire] ウィンドウが表示されます。

ステップ 15　このサービス要求の VPN が [Select VPN] フィールドに表示されます。

複数の VPN がある場合は、[Select VPN] をクリックして、VPN を選択します。

ステップ 16　設定での必要性に応じて、[EndToEnd Wire] ウィンドウで残りの項目を指定します。

- エンドツーエンド ワイヤを編集するには、青色で強調表示された値を選択します。
- デフォルトのポリシー設定を変更するには、AC リンク属性を編集できます。これらのフィールドの編集後に、青色のリンクは [Default] から [Changed] に変更されます。詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。
- エンドツーエンド ワイヤを追加するには、[Add Link] をクリックします。
- エンドツーエンド ワイヤを削除するには、[Delete Link] をクリックします。

（注）　テンプレートが追加されているサービス要求の廃止を試行する場合は、正しい方法の詳細について、「サービス要求のデコミッション」（P.8-12）を参照してください。

- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。

- ワイヤごとに表示される [Description] フィールドに各エンドツーエンド ワイヤの説明を入力できます。説明はこのウィンドウだけに表示されます。このフィールドのデータはデバイスには送信されません。このフィールドの最大長は 256 文字です。
- ID 番号は、システムによって生成される、回線の ID 番号です。
- サービスに基づいて、回線 ID が自動的に作成されます。たとえば、イーサネットの場合は VLAN 番号、フレーム リレーの場合は DLCI、ATM の場合は VPI/VCI に基づいています。

ステップ 17　エンドツーエンド ワイヤの編集が終了したら、[Save] をクリックします。

サービス要求が作成され、Prime Provisioning に保存されます。

CE が存在しない EWS（EPL）L2VPN サービス要求の作成

ここでは、EWS（EPL）について CE が存在しない L2VPN サービス要求を作成するための詳細なステップについて説明します。ERS（EVPL）、ATM、フレーム リレー ポリシーの L2VPN サービス要求を作成する場合は、「CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-132）を参照してください。

ステップ 1　CE が存在しない EWS（EPL）の L2VPN サービス要求を作成します。

[L2VPN Service Request Editor] ウィンドウが表示されます。

ステップ 2　この PE で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。

ステップ 3　[Select] 列で **VPN 名**を選択します。

ステップ 4　[Select] をクリックします。

VPN 名が示された [EndToEndWire] ウィンドウが表示されます。

ステップ 5　[Attachment Circuit 1(AC1)] 列の [Add AC] をクリックします。

[Customer and Link Selection] ウィンドウが表示されます。

ステップ 6　[Select N-PE/PE-AGG/U-PE] をクリックします。[N-PE/PE-AGG/U-PE] 列

[Select PE Device] ウィンドウが表示されます。

このウィンドウには、現在定義されている PE のリストが表示されます。

a. [Show PEs with] ドロップダウン リストから、[PEs by Customer Name]、[by Site]、または [by Device Name] 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。

ステップ 7　[Select] 列で、L2VPN リンクに対する PE を選択します。

ステップ 8　[Select] をクリックします。

[Customer and Link Selection] 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 [PE Interface] を選択します。

（注）　Prime Provisioning には、基盤となるインターフェイスの設定、インターフェイスを使用する可能性がある既存のサービス要求、サービス要求に関連付けられたカスタマーに基づいて、サービスに使用可能なインターフェイスだけが表示されます。[Details] ボタンをクリックして、インターフェイス名、カ

スタマー名、VPN 名、サービス要求 ID、サービス要求タイプ、VLAN 変換タイプ、および VLAN ID 情報など、使用可能なインターフェイスに関する情報が示されたポップアップ ウィンドウを表示できます。

ステップ 10　PE ロール タイプが N-PE の場合は、列 [Circuit Selection] と [Circuit Details] はディセーブルです。この場合は、ステップ 13 にスキップします。

ステップ 11　PE ロール タイプが U-PE の場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。

[Select NPC] ウィンドウが表示されます。

（注）　選択した PE と PE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動入力される場合は、明示的に選択する必要はありません。

ステップ 12　必要に応じて、[Select] 列から NPC の名前を選択します。

ステップ 13　[OK] をクリックします。

（注）　PE とインターフェイスを選択するたびに、この PE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

ステップ 14　[OK] をクリックします。

選択した PE の名前が [Attachment Circuit1 (AC1)] 列に示された [l2VPN Service Request] ウィンドウが表示されます。

ステップ 15　必要に応じて、[AC1 Attributes] で [Edit] リンクをクリックして、属性を編集します。

詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

ステップ 16　[Attachment Circuit2] でステップ 5 ～ 14 を繰り返します。

ステップ 17　設定の必要に応じて、[EndToEndWire] ウィンドウで残りの項目を指定します。

- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。
- ワイヤごとに表示される [Description] フィールドに各エンドツーエンド ワイヤの説明を入力できます。説明はこのウィンドウだけに表示されます。このフィールドのデータはデバイスには送信されません。このフィールドの最大長は 256 文字です。
- ID 番号は、システムによって生成される、回線の ID 番号です。
- サービスに基づいて、回線 ID が自動的に作成されます。たとえば、イーサネットの場合は VLAN 番号、フレーム リレーの場合は DLCI、ATM の場合は VPI/VCI に基づいています。

ステップ 18　[Save] をクリックします。

EWS（EPL）サービス要求が作成され、Prime Provisioning に保存されます。

L2VPN サービス要求の変更

ここでは、L2VPN サービス要求属性を編集する方法について説明します。接続回線の一部であるデバイスにテンプレートとデータ ファイルを関連付けることもできます。

次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

[L2VPN Service Request] ウィンドウが表示されます。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

[EndToEndWire] ウィンドウが表示されます。

ステップ 4　必要に応じて、属性を変更します。

- このサービス要求の VPN が [Select VPN] フィールドに表示されます。この要求に複数の VPN がある場合は、[Select VPN] をクリックして、VPN を選択します。
- エンドツーエンド ワイヤを編集するには、青色で強調表示された値を選択します。
- デフォルトのポリシー設定を変更するには、AC リンク属性を編集できます。これらのフィールドの編集後に、青色のリンクは [Default] から [Changed] に変更されます。
- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。
- ワイヤごとに表示される [Description] フィールドに各エンドツーエンド ワイヤの説明を入力できます。説明はこのウィンドウだけに表示されます。このフィールドのデータはデバイスには送信されません。このフィールドの最大長は 256 文字です。
- 回線 ID は、回線の VLAN データに基づいて自動的に作成されます。
- VC ID を手動で定義するようポリシーを設定した場合は、空の [VC ID] フィールドに入力します。VC ID を「自動選択」するようポリシーを設定した場合は、Prime Provisioning が VC ID を指定し、このフィールドは編集不可能になります。[VC ID] を手動で入力する場合、入力した値がプロバイダーの範囲内であれば、Prime Provisioning は入力値が使用可能か割り当て済みかを確認します。入力した値がすでに割り当てられている場合は、Prime Provisioning は、入力した値が使用不可であることを示すエラー メッセージを生成し、値を再度入力するよう求めます。入力した値がプロバイダーの範囲内にあり、使用可能な場合は、その値が割り当てられ、VC ID プールから削除されます。入力した値がプロバイダーの範囲外にある場合は、Prime Provisioning は、この値が使用可能であるか割り当て済みであるかを調べるための検証を実行できなかったことを示す警告を表示します。
- エンドツーエンド ワイヤを追加するには、[Add Link] をクリックします。
- エンドツーエンド ワイヤを削除するには、[Delete Link] をクリックします。

（注）　テンプレートが追加されているサービス要求の廃止を試行する場合は、正しい方法の詳細について、「サービス要求のデコミッション」（P.8-12）を参照してください。

- ID 番号は、システムによって生成される、回線の ID 番号です。
- サービスに基づいて、回線 ID が自動的に作成されます。たとえば、イーサネットの場合は VLAN 番号、フレーム リレーの場合は DLCI、ATM の場合は VPI/VCI に基づいています。

ステップ 5　AC 属性を編集するには、適切な [AC Attributes] 列で [Default] リンクをクリックします。

[Link Attributes] ウィンドウが表示されます。

ステップ 6　必要に応じて、リンク属性を編集します。

ステップ 7　接続回線にテンプレートとデータ ファイルを追加するには、デバイス名を選択して、[Templates] で [Add] をクリックします。

[Add/Remove Templates] ウィンドウが表示されます。

（注）　テンプレートを接続回線に追加するには、テンプレートをすでに作成してある必要があります。テンプレートを作成するための詳細な手順については、「概要」（P.9-1）を参照してください。サービス リクエスト内でのテンプレートおよびデータ ファイルの使用方法について詳しくは、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 8　[Add] をクリックします。

[Template Data File Chooser] ウィンドウが表示されます。

ステップ 9　左側のペインで、テンプレートにナビゲートして選択します。

関連付けられたデータ ファイルがメイン ウィンドウの行にリストされます。

ステップ 10　追加するデータ ファイルを確認して、[Accept] をクリックします。

テンプレートが示された [Add/Remove Templates] ウィンドウが表示されます。

ステップ 11　テンプレート名を選択します。

ステップ 12　[Action] で、ドロップダウン リストを使用して [APPEND] または [PREPEND] を選択します。

[Append] は、テンプレートによって生成された CLI を通常の Prime Provisioning（非テンプレート）CLI に追加するよう Prime Provisioning に指示します。[Prepend] は逆で、テンプレートを Prime Provisioning CLI に追加しません。

ステップ 13　このサービス要求にこのテンプレートを使用するには、[Active] を選択します。

[Active] を選択しないと、テンプレートは使用されません。

ステップ 14　[OK] をクリックします。

テンプレートが追加された [Link Attributes] が表示されます。

（注）　サービス要求でのテンプレートおよびデータ ファイルの使用について詳しくは、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 15　[OK] をクリックします。

[AC Attachment Circuit] 列のリンクが [Default] から [Changed] に変更されたことを示す [L2VPN Service Request] ウィンドウが表示されます。

ステップ 16　エンドツーエンド ワイヤの編集が終了したら、[Save] をクリックします。

L2VPN サービス要求の保存

L2VPN サービス要求を保存するには、次のステップを実行します。

ステップ 1　すべての接続回線のリンク属性の指定が終了したら、[Save] をクリックして、L2VPN サービス要求の作成を終了します。

L2VPN サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウにそれが一覧表示されます。新しく作成された L2VPN サービス要求が [REQUESTED] の状態で追加されます。

ステップ 2　ただし、何らかの理由で（たとえば、選択した値が範囲外である）L2VPN サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

L2VPN サービス要求の展開の詳細については、「サービス要求の展開」（P.8-10）を参照してください。

VPLS ポリシーの作成

この項では、VPLS ポリシー作成の基本的な手順について説明します。具体的な内容は、次のとおりです。

- 「Prime Provisioning をサポートするためのデバイス設定」（P.3-7）
- 「CE が存在するイーサネット ERS（EVPL）ポリシーの定義」（P.3-97）
- 「CE なしの MPLS/ERMS（EVP-LAN）ポリシーの定義」（P.3-143）
- 「CE ありの MPLS/EMS（EP-LAN）ポリシーの定義」（P.3-146）
- 「CE なしの MPLS/EMS（EP-LAN）ポリシーの定義」（P.3-150）
- 「CE ありのイーサネット /ERMS（EVP-LAN）ポリシーの定義」（P.3-154）
- 「CE なしのイーサネット /ERMS（EVP-LAN）ポリシーの定義」（P.3-157）
- 「CE ありのイーサネット /EMS（EP-LAN）ポリシーの定義」（P.3-160）
- 「CE なしのイーサネット /EMS（EP-LAN）ポリシーの定義」（P.3-164）

VPLS ポリシーの定義

サービスをプロビジョニングする前に、VPLS ポリシーを定義する必要があります。VPLS ポリシーでは、Attachment Circuit（AC; 接続回線）属性で共有する共通特性を定義します。

ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。[Editable] チェックボックスを使用すると、ネットワーク オペレータはフィールドを編集可能にできます。値が [editable] に設定されている場合は、サービス要求の作成者は、特定のポリシー項目のその他の有効値を変更できます。値が [editable] に設定*されていない*場合、サービス要求作成者は、ポリシー項目を変更できません。

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 ファイルの使用方法の詳細については、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。

VPLS ポリシーは、VPLS が提供する次のコア タイプの 1 つに対応します。

- MPLS コア タイプ：プロバイダー コア ネットワークは MPLS 対応です。
- イーサネット コア タイプ：プロバイダー コア ネットワークはイーサネット スイッチを使用します。

また、VPLS ポリシーは VPLS が提供する次のサービス タイプの 1 つに対応します。

- Ethernet Relay Multipoint Service（ERMS）ERMS のメトロ イーサネット フォーラム名は Ethernet Virtual Private LAN（EVP-LAN）です。このマニュアルで VPLS サービスを示すために使用される用語の詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* の「L2VPN Concepts」の章にある「Layer 2 Terminology Conventions」を参照してください。
- Ethernet Multipoint Service（EMS）EMS の MEF 名は Ethernet Private LAN（EP-LAN）です。

ポリシーは、VPLS サービス要求の定義に必要な大半のパラメータのテンプレートです。VPLS ポリシーを定義した後は、共通する一連の特性を共有するすべての VPLS サービス要求で使用できます。

異なるパラメータで新しいタイプ オブ サービスまたはサービスを作成するたびに新しい VPLS ポリシーを作成します。VPLS ポリシーの作成は、通常は経験のあるネットワーク技術者が行います。

Prime Provisioning で VPLS ポリシーを定義するには、次のステップを実行します。

ステップ 1　[Service Design] > [Create Policy] 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　[Policy Type] ドロップダウン リストから [VPLS] 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　VPLS ポリシーの [Policy Name] を入力します。

ステップ 4　VPLS ポリシーの [Policy Owner] を選択します。

VPLS ポリシー所有権には、次の 3 タイプがあります。

- 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：すべてのサービス オペレータがこの VPLS 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 VPLS ポリシーは、カスタマー所有のポリシーの処理を許可されたオペレータだけから表示されます。

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。

ステップ 5　[Select] をクリックして VPLS ポリシーのオーナーを選択します。

ポリシー所有者は、Prime Provisioning の設定中にカスタマーまたはプロバイダーを作成した際に設定しました。所有権がグローバルの場合は、[Select] 機能は表示されません。

ステップ 6　VPLS ポリシーの [Core Type] を選択します。

VPLS ポリシーには、2 つのコア タイプがあります。

- [MPLS]：IP ネットワークで実行されます。
- [Ethernet]：すべての PE がイーサネット プロバイダー ネットワーク上にあります。

ステップ 7　VPLS ポリシーの [Service Type] を選択します。

VPLS ポリシーには 2 つのサービス タイプがあります。

- Ethernet Relay Multipoint Service（ERMS）（ERMS の MEF 名は EVP-LAN です）。
- Ethernet Multipoint Service（EMS）（EMS の MEF 名は EP-LAN です）。

ステップ 8　Prime Provisioning がこの VPLS ポリシーを使用するサービス オペレータに、サービス アクティベーション中に CE ルータおよびインターフェイスの提供を求めるように設定するには、[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] チェックボックスがオフの場合、Prime Provisioning は、サービス アクティベーション中にサービス オペレータに、PE ルータおよびカスタマー側のインターフェイスだけを求めます。

CE ありの MPLS/ERMS（EVP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在ありの MPLS コア タイプおよび ERMS（EVP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] には [MPLS] を選択します。

ステップ 3　[Service Type] に [Ethernet Relay Multipoint Service (ERMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオンにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、PE-AGG、または U-PE インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 8　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

ステップ 9　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 10　たとえば、サービス プロバイダーがネットワークにサービスを展開するときに後でサービスをアクティブ化する場合など、サービス アクティベーション中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　**ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

ステップ 16　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 17　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 18　[PE/UNI Interface Description] フィールドに、*Customer-B ERMS (EVP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 19　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 20　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　[Filter BPDU] チェックボックスをオンにして、UNI ポートがレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）を処理しないように指定します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。[Edit] ボタンをクリックして、アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE なしの MPLS/ERMS（EVP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在なしの MPLS コア タイプおよび ERMS（EVP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] には [MPLS] を選択します。

ステップ 3　[Service Type] に [Ethernet Relay Multipoint Service (ERMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオフにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 8　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 9　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

ステップ 10　たとえば、サービス プロバイダーがネットワークにサービスを展開するときに後でサービスをアクティブ化する場合など、サービス アクティベーション中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　**ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

ステップ 16　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 17　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 18　[PE/UNI Interface Description] フィールドに、*Customer-B ERMS (EVP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 19　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 20　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　[Filter BPDU] チェックボックスをオンにして、UNI ポートがレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）を処理しないように指定します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE ありの MPLS/EMS（EP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在ありの MPLS コア タイプおよび EMS（EP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] には [MPLS] を選択します。

ステップ 3　[Service Type] に [Ethernet Multipoint Service (EMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオンにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）

- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 8　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

（注）　CE ポリシーありの MPLS/EMS（EP-LAN）に基づいてサービス要求を作成している場合、[Encapsulation] 属性は無視されます。つまり、この値を設定しても無効になります。

ステップ 9　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 14　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 15　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 16　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 17　[PE/UNI Interface Description] フィールドに、*Customer-B EMS (EP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 18　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 19　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 20　[System MTU] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。Prime Provisioning では、次に示すように、異なるプラットフォームに対して複数の範囲がサポートされます。範囲は 1500 ～ 9216 です。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Prime Provisioning は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a. [Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b. [Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c. [Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 25　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 26　コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

検査するプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Tunnel CDP] : Cisco Discover Protocol（CDP）のレイヤ 2 トンネリングをイネーブルにします。

b. [CDP Threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

c. [cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Tunnel VTP] : VLAN Trunk Protocol（VTP; 仮想トランク プロトコル）のレイヤ 2 トンネリングをイネーブルにします。

e. [VTP threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Tunnel STP] : スパニング ツリー プロトコル（STP）のレイヤ 2 トンネリングをイネーブルにします。

h. [STP Threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE なしの MPLS/EMS（EP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在なしの MPLS コア タイプおよび EMS（EP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] には [MPLS] を選択します。

ステップ 3　[Service Type] に [Ethernet Multipoint Service (EMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオフにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet

- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 8　PE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 9　N-PE/U-PE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

（注）　CE ポリシーなしの MPLS/EMS（EP-LAN）に基づいてサービス要求を作成している場合、[Encapsulation] 属性は無視されます。つまり、この値を設定しても無効になります。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 16　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 17　[PE/UNI Interface Description] フィールドに、*Customer-B EMS (EP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 18　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 19　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 20　[System MTU] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。Prime Provisioning では、次に示すように、異なるプラットフォームに対して複数の範囲がサポートされます。範囲は 1500 ～ 9216 です。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Prime Provisioning は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 25 UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 26 コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

検査するプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Tunnel CDP]：Cisco Discover Protocol（CDP）のレイヤ 2 トンネリングをイネーブルにします。

b. [CDP Threshold]：インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

c. [cdp drop threshold]：インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Tunnel VTP]：VLAN Trunk Protocol（VTP; 仮想トランク プロトコル）のレイヤ 2 トンネリングをイネーブルにします。

e. [VTP threshold]：インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

f. [vtp drop threshold]：インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Tunnel STP]：スパニング ツリー プロトコル（STP）のレイヤ 2 トンネリングをイネーブルにします。

h. [STP Threshold]：インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

i. [stp drop threshold]：インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval]：UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 27 ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE ありのイーサネット/ERMS（EVP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在ありのイーサネット コア タイプおよび ERMS（EVP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] に [Ethernet] を選択します。

ステップ 3　[Service Type] に [Ethernet Relay Multipoint Service (ERMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオンにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 8　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

ステップ 9　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　**ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

ステップ 16　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 17　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 18　[PE/UNI Interface Description] フィールドに、*Customer-B ERMS (EVP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 19　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 20　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　[Filter BPDU] チェックボックスをオンにして、UNI ポートがレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）を処理しないように指定します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE なしのイーサネット/ERMS（EVP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在なしのイーサネット コア タイプおよび ERMS（EVP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] に [Ethernet] を選択します。

ステップ 3　[Service Type] に [Ethernet Relay Multipoint Service (ERMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオフにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）

- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 8　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 9　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

[DEFAULT] が CE カプセル化タイプである場合は、Prime Provisioning では、UNI ポート タイプに別のフィールドを表示します。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　**ポート タイプ**を選択します。

選択できる基準は、次のとおりです。

- Access Port
- Trunk with Native VLAN

ステップ 16　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 17　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 18　[PE/UNI Interface Description] フィールドに、*Customer-B ERMS (EVP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 19　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 20　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　[Filter BPDU] チェックボックスをオンにして、UNI ポートがレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）を処理しないように指定します。

ステップ 25　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT]：十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN]：インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 26　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE ありのイーサネット/EMS（EP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在ありのイーサネット コア タイプおよび EMS（EP-LAN）サービス タイプで定義する方法について説明します。

次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] に [Ethernet] を選択します。

ステップ 3　[Service Type] に [Ethernet Multipoint Service (EMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオンにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。

次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 8　CE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

（注）　CE ポリシーありのイーサネット /EMS（EP-LAN）に基づいてサービス要求を作成している場合、[Encapsulation] 属性は無視されます。つまり、この値を設定しても無効になります。

ステップ 9　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 16　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 17　[PE/UNI Interface Description] フィールドに、*Customer-B EMS (EP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 18　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 19　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 20　[System MTU] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。デフォルトのサイズは 9216 で、範囲は 1500 ～ 9216 です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。

Cisco Prime Provisioning 6.3 では、異なるプラットフォームによって異なる範囲をサポートします。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Cisco Prime Provisioning 6.3 は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、これはオフになっており、[UNI MAC addresses]（下記を参照）に入力した値に基づいて Prime Provisioning は MAC ベースの ACL を自動的にカスタマー向きの UNI ポートに割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a.　[Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b.　[Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c.　[Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d.　[Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 25　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 26　コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

検査するプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a.　[Tunnel CDP] : Cisco Discover Protocol（CDP）のレイヤ 2 トンネリングをイネーブルにします。

b.　[CDP Threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

c.　[cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d.　[Tunnel VTP] : VLAN Trunk Protocol（VTP; 仮想トランク プロトコル）のレイヤ 2 トンネリングをイネーブルにします。

e.　[VTP threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

f.　[vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Tunnel STP]：スパニング ツリー プロトコル（STP）のレイヤ 2 トンネリングをイネーブルにします。

h. [STP Threshold]：インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

i. [stp drop threshold]：インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval]：UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

CE なしのイーサネット/EMS（EP-LAN）ポリシーの定義

ここでは、VPLS ポリシーを、CE 存在なしのイーサネット コア タイプおよび EMS（EP-LAN）サービス タイプで定義する方法について説明します。次のステップを実行します。

ステップ 1　ポリシー エディタの [Service Information] ウィンドウで、[Policy Type] に [VPLS] を選択します。

ステップ 2　[Core Type] に [Ethernet] を選択します。

ステップ 3　[Service Type] に [Ethernet Multipoint Service (EMS)] を選択します。

ステップ 4　[CE Present] チェックボックスをオフにします。

ステップ 5　[Next] をクリックします。

[Interface Type] ウィンドウが表示されます。

ステップ 6　ドロップダウン リストから**インターフェイス タイプ**を選択します。

サービス プロバイダーの POP 設計に基づいて、CE、N-PE、U-PE、または PE-AGG インターフェイスで特定のインターフェイスを選択できます。次のインターフェイスがあります。

- [ANY]（任意のインターフェイスを選択できます）
- [Port-Channel]（同じ特性を共有するポートのバンドル。これは、サービス プロバイダーが帯域幅と保護を集約できるようにします）
- Ethernet
- FastEthernet
- GE-WAN
- GigabitEthernet
- TenGigabitEthernet
- TenGigE

ここで定義される値は、オペレータが VPLS サービス要求の作成中に表示できるインターフェイス タイプを制限するためのフィルタとして機能します。[ANY] と定義すると、オペレータは、すべてのインターフェイス タイプを表示できます。

ステップ 7　ポート セキュリティをイネーブルにするには、[Standard UNI Port] チェックボックスをオンにします。

これはデフォルトです。このチェックボックスをオフにすると、ポートは、セキュリティ機能のないアップリンクとして扱われ、ポート セキュリティに関連する項目をなくすためにウィンドウはダイナミックに変更されます。

ステップ 8　CE インターフェイスのスロット番号またはポート番号を [Interface Format] に入力します（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と特に役立ちます。

ステップ 9　N-PE/U-PE の**カプセル化**タイプを選択します。

選択できる基準は、次のとおりです。

- DOT1Q
- DEFAULT

（注）　CE ポリシーなしのイーサネット/EMS（EP-LAN）に基づいてサービス要求を作成している場合、[Encapsulation] 属性は無視されます。つまり、この値を設定しても無効になります。

ステップ 10　サービスのアクティブ化中に UNI ポートを閉じたままにするには、[UNI Shutdown] チェックボックスをオンにします。たとえば、サービス プロバイダーがネットワークでサービスを展開し、後でそのサービスをアクティブ化するような場合です。

ステップ 11　UNI ポートでキープアライブを設定するには、[Keep Alive] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフです。これによって、**no keepalive** コマンドは UNI ポートでプロビジョニングされます。これは、セキュリティのために CPE がキープアライブ パケットを U-PE に送信するのを防止します。この属性は、サービス要求単位での変更をサポートするために編集可能です。

ステップ 12　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目としてすべてのインターフェイス タイプを表示するには、[ANY] 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は、デフォルトでオンになっています。

ステップ 13　（このポリシーに基づいてサービス要求を作成する際に）UNI インターフェイスの選択項目として、タイプ UNI として定義されたすべてのインターフェイス タイプを表示するには、[UNI] 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は、デフォルトでオンになっています。

ステップ 14　[UNI MAC addresses] に 1 つ以上のイーサネット MAC アドレスを入力します。

この選択は、[Use Existing ACL Name] チェックボックスをオフにした場合にだけ表示されます。ポートで許可または拒否する MAC アドレスを入力するポップアップ ウィンドウを表示するには、[Edit] ボタンをクリックします。基礎 MAC アドレスとフィルタリングされた MAC アドレスを設定することで、アドレスの範囲を指定することもできます。

ステップ 15　[Link Speed]（任意）に [None]、[10]、[100]、[1000]、[Auto]、または [nonegotiate] を入力します。

ステップ 16　[Link Duplex]（任意）に [None]、[Full]、[Half]、または [Auto] を入力します。

ステップ 17　[PE/UNI Interface Description] フィールドに、*Customer-B EMS (EP-LAN) Service* などのようにオプションの説明を入力します。

ステップ 18　Prime Provisioning に VLAN ID を選択させる場合は、[VLAN ID AutoPick] 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しないと、サービスのアクティブ化中に [Provider VLAN ID] フィールドに VLAN を指定するよう求めるプロンプトが表示されます。

ステップ 19　VLAN を説明する名前を指定するには、[VLAN NAME]（任意）に入力します。

名前は、1 つのトークン（スペースは使用できません）にする必要があります。VLAN 名の制限は 32 文字です。名前は固有でなければなりません。2 つの VLAN が同じ名前を使用することはできません。

ステップ 20　[System MTU] にバイト単位で入力します。

最大伝送単位（MTU）サイズは設定可能で、省略可能です。Prime Provisioning は、このカスタマイズ済みの値について完全性チェックを実行しません。このサイズが受け入れられないために、サービス要求が [Failed Deploy] 状態になる場合は、サービス要求が展開されるまでサイズを調整する必要があります。Prime Provisioning では、次に示すように、異なるプラットフォームに対して複数の範囲がサポートされます。範囲は 1500 ～ 9216 です。

- 3750 および 3550 プラットフォームでは、MTU の範囲は 1500 ～ 1546 です。
- 7600 イーサネット ポートでは、MTU サイズは常に 9216 です。同じプラットフォームと同じ IOS リリースでも、さまざまなラインカードで MTU は異なるようにサポートされます。たとえば、古いラインカードは、MTU サイズとして 9216 だけを取り、新しいカードでは 1500 ～ 9216 がサポートされます。ただし、Prime Provisioning は両方のケースで 9216 を使用します。
- 7600 SVI（インターフェイス VLAN）では、MTU サイズは 1500 ～ 9216 です。

ステップ 21　独自の名前付きアクセス リストをポートに割り当てるには、[Use Existing ACL Name] チェックボックスをオンにします。

デフォルトでは、このチェックボックスはオフで、Prime Provisioning は、[UNI MAC addresses]（下記）に入力した値に基づいて、カスタマー側の UNI ポートで MAC ベースの ACL を自動的に割り当てます。

ステップ 22　[Port-Based ACL Name] に入力します（前のステップで説明したように、[Use Existing ACL Name] チェックボックスをオンにした場合）。

（注）　Prime Provisioning は、この ACL を自動的には作成しません。ACL はデバイスにすでに存在しているか、サービス要求を展開する前にテンプレートの一部として追加しておく必要があります。そうでない場合、展開は失敗します。

ステップ 23　UNI ポートで Cisco Discover Protocol（CDP）をディセーブルにするには、[Disable CDP] チェックボックスをオンにします。

ステップ 24　インターフェイスの通過が可能な MAC アドレスを制御することで、ポートのセキュリティ関連の CLI を UNI ポートに対してプロビジョニングするには、[UNI Port Security] チェックボックスをオンにします。

a. [Maximum Number of MAC address] には、ポート セキュリティで許可する MAC アドレスの数を入力します。

b. [Aging] には、MAC アドレスがポート セキュリティ テーブルに留まることができる時間の長さを入力します。

c. [Violation Action] では、ポート セキュリティ違反の検出時に実行されるアクションを選択します。

- [PROTECT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
- [RESTRICT] : 十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、[Security Violation] カウンタを増分させます。
- [SHUTDOWN] : インターフェイスをただちに errordisable 状態にして、SNMP トラップ通知を送信します。

d. [Secure MAC Addresses] フィールドに、1 つ以上のイーサネット MAC アドレスを入力します。

ステップ 25　UNI ポートがブロードキャスト、マルチキャスト、またはユニキャスト ストームによって中断されるのを防止するには、[Enable Storm Control] チェックボックスをオンにします。

トラフィックのタイプごとにしきい値を入力します。2 桁の数字で指定できる値は、ポートの使用可能な合計帯域幅のパーセントを表します。あるトラフィック タイプのしきい値に達すると、着信トラフィックがしきい値レベル未満になるまで、そのタイプのそれ以上のトラフィックは抑制されます。

ステップ 26　コア経由で他端にトンネリングできるレイヤ 2 ブリッジ プロトコル データ ユニット（BPDU）フレームを定義するには、[Protocol Tunnelling] チェックボックスをオンにします。

検査するプロトコルごとに、そのプロトコルのシャットダウンしきい値とドロップしきい値を入力します。

a. [Tunnel CDP] : Cisco Discover Protocol（CDP）のレイヤ 2 トンネリングをイネーブルにします。

b. [CDP Threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

c. [cdp drop threshold] : インターフェイスが CDP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

d. [Tunnel VTP] : VLAN Trunk Protocol（VTP; 仮想トランク プロトコル）のレイヤ 2 トンネリングをイネーブルにします。

e. [VTP threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

f. [vtp drop threshold] : インターフェイスが VTP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

g. [Tunnel STP] : スパニング ツリー プロトコル（STP）のレイヤ 2 トンネリングをイネーブルにします。

h. [STP Threshold] : インターフェイスがシャットダウンする前に受信する 1 秒あたりのパケット数を入力します。

i. [stp drop threshold] : インターフェイスが STP パケットのドロップを開始する時点で受信する、1 秒あたりのパケット数を入力します。

j. [Recovery Interval] : UNI ポートのリカバリを行うまで待機する時間（秒）を入力します。

ステップ 27　ポリシーのテンプレート サポートをイネーブルにするには、[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、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、「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。ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

（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。

ステップ 28　[Finish] をクリックします。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

VPLS サービス要求の管理

この項では、VPLS サービスの基本的なプロビジョニング ステップについて説明します。具体的な内容は、次のとおりです。

- 「Prime Provisioning をサポートするためのデバイス設定」（P.3-7）
- 「EVC サービス要求の作成」（P.3-37）
- 「CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-128）
- 「CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-132）
- 「VPLS サービス要求の変更」（P.3-173）
- 「[Bridge Domain ID] 属性の使用」（P.3-175）
- 「EVC サービス要求の保存」（P.3-58）

VPLS サービス要求の概要

VPLS サービス要求は、マルチポイント トポロジ内のさまざまなサイトを接続する 1 つ以上の接続回線からなります。サービス要求の作成時に、CE および PE ルータ上の特定のインターフェイスと UNI パラメータを含め、いくつかのパラメータを入力します。

また、Prime Provisioning テンプレートおよびデータ ファイルをサービス要求と関連付けることもできます。サービス要求でのテンプレートおよびデータ ファイルの使用について詳しくは、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。

サービス要求を作成するには、「VPLS ポリシーの作成」（P.3-138）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。定義済みの VPLS ポリシーに基づいて、オペレータは、VPLS ポリシーに変更を行うか、変更を行わずに、VPLS サービス要求を作成してサービスを展開します。サービス要求は、選択したポリシーと同じサービス タイプ（ERMS/EVP-LAN または EMS/EP-LAN）でなければなりません。サービスの作成と展開は一般に、ネットワーク プロビジョニングの毎日の操作として、担当のネットワーク技術者が実行します。

カスタマー サイト間のレイヤ 2 接続のためにサービス要求を作成する際に、次のステップを実行する必要があります。

- VPLS ポリシーを選択します。
- VPN を選択します。詳細については、「VPN の定義」（P.3-10）を参照してください。
- リンクを追加します。
- CE または UNI インターフェイスを選択します。
- CE または UNI インターフェイスに複数の NPC が存在する場合は、Named Physical Circuit（NPC; 名前付き物理回線）を選択します。
- リンク属性を編集します。

VPLS シナリオのサンプル コングレットについては、「サンプル コンフィグレット」（P.3-186）を参照してください。

VPLS サービス要求の作成

VPLS サービス要求を作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Create Service Request] 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　ポリシー選択機能を使用して、以前に作成したポリシーから VPLS ポリシーを選択します（「VPLS ポリシーの作成」（P.3-138）を参照）。

[L2VPN Service Request Editor] ウィンドウが表示されます。

新しいサービス要求は、すべての編集可能な機能と編集不可能な機能およびプリセットされたパラメータなど、その VPLS ポリシーのプロパティをすべて継承します。

ステップ 3　VPLS サービス要求の作成を続行するには、次のいずれかの項に移動します。

- 「CE が存在する ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-128）。
- 「CE が存在しない ERS（EVPL）、ATM、またはフレーム リレー L2VPN サービス要求の作成」（P.3-132）。

CE が存在する VPLS サービス要求の作成

ここでは、CE が存在する VPLS サービス要求を作成するための詳細なステップについて説明します。この例では、サービス要求は、ERMS（EVP-LAN）サービス タイプが指定され、CE が存在する MPLS コアを介した VPLS ポリシー用です。

次のステップを実行します。

ステップ 1　適切な VPLS ポリシーを選択します。

[Edit VPLS Link] ウィンドウが表示されます。

ステップ 2　この CE で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。選択したポリシーと同じサービス タイプ（ERMS/EVP-LAN または EMS/EP-LAN）が指定された VPN だけが表示されます。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このチェックボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

ステップ 3　[Select] 列で **VPN 名**を選択します。

ステップ 4　[Select] をクリックします。

[Edit VPLS Link] ウィンドウに VPN 名が表示されます。

ステップ 5　[Add Link] をクリックします。

ウィンドウが更新され、CE エンドポイントを指定できるようになります。

ステップ 6　[Description] フィールドにサービス要求の説明を入力できます。

説明は、このウィンドウと、[VPLS Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。

ステップ 7　[CE] 列の [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。

このウィンドウには、現在定義されている CE のリストが表示されます。

a.　[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。

b.　[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。

c.　[Rows per page] は [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

ステップ 8　[Select] 列で、VPLS リンクに対する CE を選択します。

ステップ 9　[Select] をクリックします。

[Edit VPLS Link] ウィンドウが開き、[CE] 列に選択された CE の名前が表示されます。

ステップ 10　インターフェイス選択機能から [CE Interface] を選択します。

（注）　ERMS（EVP-LAN）サービスをプロビジョニングする場合（および、あるデバイスに UNI を選択する場合）、同じ UNI を使用する他のサービスが存在するかどうかを Prime Provisioning が判別します。ある場合は、警告メッセージが表示されます。メッセージを無視して、サービス要求を保存すると、同じ UNI に依存する、基礎となるサービス要求はすべて、最新のサービス要求の変更された共有属性と同期されます。さらに、既存のサービス要求の状態は、[Requested] 状態に変更されます。

ステップ 11　[Circuit Selection] 列で [Select one circuit] をクリックします。

[Select NPC] ウィンドウが表示されます。選択した CE と CE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動的に入力される場合は、明示的に選択する必要はありません。

ステップ 12　[Select] 列から NPC の名前を選択します。

ステップ 13　[OK] をクリックします。

CE とインターフェイスを選択するたびに、この CE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

ステップ 14　この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。

[NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

ステップ 15　回線 ID は、回線の VLAN データに基づいて自動的に作成されます。

ステップ 16　VPLS ポリシーによって設定された値（つまり、VPLS ポリシーの作成中に [editable] とマークされた値）を編集するには、リンクの [Link Attributes] 列で [Edit] リンクをクリックします。

[Edit VPLS] ウィンドウが表示されます。

（注）　このウィンドウで属性の設定に関する詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

（注）　一部の VPLS サービス要求シナリオで表示される [Bridge Domain ID] 属性については、「VPLS サービス要求の変更」（P.3-173）を参照してください。

ステップ 17　必要に応じて、前のステップと同様に、追加の CE の指定を続けます。

ステップ 18　[OK] をクリックします。

ステップ 19　[Save] をクリックします。

サービス要求が作成され、Prime Provisioning に保存されます。

CE が存在しない VPLS サービス要求の作成

ここでは、CE が存在しない VPLS サービス要求を作成するための詳細なステップについて説明します。この例では、サービス要求は、EMS（EP-LAN）サービス タイプが指定され、CE が存在しない MPLS コアを介した VPLS ポリシー用です。

次のステップを実行します。

ステップ 1　適切な VPLS ポリシーを選択します。

[Edit VPLS Link] ウィンドウが表示されます。

ステップ 2　この PE で使用する VPN を選択するには、[Select VPN] をクリックします。

システムで定義された VPN が示された [Select VPN] ウィンドウが表示されます。選択したポリシーと同じサービス タイプ（ERMS/EVP-LAN または EMS/EP-LAN）が指定された VPN だけが表示されます。

（注）　VC ID が VPN ID からマップされます。デフォルトでは、Prime Provisioning はこの値を「自動選択」します。ただし、必要に応じてこれは手動で設定できます。これは、関連する VPN 設定を編集することで行います。[Edit VPN] ウィンドウには [Enable VPLS] チェックボックスがあります。このチェックボックスをオンにすると、表示されるフィールドに VPN ID を手動で入力できます。VPN の作成と変更の詳細については、「論理的インベントリの設定」（P.2-56）を参照してください。

ステップ 3　[Select] 列で **VPN 名**を選択します。

ステップ 4　[Select] をクリックします。

[Edit VPLS Link] ウィンドウに VPN 名が表示されます。

ステップ 5　[Add Link] をクリックします。

[Edit VPLS Link] ウィンドウが更新され、U-PE/PE-AGG/U-PE エンドポイントを指定できるようになります。ウィンドウで 1 つ以上のリンクを追加できます。

ステップ 6　最初の [Description] フィールドにサービス要求の説明を入力できます。

説明は、このウィンドウと、[VPLS Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。

ステップ 7　[N-PE/PE-AGG/U-PE] 列で [Select N-PE/PE-AGG/U-PE] をクリックします。

[Select PE Device] ウィンドウが表示されます。

このウィンドウには、現在定義されている PE のリストが表示されます。

a. [Show PEs with] ドロップダウン リストには、カスタマー名、サイト、またはデバイス名別に PE が表示されます。

b. [Find] ボタンを使用すると、特定の PE を検索するか、ウィンドウを更新できます。

c. [Rows per page] ドロップダウン リストを使用すると、ページを [5]、[10]、[20]、[30]、[40]、または [All] に設定できます。

ステップ 8　[Select] 列で、VPLS リンクの PE デバイス名を選択します。

ステップ 9　[Select] をクリックします。

[Edit VPLS Link] ウィンドウの [N-PE/PE-AGG/U-PE] 列に選択された N-PE/PE-AGG/U-PE の名前が表示されます。

ステップ 10　インターフェイス選択機能から [UNI Interface] を選択します。

（注）　ERMS（EVP-LAN）サービスをプロビジョニングする場合（および、あるデバイスに UNI を選択する場合）、同じ UNI を使用する他のサービスが存在するかどうかを Prime Provisioning が判別します。ある場合は、警告メッセージが表示されます。メッセージを無視して、サービス要求を保存すると、同じ UNI に依存する、基礎となるサービス要求はすべて、最新のサービス要求の変更された共有属性と同期されます。さらに、既存のサービス要求の状態は、[Requested] 状態に変更されます。

ステップ 11　PE ロール タイプが U-PE の場合は、[Circuit Selection] 列で [Select one circuit] をクリックします。

[Select NPC] ウィンドウが表示されます。選択した PE と PE インターフェイスに NPC が 1 つだけ存在し、その NPC が [Circuit Selection] 列に自動的に入力される場合は、明示的に選択する必要はありません。

（注）　PE ロール タイプが N-PE の場合は、列 [Circuit Selection] と [Circuit Details] はディセーブルです。

ステップ 12　[Select] 列から NPC の名前を選択します。

ステップ 13　[OK] をクリックします。

PE とインターフェイスを選択するたびに、この PE とインターフェイスから事前作成した NPC が [Circuit Selection] の下に自動的に表示されます。これは、リンクを完成させるために PE をさらに指定する必要はないことを意味します。

ステップ 14　この NPC の詳細を確認するには、[Circuit Details] 列で [Circuit Details] をクリックします。

[NPC Details] ウィンドウが表示され、この NPC の回線の詳細がリストされます。

回線 ID は、回線の VLAN データに基づいて自動的に作成されます。

ステップ 15　VPLS ポリシーによって設定された値（つまり、VPLS ポリシーの作成中に [editable] とマークされた値）を編集するには、リンクの [Link Attributes] 列で [Edit] リンクをクリックします。

（注）　このウィンドウで属性の設定に関する詳細については、「EVC サービス要求の変更」（P.3-57）を参照してください。

（注）　一部の VPLS サービス要求シナリオで表示される [Bridge Domain ID] 属性については、「VPLS サービス要求の変更」（P.3-173）を参照してください。

ステップ 16　必要に応じて、前のステップと同様に、追加の PE の指定を続けます。

ステップ 17　[Save] をクリックします。

VPLS サービス要求が作成され、Prime Provisioning に保存されます。

VPLS サービス要求の変更

VPLS リンクを変更する必要がある場合は、VPLS サービス要求を変更できます。リンクにテンプレートとデータ ファイルを関連付けることもできます。

次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

[Edit VPLS Link] ウィンドウが表示されます。

ステップ 4　設定での必要性に応じて、ウィンドウで項目を指定します。

- VPLS リンクを編集するには、青色で強調表示された値を選択します。

- [Add Link] をクリックして、VPLS リンクを追加します。
- [Delete Link] をクリックして、VPLS リンクを削除します。

（注）　テンプレートが追加されているサービス要求の廃止を試行する場合は、正しい方法の詳細について、「サービス要求のデコミッション」（P.8-12）を参照してください。

- 最初の [Description] フィールドにサービス要求の説明を入力できます。説明は、このウィンドウと、[Service Requests] ウィンドウの [Description] 列にも表示されます。このフィールドの最大長は 256 文字です。
- 回線 ID は、回線の VLAN データに基づいて自動的に作成されます。

ステップ 5　リンク属性を変更するには、VPLS リンク エディタに表示される [Link Attributes] 列の [Edit] をクリックします。

[Edit VPLS] ウィンドウが表示されます。

ステップ 6　必要に応じてリンク属性を編集します。

（注）　VPLS ポリシーで [VLANI D AutoPick] を選択しなかった場合は、[Provider VLAN ID] フィールドに VLAN を指定するよう求められます。

（注）　一部の VPLS サービス要求シナリオで表示される [Bridge Domain ID] 属性については、「VPLS サービス要求の変更」（P.3-173）を参照してください。

ステップ 7　リンクにテンプレートとデータ ファイルを追加するには、デバイス名を選択して、[Templates] 列にある [Add] 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。

（注）　テンプレートをリンクに追加するには、テンプレートをすでに作成してある必要があります。テンプレートを作成するための詳細な手順については、「概要」（P.9-1）を参照してください。サービス リクエスト内でのテンプレートおよびデータ ファイルの使用方法について詳しくは、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 8　[Add] をクリックします。

[Template Data File Chooser] ウィンドウが表示されます。

ステップ 9　左側のペインで、テンプレートにナビゲートして選択します。

関連付けられたデータ ファイルがメイン ウィンドウの行にリストされます。

ステップ 10　追加するデータ ファイルを確認して、[Accept] をクリックします。

テンプレートが示された [Add/Remove Templates] ウィンドウが表示されます。

ステップ 11　テンプレート名を選択します。

ステップ 12　[Action] で、ドロップダウン リストを使用して [APPEND] または [PREPEND] を選択します。

[Append] は、テンプレートによって生成された CLI を通常の Prime Provisioning（非テンプレート）CLI に追加するよう Prime Provisioning に指示します。[Prepend] は逆で、テンプレートを Prime Provisioning CLI に追加しません。

ステップ 13　このサービス要求にこのテンプレートを使用するには、[Active] を選択します。

[Active] を選択しないと、テンプレートは使用されません。

ステップ 14　[OK] をクリックします。

テンプレートが追加された状態で、[Edit VPLS] ウィンドウが表示されます。

ステップ 15　[OK] をクリックします。

[Edit VPLS Link] ウィンドウが表示されます。

ステップ 16　VPLS リンクの編集が終了したら、[Save] をクリックします。

[Bridge Domain ID] 属性の使用

ブリッジ ドメイン ID 属性は、一部の VPLS サービス要求シナリオの [Link Attributes] ウィンドウに表示されます。

[Bridge Domain ID] 属性を使用するには、[Bridge Domain ID] テキスト フィールドに ID 番号を入力して、VPLS サービス要求のブリッジ ドメイン機能をイネーブルにします。

許容可能な値は 1 ～ 4294967295 です。

使用方法に関する注釈：

- [Bridge Domain ID] 属性は、次のサービス要求シナリオだけで使用可能です。
  - CE が存在する Ethernet/ERMS（EVP-LAN）
  - CE が存在しない Ethernet/ERMS（EVP-LAN）
  - CE が存在する Ethernet/EMS（EP-LAN）
  - CE が存在しない Ethernet/EMS（EP-LAN）
- [Bridge Domain ID] 属性は、IOS 12.0(32)SY6 が実行され、N-PE ロールで機能している Cisco GSR 12406 だけでサポートされます。この属性は、このプラットフォームのサービス要求だけで表示されます。それ以外の場合は、属性は、サービス要求の [Link Attributes] ウィンドウからフィルタリングされます。
- 次の点が、このポリシーに基づくサービス要求に適用されます。
  - N-PE（GSR プラットフォーム）が UNI デバイスとして使用される場合は、標準の UNI 属性は、サービス要求ワークフローの [Link Attributes] ウィンドウに表示されません。
  - U-PE（非 GSR プラットフォーム）が UNI デバイスとして使用される場合は、標準の UNI 属性はすべて、サービス要求ワークフローの [Link Attributes] ウィンドウに表示されます。
  - VPLS EMS サービスでは、GSR デバイス（N-PE）で終端する同じ回線で U-PE（非 GSR プラットフォーム）を使用する必要があります。つまり、NPC 回線を使用して、GSR デバイスで VPLS EMS をプロビジョニングする必要があります。

VPLS サービス要求の保存

VPLS サービス要求を保存するには、次のステップを実行します。

ステップ 1　すべての接続回線の属性の設定が終了したら、[Save] をクリックして、VPLS サービス要求の作成を終了します。

VPLS サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウにサービス要求のリスト表示されます 新しく作成された VPLS サービス要求が [REQUESTED] の状態で追加されます。

ステップ 2　ただし、何らかの理由で（たとえば、選択した値が範囲外である）VPLS サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。

そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

サービス要求の展開、モニタリング、および監査

L2VPN、VPLS、または EVC ポリシーをネットワーク デバイスに適用するには、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」を参照してください。これらのタスクについては、その章を参照してください。

この項では、EVC、L2VPN および VPLS サービスのサービス要求タスクの管理に固有の問題について説明します。

導入前の変更点

EVC、L2VPN、または VPLS のサービス要求を展開する前に、Dynamic Component Properties Library（DCPL）パラメータ **actionTakenOnUNIVlanList** を変更できます。この変更は、[trunk allowed vlan] のリストが User Network Interface（UNI; ユーザ ネットワーク インターフェイス）上に存在しない場合に必要になります。

この変更を行うには、次のステップを実行します。

ステップ 1　[Administration] > [Hosts] を選択します。

ステップ 2　変更するホストを選択します。

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　[DCPL properties] パネルで、[Provisioning] > [Service] > [shared] > [actionTakenOnUNIVlanList] を選択します。

属性の詳細が表示されます。

ステップ 5　[New Value] ドロップダウン リストで、次のいずれかを選択します。

- [prune] : Prime Provisioning は最小 VLAN リストを作成します。これはデフォルトです。
- [abort] : Prime Provisioning は「trunk allowed vlan list is absent on ERS UNI」というエラー メッセージを表示し、L2VPN または VPLS のサービス要求のプロビジョニングを停止します。
- [nochange] : Prime Provisioning はすべての VLAN を許可します。

ステップ 6　[Set Property] をクリックします。

L2 サービスに対する自動検出の使用

すべてのディスカバリ ステップは、検出ワークフローに統合され、Prime Provisioning GUI から制御します。これには、Prime Provisioning 内で [Inventory] > [Discovery] からアクセスします。次のディスカバリ機能がサポートされています。

- ファイルに基づくデバイス ディスカバリがサポートされています。
- ルールに基づくデバイス ロールの割り当てがサポートされています。
- ディスカバリの進捗メッセージおよびログを GUI で表示し、ディスカバリのさまざまな段階を追跡できます。
- XML データ ファイルにより、プロバイダー、カスタマー、サイト、およびリージョン オブジェクトの一括作成が可能です。

Prime Provisioning で自動検出機能を使用するステップの詳細については、付録 E「インベントリ - ディスカバリ」を参照してください。

EVC サービス要求を使用したデバイス上での VPLS 自動検出のプロビジョニング

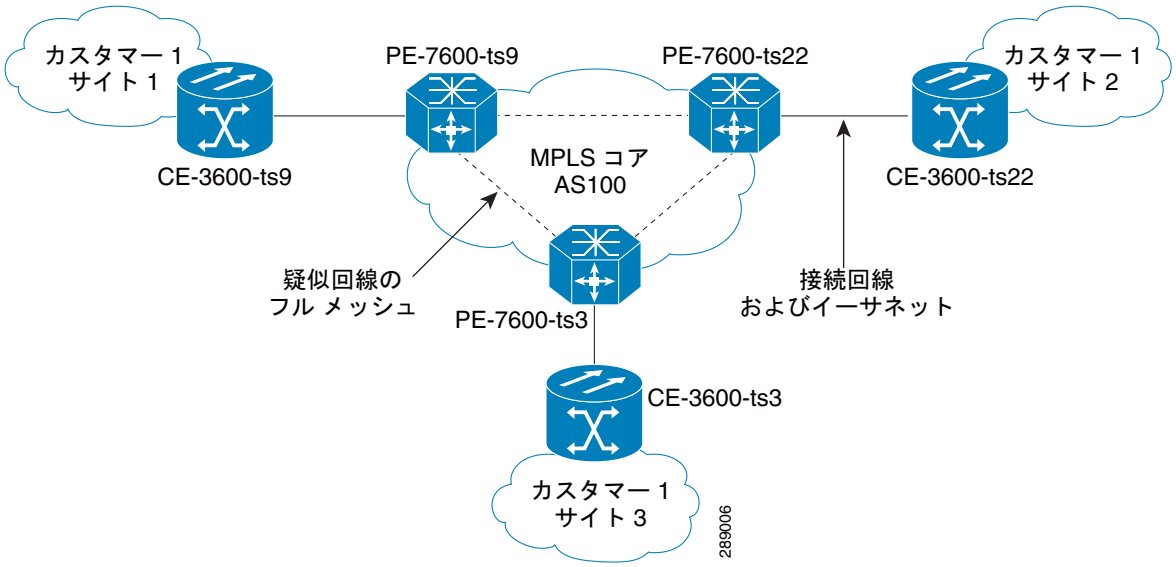
この項では、Prime Provisioning で VPLS 自動検出をイネーブルにする方法について説明します。次の事項について説明します。

概要

IOS および IOS XR での VPLS の初期実装では、VPLS ドメインに対してデバイスが追加または削除されるときに、各 VPLS PE ネイバーを手動で設定する必要がありました。VPLS の自動検出によって、VPLS ネイバーを手動で設定する必要がなくなります。この機能により、同じ VPLS ドメイン内の PE が検出され、ドメインに対して PE が追加または削除されると、自動的にそれが検出されます。

図 3-1 には、この項で参照される VPLS トポロジの例が示されています。3 台の PE デバイスが、VPLS ドメインでネイバーを構成しています。ドメインに対して PE が追加または削除されると、VPLS の自動検出機能によって PE 構成は交信された状態を保ちます。

図 3-1　VPLS 自動検出トポロジの例



VPLS ドメインの PE デバイスで VPLS の自動検出をプロビジョニングするには、2 種類の基本タスクを実行する必要があります。

- デバイス上の一部のコンフィグレットが Prime Provisioning によってプロビジョニングされる前に、それらを事前設定する必要があります。これは、手動またはテンプレートを使用して行う必要があります。「VPLS 自動検出をサポートするための PE デバイスの事前設定」（P.3-179）を参照してください。
- VPLS ドメインでの PE のプロビジョニングに使用する EVC サービス要求内で、VPLS の自動検出をイネーブルにする必要があります。

この項の残りの部分には、VPLS 自動検出の制限事項と制約事項が記載されています。また、それをイネーブルにするためのワークフローで実行する必要のある手順を説明し、IOS および IOS XR デバイスで生成されるサンプル コンフィグレットを提供します。

VPLS 自動検出の制限事項および制約事項

VPLS 自動検出 Prime Provisioning を使用する場合は、次の制限事項と制約事項に注意してください。

- VPLS 自動検出を使用するには、VPLS ドメインのすべての PE デバイスで VPLS 自動検出をイネーブルにする必要があります。混在トポロジ（つまり、および一部の PE は VPLS 自動検出がイネーブルに設定されており、一部の PE はイネーブルに設定されていない状況）はサポートされません。VPLS ディスカバリ モードは、同じ仮想転送インターフェイス（VFI）の下のすべてのサービス要求に対してイネーブルにする必要があります。
- VPLS ドメインの PE で、事前設定が必要な場合があります。「VPLS 自動検出をサポートするための PE デバイスの事前設定」（P.3-179）を参照してください。
- VPLS 自動検出を使用する場合、スプリット ホライズンをイネーブルにする必要があります。
- VPLS 自動検出は、[MPLS Core Connectivity Type] が [VPLS] に設定されている EVC イーサネット サービス要求を使用する Prime Provisioning にのみ設定できます。この機能は、他の Prime Provisioning サービス要求と接続タイプではサポートされません。

- 2 つの PE ピア間に疑似回線を作成するために、同じ検出メカニズムを使用する必要があります。同じ VFI で自動検出された疑似回線と手動で設定された疑似回線の両方を同じピア PE に伝達することはできません。たとえば、PE1 を PE2 に対して手動で設定し、PE1 を検出するように PE2 を動的に設定することはできません。
- 必要なサービスで VPLS ディスカバリ モードが（手動または自動検出として）プロビジョニングされた後、それを変更することはできません。
- VPLS 自動検出は、階層型 VPLS（H-VPLS）のようなハブ アンド スポーク トポロジではなく、フルメッシュ トポロジに対してのみサポートされます。
- VPLS 自動検出は、相互自律システム設定ではサポートされません。

VPLS 自動検出をサポートするための PE デバイスの事前設定

IOS および IOS XR デバイスで VPLS を自動検出する前に、次のコンフィグレットをそれらのデバイスで事前設定する必要があります。これらのコンフィグレットは、他の PE との MP iBGP ピアリングを設定し、同じ VPLS ドメイン内で他の PE との VPLS L2VPN コミュニティ情報交換をイネーブルにするために必要です。

```
!  Setup MP-iBGP peering with other PEs  !
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 193.193.20.3 remote-as 100
 neighbor 193.193.20.3 update-source Loopback0
 neighbor 193.193.20.5 remote-as 100
 neighbor 193.193.20.5 update-source Loopback0

 ! Enable VPLS l2vpn community info exchange with other PEs in the same VPLS domain  !
address-family l2vpn vpls
 neighbor 193.193.20.3 activate
 neighbor 193.193.20.3 send-community extended
 neighbor 193.193.20.5 activate
 neighbor 193.193.20.5 send-community extended
 exit-address-family
      !
```

EVC のワークフローでの VPLS 自動検出のイネーブル化

EVC イーサネット ワークフローで VPLS 検出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　EVC イーサネット ポリシーまたはサービス要求ワークフローでは、[MPLS Core Connectivity Type] を [VPLS] に設定します。

コア接続が VPLS である場合、[Discovery Mode] 属性は [EVC Service Request Editor] ウィンドウの [Service Request Details] セクションに動的に表示されます。このウィンドウには、接続回線間の VPLS 接続の説明が表示されます。VPLS 接続で、直接接続リンクまたは L2 アクセス リンクを使用して、2 つのカスタマー サイト間でのマルチポイント接続を作成できます。

ステップ 2　[EVC Service Request Editor] ウィンドウで、[Discovery Mode] タイプを選択します。

選択できる基準は、次のとおりです。

- [Manual] : [Manual] オプションが選択されている場合、**vfi** コマンドは **manual** オプションとともにレガシーの場合のように設定されます。これは、IOS デバイスと IOS XR デバイスの両方で同じです。実装されるシグナリング プロトコルは LDP です。

- [Auto Discovery] : [Auto Discovery] オプションが選択されている場合、**vfi** コマンドは **autodiscovery** オプションとともに設定され、**neighbor** コマンドは必要ありません。

これらの選択によって生成される結果のコンフィグレットの例については、「サンプル コンフィグレット」（P.3-180）を参照してください。

ステップ 3　サービス要求を保存し、VPLS ドメインのデバイスに展開します。

サンプル コンフィグレット

この項では、VPLS 自動検出用に IOS と IOS XR デバイスの両方に Prime Provisioning によって生成されるサンプル コンフィグレットを提供します。

IOS デバイスのサンプル コンフィグレット

```
! Setup VPLS intstance,!
l2 vfi customer1 autodiscovery
 vpn id 100

! Set attachment circuit interface in VLAN mode  !
interface FastEthernet4/1
 description VPN for CE9-3640-ts22
 switchport
 switchport access vlan 100
 switchport mode access
 no cdp enable

! Bind VLAN100(AC) to the customer1 pseudowire !
interface Vlan100
 no ip address
 xconnect vfi customer1
```

IOS XR デバイスのサンプル コンフィグレット

```
l2vpn
bridge group abc
  bridge-domain east
   vfi vfiname
    vpn-id 678
    autodiscovery bgp
     rd auto
     route-target 456:567
```

（注）　IOS XR デバイスの場合、ルート ターゲット値は VPN の作成時に保存する必要があります。

L2VPN ERS（EVPL）サービスの VLAN 変換の設定

この項では、L2VPN ERS（EVPL）サービスに VLAN 変換を設定する方法についての補足情報を提供します。具体的な内容は、次のとおりです。

- 「VLAN 変換の概要」（P.3-181）
- 「VLAN 変換の設定」（P.3-181）図 3-1

- 「プラットフォーム固有の使用上の考慮事項」（P.3-185）

（注）　VLAN 変換を使用してポリシーおよびサービスを作成する前に考慮すべき有用な情報については、「プラットフォーム固有の使用上の考慮事項」（P.3-185）を確認してください。

VLAN 変換の概要

VLAN 変換は、VLAN およびメトロ イーサネット関連のサービスを管理する場合に柔軟性を提供します。VLAN 変換には、1 対 1 変換（1:1）および 2 対 1 変換（2:1）の 2 種類があります。この機能は、L2VPN ERS（EVPL）で（CE あるなしにかかわらず）利用できます。L2VPN ERS（EVPL）サービスの動作は、1 つの Q-in-Q ポートを EWS（EPL）および ERS（EVPL）の両サービスで共有することが可能になった現在も変わらず同一です。VLAN 変換はイーサネット インターフェイス専用です。ATM やフレーム リレーなど他のタイプのインターフェイスでは使用しません。

1:1 VLAN 変換では、着信トラフィックの VLAN（CE VLAN）はもう一方の VLAN（PE VLAN）に置き換えられます。これは、同一 CE VLAN を共有する 2 人の別々のカスタマーからトラフィックが着信する状況をサービス プロバイダーが処理できるようなったことを意味します。SP はこの 2 つの CE VLAN をそれぞれ別の PE VLAN にマップできるため、カスタマー トラフィックが混同されることはありません。

2:1 VLAN 変換では、U-PE UNI ポートでのダブル タグ（Q-in-Q）トラフィックを、サービスを多重化するために複数のフローにマップできます。変換は、CE VLAN（内部タグ）と PE VLAN（外部タグ）との組み合わせに基づいて実行されます。この変換を行わないと、Q-in-Q ポートからのすべてのトラフィックが 1 箇所にだけ集中する可能性があります。これは、トラフィックのスイッチングが外部タグだけで行われるためです。

VLAN 変換の設定

ここでは、VLAN 変換をサポートするためのポリシーおよびサービス要求の作成方法と管理方法について説明します。

- 「ポリシーの作成」（P.3-181）
- 「サービス要求の作成」（P.3-182）
- 「サービス要求の変更」（P.3-184）
- 「サービス要求の削除」（P.3-184）

ポリシーの作成

VLAN 変換は、ERS の L2VPN（EVPL）で、（CE のあるなしにかかわらず）のポリシー作成中に指定します。L2VPN（ポイントツーポイント）Editor のウィンドウには、[VLAN Translation] という名前の新規オプションが含まれています。

VLAN 変換には次の 3 つのオプションがあります。

- [No]：これはデフォルトの選択肢です。VLAN 変換は実行されません。

（注）　[No] を選択し、サービス要求の作成中に VLAN 変換に関するすべての動作も希望しない場合、[Editable] チェックボックスをオフにします。これが VLAN 変換なしを選択した場合の推奨手順です。

- [1:1] : 1:1 VLAN 変換。着信トラフィックの VLAN（CE VLAN）は、もう一方の VLAN（PE VLAN）に置き換えられます。「サービス要求の作成」（P.3-182）で説明するように、VLAN 変換の指定は、ポリシーのサービス要求の作成中に行います。
- [2:1] : 2:1 VLAN 変換。U-PE UNI ポートでのダブル タグ（Q-in-Q）トラフィックを、サービスを多重化するために複数のフローにマップできます。2:1 VLAN 変換を選択すると、2:1 VLAN 変換の実行場所を選択できるように、L2VPN（ポイントツーポイント）Editor のウィンドウが動的に変更されます。

2:1 VLAN 変換は、次のいずれかを選択して行います。

- [Auto]（これがデフォルトの選択です）。
- U-PE
- PE-AGG
- N-PE

[Auto] を選択すると、UNI ポートに最も近いデバイスで 2:1 VLAN 変換が行われます。これ以外の選択肢は、2:1 VLAN 変換を実行できる場所が 2 箇所以上ある場合にだけ有効です。この変換を実行可能な場所が 1 箇所だけの場合は、これ以外の選択肢は無視されます。

実際の VLAN 値は、このポリシーに基づいてサービス要求を作成するときに指定します。「サービス要求の作成」（P.3-182）を参照してください。

サービス要求の作成

L2VPN ERS（EVPL）ポリシーに基づいてサービス要求を作成するときは、ポリシーで編集可能と設定されているかのように VLAN オプションを変更できます。ユーザは、VLAN 変換のタイプと変換の実施場所について、ポリシーの情報を上書きできます。このような柔軟性により、次のプロビジョニングが可能になります。

- 1 箇所の AC で 2:1 VLAN 変換を行い、別の AC では VLAN 変換を行わないか、1:1 VLAN 変換を行います。
- 1 箇所の AC の VLAN 変換を UNI ボックス上で実行可能とし、他の AC の変換を PE-AGG で実行可能とします。

（注） このような変更は、サービス要求を新規作成する場合にだけ行うことができることに注意してください。既存のサービス要求の変更時には許可されません。

VLAN 変換の指定は、[Link Attributes] ウィンドウ内でサービス要求作成中に行われます。この時点で、変換元の VLAN と変換先の VLAN を指定できます。[Attachment Tunnel Editor] ウィンドウで UNI ポートを選択した後に、[Link Attributes] ウィンドウにアクセスします。VLAN 変換タイプは UNI の選択後に設定できるため、UNI ポートの表示リストからはいずれのタイプの UNI ポートも除外されません。これには次の理由があります。

- （[Link Attributes] ウィンドウで）VLAN を実施しない、または 1:1 VLAN 変換を実施すると後で決定した場合に備えて、UNI ポートのリストに通常のトランク ポートを含める必要があります。
- 2:1 VLAN 変換の実施を決定した場合に備えて、UNI ポートのリストには、EWS（EPL）（Q-in-Q）ポートを含める必要があります。

VLAN 変換を開始するためにポートをすべて備えているにもかかわらず、VLAN 変換のタイプに応じて特定のタイプのポートを選択する必要があります。具体的には、次のように選択します。

- VLAN 変換を実施しないか、1:1 VLAN 変換を実施する場合は、空のポートかトランク ポートを UNI として選択する必要があります。

- 2:1 VLAN 変換の場合は、空のポートか Q-in-Q ポートを UNI ポートとして選択する必要があります。

使用する適切なポートを判別しやすくするために、[Attachment Tunnel Editor] ウィンドウの [Details] ボタンをクリックして、ポートのタイプとそのポートに関連付けられているサービスを表示できます。

次の項では、[Link Attribute] ウィンドウで行う、さまざまなタイプの VLAN 変換ごとの VLAN 変換の定義方法について説明します。

VLAN 変換なし

VLAN 変換なしを選択した場合は、情報の追加は不要です。

1:1 VLAN 変換

1:1 VLAN 変換を選択すると、ウィンドウは動的に変更されます。

空白のフィールドに、変換元とする CE VLAN を入力する必要があります。VLAN 番号は 1 ～ 4096 の数字にする必要があります。

変換元の CE VLAN からの変換先となる PE VLAN には、「自動選択」を選択することも、手動で入力することもできます。([Link Attributes] ウィンドウの上方に表示される）[VLAN ID AutoPick] チェックボックスをオンにすると、PE VLAN が自動的に割り当てられます。

[VLAN ID AutoPick] チェックボックスをオフにすると、ウィンドウに [Provider VLAN ID] が表示され、手動で PE VLAN を入力できます。

サービス要求の作成が終了すると、Prime Provisioning はサービス要求を保存する前に整合性チェックを行います。1 対 1 の VLAN 変換では、同一ポート上で別の 1 対 1 の VLAN 変換に CE VLAN が使用されていると、Prime Provisioning はサービス要求を拒否します。

2:1 VLAN 変換

2:1 VLAN 変換を選択すると、ウィンドウは動的に変更されます。

（注） UNI ポートが EWS（EPL）サービスでプロビジョニングされている場合、外部 VLAN 値はグレー表示になります。

2:1 VLAN 変換では、次の 3 つの VLAN が関与します。

- 「A」: 変換元の CE VLAN。ユーザは [From CE VLAN] フィールドでこの値を指定します。範囲外の変換の場合は、「*」（アスタリスク文字）の値を指定する必要があります。
- 「B」: Q-in-Q ポートの外部 VLAN である PE VLAN。ユーザは [Outer VLAN] フィールドでこの値を指定します。この VLAN は、値を入力して手動で選択するか、[AutoPick] チェックボックスをオンにして自動的に割り当てることができます。
- 「C」:「A」および「B」VLAN の変換先となる PE VLAN。これは、前述の [VLAN and Other Information] で指定します（[Link Attributes] ウィンドウ）。

ユーザは VLAN「A」（CE VLAN）および VLAN「C」（変換先の PE VLAN）を指定する必要があります。VLAN「B」（Q-in-Q 外部 VLAN）の場合、指定する内容は UNI ポートのタイプによって次のように異なります。

- ポートが空の場合、VLAN「B」を指定する必要があります。
- 既存の Q-in-Q ポートで VLAN「B」が定義されている場合、この時点での変更はできません。

2:1 VLAN 変換には、次の考慮事項があります。

- 2:1 VLAN 変換の場合、空のポートで ERS（EVPL）サービスをビルドすると、この UNI ポートは ERS（EVPL）サービスとしてプロビジョニングされます。後で同一ポートに EWS（EPL）サービスを追加すると、EWS（EPL）サービスによって直前の ERS（EVPL）プロビジョニングが上書きされます。ERS（EVPL）と EWS（EPL）の主な相違点は、L2PT BPDU の対応です。ERS（EVPL）では、BPDU がブロックされます。EWS（EPL）の場合は、BPDU はトンネリングされます。
- 2:1 VLAN 変換は、ERS（EVPL）サービスとして、通常の ERS（EVPL）ポートとまったく同じように同一ポートを共有できます。
- ERS（EVPL）2:1 サービスは、既存の EWS（EPL）サービスの最上部に追加できます。

サービス要求の作成が終了すると、Prime Provisioning はサービス要求を保存する前に整合性チェックを行います。2 対 1 の VLAN 変換では、CE VLAN と外部タグの PE VLAN の組み合わせが同一ポート上で別の 2 対 1 の VLAN 変換に使用されていると、Prime Provisioning はサービス要求を拒否します。

サービス要求の変更

1:1 および 2:1 VLAN 変換では両方とも、既存のサービス要求について次の変更が行えます。

- 変換元を新規 CE VLAN に変更する。
- サービス要求に関する他のすべての通常変更を許可する。

ただし、次の変更は許可されません。

- 指定の AC では VLAN 変換のタイプを変更できません。たとえば、2:1 から 1:1 の VLAN 変換には変更できません。
- 2:1 VLAN 変換の実施場所は変更できません。

サービス要求の削除

サービス要求の削除中に、次のようなリソースが解放されます。

1:1 VLAN 変換：

- CE VLAN が再び変換可能になります。
- PE VLAN が解放されます。
- 削除されたリンクが UNI ポート上の最後のリンクの場合、このポートは新規に設定されます。

2:1 VLAN 変換：

- CE VLAN が再び変換可能になります。
- 「変換先」の PE VLAN が解放されます。
- 削除されたリンクがこの UNI ポート上の最後の「CE-PE」ペアで、このポート上に EWS（EPL）サービスが存在しない場合は、このポートは新規に設定されます。さらに、外部 VLAN が解放されます。

プラットフォーム固有の使用上の考慮事項

VLAN 変換は、7600 および 3750 ME プラットフォームで利用できます。7600 と 3750 ME では VLAN 変換のサポートに違いがあります。コマンド構文が異なるだけでなく、VLAN 変換の実施場所も違います。7600 で 1:1 VLAN 変換を行う場合、PFC カード上で操作します。2:1 VLAN 変換の場合は、アップリンク GE-WAN（OSM モジュール）で操作します。これが 3750 ME の場合は、両変換ともアップリンク（ES ポート）で行われます。

3750 の VLAN 変換

3750 で VLAN 変換を行う場合、次の事項に注意してください。

- VLAN 変換を行う 3750 の場合は、ロールを N-PE ではなく、U-PE または PE-AGG として指定する必要があります。
- アップリンク（ES）ポートの VLAN 変換は、Gigabit 1/1/1 または Gigabit 1/1/2 ポートで行う必要があります。
- 3750 PE で構成されるリング上で 1:1 VLAN 変換を行う場合、すべての 3750 が ES ポート（「東」ポートと「西」ポート）をアップリンク ポートして使用して他のリング ノードと接続するようにします。

7600 の VLAN 変換

7600 で VLAN 変換を行う場合は、次の事項に注意してください。

- 1:1 VLAN 変換は、常に UNI ポート上で行われます。ただし、すべてのイーサネット インターフェイスで 1:1 VLAN 変換をサポートするわけではありません。このサポートはラインカードによって異なります。
- 2:1 VLAN 変換は常に GE-WAN ポートで実行されます。ポートは NNI アップリンク ポートにする必要があります。
- 2:1 VLAN 変換は、N-PE ではなく、U-PE または PE-AGG の 7600 だけで行われます。これは、GE-WAN インターフェイス上で 2:1 VLAN 変換を行うと、変換後の新しい VLAN を使用した L3VPN および L2VPN のサービスをこのインターフェイスで提供できなくなるためです。L3/L2VPN サービスは別の（N-PE）ボックスでプロビジョニングする必要があります。

ハードウェアが VLAN 変換をサポートしない場合のサービス要求の失敗

1:1 VLAN 変換機能では、ターゲット ハードウェア（ラインカード）が VLAN 変換をサポートしない場合、サービス要求は [Fail Deployed] 状態になります。サービス要求が [Invalid] 状態ではなく [Fail Deployed] 状態になるのは、特定のラインカードで VLAN 変換の CLI コマンドを受け入れるかまたは拒否するかを Prime Provisioning が事前に検知しないことが理由です。この場合、Prime Provisioning はコマンドをプッシュ ダウンしようとし、導入は失敗します。[Invalid] 状態とは、Prime Provisioning がなんらかの不正を（事前に）検出し、プロビジョニング タスクをアボートすることを意味します。この場合、CLI はプッシュ ダウンされません。指定のハードウェアでサポートする機能がない場合、これが一般的な Prime Provisioning の動作です。この場合は、目的のサービスをサポートするために適切なハードウェアをユーザの責任で選択します。

サンプル コンフィグレット

この項では、Prime Provisioning の L2VPN およびメトロ イーサネット サービス プロビジョニングのサンプル コンフィグレットを提供します。具体的な内容は、次のとおりです。

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）　太字で示してある CLI が最も関連するコマンドです。

（注）　この項にあるすべての例は MPLS コアを前提としています。

ERS（EVPL）（ポイントツーポイント）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）（ポイントツーポイント）。
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。
    インターフェイス：FA8/17。
  - U-PE は、12.2(25)EY1 を備えた、ポートセキュリティなしの Cisco 3750ME です。
    インターフェイス：FA1/0/4 – FA1/0/23。
  - L2VPN ポイントツーポイント。

コンフィグレット

U-PE

```
vlan 772
exit
!
interface FastEthernet1/0/23
switchport trunk allowed vlan 500,772
!
interface FastEthernet1/0/4
no cdp enable
no keepalive
no ip address
switchport trunk allowed vlan 500,772
spanning-tree bpdufilter enable
mac access-group ISC-FastEthernet1/0/4 in
!
mac access-list extended
ISC-FastEthernet1/0/4
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
```

N-PE

```
vlan 772
exit
!
interface FastEthernet8/17
switchport trunk allowed vlan
1,451,653,659,766-768,772,878
!
interface Vlan772
no ip address
description L2VPN ERS
xconnect 99.99.8.99 89027 encapsulation
mpls
no shutdown
```

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。カスタマー BPDU は PACL によってブロックされます。

ERS（EVPL）（ポイントツーポイント、UNI ポート セキュリティ）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：UNI ポート セキュリティのある ERS（EVPL）（ポイントツーポイント）。
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、OSM を備えた Cisco 7600 です。インターフェイス：FA2/18。
  - U-PE は IOS 12.2(25)SEC2 を備えた Cisco 3550 です。ポート セキュリティはイネーブルです。インターフェイス：FA3/31– FA3/23。
  - L2VPN ポイントツーポイント。

コンフィグレット

U-PE

```
vlan 788
exit
!
interface FastEthernet3/23
no ip address
switchport trunk allowed vlan 783,787-788
!
interface FastEthernet3/31
no cdp enable
no keepalive
no ip address
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan none
switchport trunk allowed vlan 788
switchport port-security
switchport nonegotiate
switchport port-security maximum 45
switchport port-security aging time 34
switchport port-security violation shutdown
switchport port-security mac-address
3456.3456.5678
spanning-tree bpdufilter enable
mac access-group ISC-FastEthernet3/31 in
!
mac access-list extended
ISC-FastEthernet3/31
deny any host 0100.0ccc.cccc
deny any host 0100.0ccc.cccd
deny any host 0100.0ccd.cdd0
deny any host 0180.c200.0000
deny any host 1234.3234.3432
permit any any
```

N-PE

```
vlan 788
exit
!
interface FastEthernet2/18
switchport trunk allowed vlan
350,351,430,630,777,780,783,785-788
!
interface Vlan788
no ip address
description L2VPN ERS with UNI port
security
xconnect 99.99.5.99 89028 encapsulation
mpls
no shutdown
```

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。カスタマー BPDU は PACL によってブロックされます。
- さまざまな UNI ポート セキュリティ コマンドがプロビジョニングされます。
- ユーザ定義 PACL エントリがデフォルト PACL に追加されます。

ERS（EVPL）（1:1 VLAN 変換）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：1:1 VLAN 変換を備えた ERS（EVPL）。
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。

    インターフェイス：FA8/34。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。NNI ポート（アップリンク）上の VLAN 変換。

    インターフェイス：FA1/0/8 – GI1/1/1。
  - L2VPN ポイントツーポイント。

コンフィグレット

U-PE	N-PE
! **vlan 123** exit ! interface FastEthernet1/0/8 no cdp enable no keepalive no ip address **switchport trunk allowed vlan 123** switchport nonegotiate switchport port-security maximum 34 switchport port-security aging time 23 switchport port-security violation protect switchport port-security spanning-tree bpdufilter enable mac access-group ISC-FastEthernet1/0/8 in ! interface GigabitEthernet1/1/1 no ip address switchport mode trunk **switchport trunk allowed vlan 1,123** **switchport vlan mapping 123 778**	vlan 778 exit ! interface FastEthernet8/34 switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,778 ! interface Vlan778 no ip address description L2VPN ERS 1 to 1 vlan translation xconnect 99.99.8.99 89032 encapsulation mpls no shutdown

コメント

- VLAN 変換は、L2VPN（ポイントツーポイント）ERS（EVPL）対してだけ可能です。
- この場合、U-PE（3750）で 1:1 VLAN 変換が実行されます。NNI（アップリンク）ポートでプロビジョニングされます。
- カスタマー VLAN 123 はプロバイダー VLAN 778 に変換されます。

ERS（EVPL）（2:1 VLAN 変換）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：VLAN 2:1 変換対応の ERS（EVPL）。デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。

    インターフェイス：FA8/34。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。NNI ポート（アップリンク）上の VLAN 変換。

    インターフェイス：FA1/0/5 – GI1/1/1。
  - L2VPN ポイントツーポイント。

コンフィグレット

U-PE	N-PE
vlan 567 exit ! interface FastEthernet1/0/5 no cdp enable no keepalive no ip address switchport **switchport access vlan 567** **switchport mode dot1q-tunnel** switchport trunk allowed vlan none switchport nonegotiate spanning-tree bpdufilter enable mac access-group ISC-FastEthernet1/0/5 in ! interface GigabitEthernet1/1/1 no ip address switchport trunk allowed vlan 1,123,567 **switchport vlan mapping dot1q-tunnel 567 234 779** ! mac access-list extended ISC-FastEthernet1/0/5 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	vlan 779 exit ! interface FastEthernet8/34 switchport trunk allowed vlan 1,778-779 ! interface Vlan779 no ip address description L2VPN ERS 2 to 1 vlan translation xconnect 99.99.8.99 89033 encapsulation mpls no shutdown

コメント

- VLAN 変換は、L2VPN（ポイントツーポイント）ERS（EVPL）対してだけ可能です。
- この場合、U-PE（3750）で 2:1 VLAN 変換が実行されます。NNI（アップリンク）ポートでプロビジョニングされます。
- （Q -in-Q の一部としての）カスタマー VLAN 123 およびプロバイダー VLAN 234 が新規プロバイダー VLAN 779 へ変換されます。

ERS（疑似回線クラス、E-Line、L2VPN グループ名、IOS XR デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）。
- デバイス設定：
  - N-PE は IOS XR 3.6.1 以降を備えた CRS-1 です。
  - N-PE 上の UNI。
  - U-PE 上の UNI。

コンフィグレット

U-PE

```
!
vlan 700
exit
!
interface FastEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 700
 switchport mode trunk
 switchport nonegotiate
 no keepalive
 mac access-group ISC-FastEthernet1/0/2 in
 no cdp enable
 spanning-tree bpdufilter enable
!
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 700
 switchport mode trunk
 keepalive 10
!
!
mac access-list extended
ISC-FastEthernet1/0/2
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
!
```

N-PE

```
!
interface GigabitEthernet0/3/1/1.700
l2transport
 dot1q vlan 700
!
l2vpn
 pw-class PW_AD3-AD7_Customer1
  encapsulation mpls
   transport-mode vlan
   preferred-path interface tunnel-te 1370
fallback disable
  !
 !
 xconnect group L2VPN_Customer1-Gold_class
  p2p GoldPkg_AD3-AD7_Customer1
   interface GigabitEthernet0/3/1/1.700
   neighbor 192.169.105.30 pw-id 1000
    pw-class PW_AD3-AD7_Customer1
   !
  !
```

コメント

- N-PE は IOS XR 3.7 を備えた CRS-1 です。
- 疑似回線クラス機能は、カプセル化、トランスポート モード、優先パス、フォールバック オプションなどさまざまな関連属性とともに設定します。
- フォールバックのディセーブル オプションは、IOS XR 3.6.1 で必須、IOS XR 3.7 以降で任意になっています。
- E-Line 名（**p2p** コマンド）および L2VPN グループ名（**xconnect group** コマンド）は、ユーザが設定します。

ERS（EVPL）（L2VPN の NBI 拡張、IOS デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）。
- デバイス設定：
  - N-PE は IOS を備えた 12.2(18)SXF です。
  - U-PE は IOS を備えた 12.2(25)EY4 です。
  - N-PE 上の UNI。
  - U-PE 上の UNI。

コンフィグレット

U-PE	N-PE
!	!
vlan 3200	vlan 3300
exit	exit
!	!
interface FastEthernet1/0/2	interface FastEthernet1/0/24
no cdp enable	no cdp enable
no ip address	no ip address
duplex auto	duplex auto
switchport	switchport
switchport trunk encapsulation dot1q	switchport trunk encapsulation dot1q
switchport mode trunk	switchport mode trunk
switchport trunk allowed vlan none	switchport trunk allowed vlan none
switchport trunk allowed vlan 3200	switchport trunk allowed vlan 3300
switchport nonegotiate	switchport nonegotiate
switchport port-security aging type inactivity	switchport port-security aging type inactivity
switchport port-security maximum 100	switchport port-security maximum 100
switchport port-security aging time 1000	switchport port-security aging time 1000
switchport port-security violation protect	switchport port-security violation protect
switchport port-security	switchport port-security
storm-control unicast level 1.0	**storm-control unicast level 1.0**
storm-control broadcast level 50.0	**storm-control broadcast level 50.0**
storm-control multicast level 50.0	**storm-control multicast level 50.0**
shutdown	shutdown
keepalive	keepalive
spanning-tree bpdufilter enable	spanning-tree bpdufilter enable
!	!
interface GigabitEthernet1/0/1	**interface Vlan3300**
no ip address	no ip address
switchport	xconnect 192.169.105.40 7502 encapsulation
switchport trunk encapsulation dot1q	mpls
switchport mode trunk	no shutdown
switchport trunk allowed vlan 3200	!
!	

コメント

なし。

ERS（EVPL）または EWS（EPL）（IOS XR デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）または EWS（EPL）。
- デバイス設定：
  - N-PE は IOS XR 3.4.2 を備えた CRS-1 です。
  - N-PE 上の UNI。ERS（EVPL）だけ。
  - U-PE。EWS（EPL）または ERS（EVPL）。

コンフィグレット

N-PE

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <Set>
    <Configuration Source="CurrentConfig">
      <InterfaceConfigurationTable>
        <InterfaceConfiguration>
          <Naming>
            <Name>GigabitEthernet0/0/0/1.302</Name>
            <Active>act</Active>
          </Naming>
          <InterfaceModeNonPhysical>L2Transport</InterfaceModeNonPhysical>
        </InterfaceConfiguration>
      </InterfaceConfigurationTable>
      <L2VPN>
        <Enabled>true</Enabled>
        <XConnectGroupTable>
          <XConnectGroup>
            <Naming>
              <Name>VPNSC</Name>
            </Naming>
            <Enabled>true</Enabled>
            <P2PXConnectTable>
              <P2PXConnect>
                <Naming>
                  <Name>GigabitEthernet0_0_0_1.302</Name>
                </Naming>
                <Enabled>true</Enabled>
                <AttachmentCircuitTable>
                  <AttachmentCircuit>
                    <Naming>
                      <Name>GigabitEthernet0/0/0/1.302</Name>
                    </Naming>
                    <Enabled>true</Enabled>
                  </AttachmentCircuit>
                </AttachmentCircuitTable>
                <PseudoWireTable>
                  <PseudoWire>
                    <Naming>
                      <Neighbor>
                        <IPV4Address>10.11.13.15</IPV4Address>
                      </Neighbor>
                      <PseudowireID>1005</PseudowireID>
                    </Naming>
                    <PseudoWireParameters/>
                  </PseudoWire>
                </PseudoWireTable>
              </P2PXConnect>
            </P2PXConnectTable>
          </XConnectGroup>
        </XConnectGroupTable>
      </L2VPN>
    </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。

ERS（EVPL）および EWS（EPL）（E-Line ローカル接続）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）および EWS（EPL）。
- デバイス設定：
  - N-PE は、IOS XR 3.6 以降を備えた CRS-1 です。
  - U-PE は IOS を備えた 12.2(18)SXF です。

コンフィグレット

U-PE	N-PE
	interface GigabitEthernet0/0/0/2.559 dot1q vlan 559 l2transport ! interface GigabitEthernet0/0/0/4.559 dot1q vlan 559 l2transport ! l2vpn xconnect group ISC p2p **cl-test-l2-crs1-1--0--559** interface GigabitEthernet0/0/0/2.559 interface GigabitEthernet0/0/0/4.559 ! ! !

コメント

- デフォルトの E-Line 名は、ローカル接続コンフィグレット用に変更されました。
- デフォルトの E-line 名の形式は次のとおりです。
  device_name_with_underscores--VCID--VLANID

ERS（EVPL）、EWS（EPL）、ATM、またはフレーム リレー（L2VPN の追加テンプレート変数、IOS および IOS XR デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ERS（EVPL）、EWS（EPL）、ATM およびフレーム リレー。
- デバイス設定：
  - N-PE は ERS（EVPL）、EWS（EPL）、フレーム リレー サービス用の IOS を備えた 12.2(18)SXF です。
  - N-PE は ERS（EVPL）、EWS（EPL）サービス用の IOS XR 3.6 以降、および ATM サービス（ATM ポート モード）用の IOS XR 3.7 以降を備えた CRS-1 です。
  - U-PE は、ERS（EVPL）または EWS（EPL）サービス用 IOS を備えた 12.2(25)EY4 です。

コンフィグレット

U-PE	N-PE

（なし）	テンプレートの内容：
	`interface Loopback0`
	`description`
	`LocalLoopbackAddress=$L2VPNLocalLoopback`
	`LocalHostName=$L2VPNLocalHostName`
	`RemoteLoopbackAddress=$L2VPNRemoteLoopback`
	`RemoteHostName=$L2VPNRemoteHostName`
	
	コンフィグレット：
	`interface Loopback0`
	`description LocalLoopbackAddress=`
	`192.169.105.40`
	`LocalHostName=cl-test-l2-7600-2`
	`RemoteLoopbackAddress=192.169.105.80`
	`RemoteHostName= cl-test-l2-7600-4`

コメント

- これら 4 つの変数は、N-PE だけでサポートされています。
- 他のすべてのデバイス ロール（U-PE、PE-AGG、および CE）については、値はすべて空白です。

EWS（EPL）（ポイントツーポイント）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：EWS（EPL）（ポイントツーポイント）。
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。

    インターフェイス：FA8/17。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。ポート セキュリティおよびトンネリングなし。

    インターフェイス：FA1/0/20 – FA1/0/23。
  - L2VPN ポイントツーポイント。
  - Q-in-Q UNI。

コンフィグレット

U-PE	N-PE
system mtu 1522 ! vlan 774 exit ! interface FastEthernet1/0/20 no cdp enable no keepalive switchport **switchport access vlan 774** **switchport mode dot1q-tunnel** **switchport nonegotiate** **spanning-tree portfast** **spanning-tree bpdufilter enable** ! interface FastEthernet1/0/23 no ip address switchport trunk allowed vlan 774,787-788	vlan 774 exit ! interface FastEthernet8/17 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-774,878 ! interface Vlan774 no ip address description L2VPN EWS xconnect 99.99.8.99 89029 encapsulation mpls no shutdown

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。プロビジョニングは ERS（EVPL）の例と同じです。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。
- デフォルトで PACL はプロビジョニングされていません。必要に応じて BPDU をトンネリング可能です。
- 追加 4 バイトの Q-in-Q フレームを扱うためには、システム MTU を 1522 に設定する必要があります。

EWS（EPL）（ポイントツーポイント、UNI ポート セキュリティ、BPDU トンネリング）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ポート セキュリティ、BPDU トンネリングを備えた EWS（EPL）（ポイントツーポイント）
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。ポート セキュリティなし、トンネリングあり。
  - L2VPN ポイントツーポイント。
  - Q-in-Q UNI。

コンフィグレット

U-PE	N-PE
system mtu 1522 ! vlan 775 exit ! system mtu 1522 ! vlan 775 exit ! interface FastEthernet1/0/19 no cdp enable no keepalive switchport switchport access vlan 775 switchport mode dot1q-tunnel switchport nonegotiate **switchport port-security maximum 34** **switchport port-security aging time 32** **switchport port-security violation shutdown** **switchport port-security** **l2protocol-tunnel cdp** **l2protocol-tunnel stp** **l2protocol-tunnel vtp** **l2protocol-tunnel shutdown-threshold cdp 88** **l2protocol-tunnel shutdown-threshold stp 99** **l2protocol-tunnel shutdown-threshold vtp 56** **l2protocol-tunnel drop-threshold cdp 56** **l2protocol-tunnel drop-threshold stp 64** **l2protocol-tunnel drop-threshold vtp 34** **storm-control unicast level 34.0** **storm-control broadcast level 23.0** **storm-control multicast level 12.0** spanning-tree portfast spanning-tree bpdufilter enable mac access-group ISC-FastEthernet1/0/19 in interface FastEthernet1/0/23 no ip address switchport trunk allowed vlan 774-775,787-788 ! mac access-list extended ISC-FastEthernet1/0/19 no permit any any **deny any host 3456.3456.1234** permit any any	vlan 775 exit ! interface FastEthernet8/17 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-775,878 ! interface Vlan775 no ip address description L2VPN EWS xconnect 99.99.8.99 89029 encapsulation mpls no shutdown

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。プロビジョニングは ERS（EVPL）の例と同じです。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。
- 1 ユーザ定義エントリのある PACL。
- BPDU（CDP、STP、および VTP）は MPLS コアを介してトンネリングされます。
- ストーム制御は、ユニキャスト、マルチキャスト、およびブロードキャストに対してイネーブルです。

EWS（EPL）（ハイブリッド）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：EWS（EPL）ハイブリッド。一方は EWS（EPL）UNI、もう一方は ERS（EVPL）NNI です。
- デバイス設定：
  - N-PE は、12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。

    インターフェイス：FA8/17。
  - U-PE は 12.2(25)EY1 を備えた Cisco 3750ME です。ポート セキュリティなし、トンネリングあり。

    インターフェイス：FA1/0/20 – FA1/0/23。
  - L2VPN ポイントツーポイント。
  - Q-in-Q UNI。

（注） 最初のコンフィグレット例は EWS（EPL）側（UNI）です。次のコンフィグレットは ERS（EVPL）側（NNI）です。

コンフィグレット

U-PE	N-PE
system mtu 1522 ! vlan 775 exit ! system mtu 1522 ! vlan 775 exit ! interface FastEthernet1/0/19 no cdp enable no keepalive switchport switchport access vlan 775 switchport mode dot1q-tunnel switchport nonegotiate **switchport port-security maximum 34** **switchport port-security aging time 32** **switchport port-security violation shutdown** **switchport port-security** **l2protocol-tunnel cdp** **l2protocol-tunnel stp** **l2protocol-tunnel vtp** **l2protocol-tunnel shutdown-threshold cdp 88** **l2protocol-tunnel shutdown-threshold stp 99** **l2protocol-tunnel shutdown-threshold vtp 56** **l2protocol-tunnel drop-threshold cdp 56** **l2protocol-tunnel drop-threshold stp 64** **l2protocol-tunnel drop-threshold vtp 34** **storm-control unicast level 34.0** **storm-control broadcast level 23.0** **storm-control multicast level 12.0** spanning-tree portfast spanning-tree bpdufilter enable mac access-group ISC-FastEthernet1/0/19 in interface FastEthernet1/0/23 no ip address switchport trunk allowed vlan 774-775,787-788 ! mac access-list extended ISC-FastEthernet1/0/19 no permit any any **deny any host 3456.3456.1234** permit any any	vlan 775 exit ! interface FastEthernet8/17 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-775,878 ! interface Vlan775 no ip address description L2VPN EWS xconnect 99.99.8.99 89029 encapsulation mpls no shutdown

コメント

- これは EWS（EPL）側（UNI）です。
- N-PE は、OSM または SIP-600 モジュール搭載の 7600 です。プロビジョニングは ERS（EVPL）と同じです。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。
- 1 ユーザ定義エントリのある PACL。
- BPDU（cdp、stp、および vtp）は MPLS コアを介してトンネリングされます。

- ストーム制御は、ユニキャスト、マルチキャスト、およびブロードキャストに対してイネーブルです。

コンフィグレット

U-PE	N-PE
system mtu 1522 vlan 775 exit interface FastEthernet1/17 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-775,878 interface FastEthernet1/10 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-775,878	vlan 775 exit ! interface FastEthernet8/17 switchport trunk allowed vlan 1,451,653,659,766-768,772,773-775,878 ! interface Vlan775 no ip address description L2VPN EWS xconnect 99.99.8.99 89029 encapsulation mpls no shutdown

コメント

- これは ERS（EVPL）側（NNI）です。
- N-PE は、OSM または SIP-600 モジュール搭載の 7600 です。プロビジョニングは ERS（EVPL）と同じです。
- U-PE は実際には PE-AGG です。NNI としてホールセール顧客に接続されます。両方のポートは通常の NNI ポートです。

EWS（EPL）（疑似回線クラス、E-Line、L2VPN グループ名、IOS XR デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：EWS（EPL）。
- デバイス設定：
  - N-PE は IOS XR 3.6.1 以降を備えた CRS-1 です。
  - U-PE 上の UNI。

コンフィグレット

U-PE	N-PE
!	!
system mtu 1522	interface GigabitEthernet0/3/1/1.700
!	l2transport
vlan 700	dot1q vlan 700
exit	**!**
!	**!**
interface FastEthernet1/0/2	**l2vpn**
switchport	**pw-class PW_AD7-AD3_Cutsomer2**
switchport access vlan 700	**encapsulation mpls**
switchport mode dot1q-tunnel	**transport-mode ethernet**
switchport nonegotiate	**preferred-path interface tunnel-te 2730**
no keepalive	**!**
no cdp enable	**!**
spanning-tree portfast	**xconnect group ISC**
spanning-tree bpdufilter enable	**p2p cl-test-l2-12404-2--1000**
!	interface GigabitEthernet0/3/1/1.700
interface GigabitEthernet1/0/1	neighbor 192.169.105.30 pw-id 1000
no ip address	**pw-class PW_AD7-AD3_Cutsomer2**
switchport	**!**
switchport trunk encapsulation dot1q	
switchport trunk allowed vlan 700	
switchport mode trunk	
!	

コメント

- N-PE は IOS XR 3.7 を備えた CRS-1 ルータです。
- 疑似回線クラス機能は、カプセル化、トランスポート モード、優先パス、フォールバック オプションなどさまざまな関連属性とともに設定されます。
- フォールバックのディセーブル オプションは、IOS XR 3.6.1 で必須、IOS XR 3.7 以降で任意になっています。
- ユーザ入力がない場合、E-Line 名（**p2p** コマンド）および L2VPN グループ名（**xconnect group** コマンド）は Prime Provisioning 生成デフォルト値です。

EWS（EPL）（L2VPN の NBI 拡張、IOS デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：EWS（EPL）。
- デバイス設定：
  - N-PE は IOS を備えた 12.2(18)SXF です。
  - U-PE は IOS を備えた 12.2(25)EY4 です。
  - N-PE 上の UNI。
  - U-PE 上の UNI。

コンフィグレット

U-PE	N-PE
!	!
vlan 3201	vlan 3301
exit	exit
!	!
interface FastEthernet1/0/2	interface FastEthernet1/0/24
no cdp enable	no cdp enable
no ip address	no ip address
duplex auto	duplex auto
switchport	switchport
switchport access vlan 3201	switchport access vlan 3301
switchport mode dot1q-tunnel	switchport mode dot1q-tunnel
switchport nonegotiate	switchport nonegotiate
switchport port-security aging type inactivity	switchport port-security aging type inactivity
switchport port-security maximum 100	switchport port-security maximum 100
switchport port-security aging time 1000	switchport port-security aging time 1000
switchport port-security violation protect	switchport port-security violation protect
switchport port-security	switchport port-security
storm-control unicast level 1.0	**storm-control unicast level 1.0**
storm-control broadcast level 50.0	**storm-control broadcast level 50.0**
storm-control multicast level 50.0	**storm-control multicast level 50.0**
shutdown	shutdown
keepalive	**keepalive**
spanning-tree bpdufilter enable	spanning-tree bpdufilter enable
!	!
interface GigabitEthernet1/0/1	**interface Vlan3301**
no ip address	no ip address
switchport	xconnect 192.169.105.40 7502 encapsulation mpls
switchport trunk encapsulation dot1q	no shutdown
switchport mode trunk	!
switchport trunk allowed vlan 3201	
!	

コメント

なし。

ATM over MPLS（VC モード）

設定

- サービス：L2VPN
- 機能：VC モードの ATM over MPLS（ATMoMPLS、AToM の一種）
- デバイス設定：
  - N-PE は、IOS 12.0(28)S を備えた Cisco 7200 です。
  - CE なし。
  - U-PE なし。
  - L2VPN ポイントツーポイント（ATMoMPLS）。
  - C7200（ATM2/0）。

コンフィグレット

U-PE	N-PE

（なし）	`interface ATM2/0.34234 point-to-point`
	`pvc 213/423 l2transport`
	`encapsulation aal5`
	`xconnect 99.99.4.99 89025 encapsulation mpls`

コメント

- N-PE は任意の MPLS 対応ルータです。
- L2VPN プロビジョニングは ATM VC 接続で実行されます。

ATM over MPLS（VP モード）

設定

- サービス：L2VPN
- 機能：VP モードの ATM over MPLS（ATMoMPLS、AToM の一種）
- デバイス設定：
  - N-PE は、IOS 12.0(28)S を備えた Cisco 7200 です。
    インターフェイス：ATM2/0。
  - CE なし。
  - U-PE なし。
  - L2VPN ポイントツーポイント（ATMoMPLS）。

コンフィグレット

U-PE	N-PE

（なし）	`pseudowire-class ISC-pw-tunnel-123`
	`encapsulation mpls`
	`preferred-path interface tunnel123`
	`disable-fallback`
	`!`
	`interface ATM2/0`
	`atm pvp 131 l2transport`
	`xconnect 99.99.4.99 89024 pw-class`
	`ISC-pw-tunnel-123`

コメント

- N-PE は任意の MPLS 対応ルータです。
- L2VPN プロビジョニングは ATM VP 接続で実行されます。
- L2VPN 疑似回線は TE トンネルにマッピングされます。

ATM（ポート モード、疑似回線クラス、E-Line、L2VPN グループ名、IOS XR デバイス）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：ATM。
- デバイス設定：
  - N-PE は、ATM サービス用の IOS XR 3.7 以降を備えた CRS-1 です（ポート モードだけ）。
  - N-PE 上の UNI。

コンフィグレット

U-PE	N-PE

（なし）	interface ATM0/1/0/0
	 description UNIDesc_AC1
	 l2transport
	 !
	!
	l2vpn
	 pw-class PWClass-1
	  encapsulation mpls
	  preferred-path interface tunnel-te 500
	fallback disable
	  !
	 !
	 xconnect group ISC
	  p2p ELine_AC1
	  interface ATM0/1/0/0
	  neighbor 192.169.105.70 pw-id 100
	  pw-class PWClass-1
	  !

コメント

- N-PE は CRS-1 ルータです。
- 疑似回線クラス機能は任意で、設定されていません。
- E-Line 名（**p2p** コマンド）および L2VPN グループ名（**xconnect group** コマンド）は、ユーザによって設定されます。
- PORT モードだけが IOS XR でサポートされています。
- この PORT モードは、IOS XR デバイス上で **pvp** や **pvc** などの特定のコマンドを生成しません。
- ATM インターフェイスは **xconnect** に含まれます。

Frame Relay over MPLS

設定

- サービス：L2VPN
- 機能：MPLS を介したフレーム リレー（FRoMPLS、AToM の一種）。
- デバイス設定：
  - N-PE は、IOS 12.0(28)S を備えた Cisco 7200 です。
    インターフェイス：ATM2/0。
  - CE なし。
  - U-PE なし。
  - L2VPN ポイントツーポイント（ATMoMPLS）。

コンフィグレット

U-PE	N-PE

（なし）	`interface Serial1/1`
	`exit`
	`!`
	`connect C1_89001 Serial1/1 135 l2transport`
	`xconnect 99.99.4.99 89001 encapsulation mpls`

コメント

- N-PE は任意の MPLS 対応ルータです。
- L2VPN プロビジョニングは、フレーム リレー接続のシリアル ポート上で実行されます。

フレーム リレー（DLCI モード）

設定

- サービス：L2TPv3 コアを介した L2VPN。
- 機能：DLCI モードの FR。
- デバイス設定：
  - N-PE は、IOS 12.0(28)S を備えた Cisco 7200 です。
    インターフェイス：ATM2/0。
  - CE なし。
  - U-PE なし。
  - L2VPN ポイントツーポイント（ATMoMPLS）。

コンフィグレット

U-PE	N-PE

（なし）	`pseudowire-class ISC-pw-dynamic-default`
	`encapsulation l2tpv3`
	`ip local interface Loopback10`
	`ip dfbit set`
	`!`
	`interface Serial3/2`
	`encapsulation frame-relay`
	`exit`
	`!`
	`connect ISC_1054 Serial3/2 86 l2transport`
	`xconnect 10.9.1.1 1054 encapsulation l2tpv3`
	`pw-class ISC-pw-dynamic-default`

コメント

- N-PE は任意の L2TPv3 対応ルータです。
- L2VPN プロビジョニングは、フレーム リレー接続のシリアル ポート上で実行されます。

VPLS（マルチポイント、ERMS/EVP-LAN）

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：VPLS（マルチポイント）ERMS（EVP-LAN）。
- デバイス設定：
  - N-PE は、IOS 12.2(18)SXF、Sup720-3BX.L を備えた Cisco 7600 です。

    インターフェイス：FA2/18。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。ポート セキュリティおよびトンネリングなし。

    インターフェイス：FA1/0/21 – FA1/0/23。
  - VLAN 767 を備えた VPLS マルチポイント VPN。

コンフィグレット

U-PE

```
vlan 767
exit
!
interface FastEthernet1/0/21
no cdp enable
no keepalive
no ip address
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan none
switchport trunk allowed vlan 767
switchport nonegotiate
spanning-tree bpdufilter enable
mac access-group ISC-FastEthernet1/0/21 in
!
interface FastEthernet1/0/23
no ip address

mac access-list extended
ISC-FastEthernet1/0/21
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
```

N-PE

```
l2 vfi vpls_ers_1-0 manual
vpn id 89017
neighbor 99.99.10.9 encapsulation mpls
neighbor 99.99.5.99 encapsulation mpls
!
vlan 767
exit
!
interface FastEthernet2/18
switchport trunk allowed vlan
350,351,430,630,767,780,783,785-791
!
interface Vlan767
no ip address
description VPLS ERS
xconnect vfi vpls_ers_1-0
no shutdown
```

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。
- VFI には、この N-PE が対話するすべての N-PE（ネイバー）が含まれています。
- U-PE は、汎用 Metro Ethernet（ME; メトロ イーサネット）スイッチです。カスタマー BPDU は PACL によってブロックされます。VPLS ERMS（EVP-LAN）UNI は L2VPN（ポイントツーポイント）ERS（EVPL）UNI と同じです。
- SVI（インターフェイス 767）はグローバル VFI を参照します。これには複数のピアリング N-PE が含まれます。

VPLS（マルチポイント、EMS/EP-LAN）、BPDU トンネリング

設定

- サービス：L2VPN/メトロ イーサネット。
- 機能：BPDU トンネリングのある VPLS（マルチポイント）EMS（EP-LAN）。
- デバイス設定：
  - N-PE は IOS 12.2(18)SXF、Sup720-3BXL を備えた Cisco 7600 です。

    インターフェイス：FA2/18。
  - U-PE は、IOS 12.2(25)EY1 を備えた Cisco 3750ME です。ポート セキュリティおよびトンネリングなし。

    インターフェイス：FA1/0/12 – FA1/0/23。
  - VPLS マルチポイント VPN（VLAN 767）
  - Q-in-Q UNI。

コンフィグレット

U-PE	N-PE
system mtu 1522 ! errdisable recovery interval 33 ! vlan 776 exit ! interface FastEthernet1/0/12 no cdp enable no keepalive switchport **switchport access vlan 776** **switchport mode dot1q-tunnel** **switchport nonegotiate** **l2protocol-tunnel cdp** **l2protocol-tunnel stp** **l2protocol-tunnel vtp** **l2protocol-tunnel shutdown-threshold cdp 88** **l2protocol-tunnel shutdown-threshold stp 64** **l2protocol-tunnel shutdown-threshold vtp 77** **l2protocol-tunnel drop-threshold cdp 34** **l2protocol-tunnel drop-threshold stp 23** **l2protocol-tunnel drop-threshold vtp 45** no shutdown spanning-tree portfast spanning-tree bpdufilter enable	**l2 vfi vpls_ews-89019 manual** **vpn id 89019** **neighbor 99.99.8.99 encapsulation mpls** **!** **vlan 776** **exit** **!** **interface FastEthernet8/17** **switchport trunk allowed vlan** **1,451,653,659,766-768,772-776,878** **!** **interface Vlan776** **no ip address** **description VPLS EWS** **xconnect vfi vpls_ews-89019** **no shutdown**

コメント

- N-PE は OSM または SIP-600 モジュール搭載の 7600 です。
- VFI には、この N-PE が対話するすべての N-PE（ネイバー）が含まれています。
- VPLS EMS（EP-LAN）UNI は L2VPN（ポイントツーポイント）EWS（EPL）UNI と同様です。
- SVI は VPLS ERS（EVP-LAN）SVI と同じです。

EVC（疑似回線コア接続、UNI ポート セキュリティ）

設定

- サービス：EVC/Metro イーサネット。
- 機能：疑似回線コア接続および UNI ポートセキュリティを備えている EVC。
- デバイス設定：
  - N-PE は IOS 12.2(33)SRB3 を備えた Cisco 7600 です。

    インターフェイス：GI2/0/0。
  - U-PE は IOS 12.2(25)EY2 を備えた Cisco 3750ME です。ポート セキュリティはイネーブルです。

    インターフェイス：FA1/14 ～ FA3/23。

コンフィグレット

U-PE	N-PE
vlan 788 exit ! interface FastEthernet3/23 no ip address switchport trunk allowed vlan 783,787-788 ! interface FastEthernet1/14 no cdp enable no keepalive no ip address switchport **switchport trunk encapsulation dot1q** **switchport mode trunk** switchport trunk allowed vlan none **switchport trunk allowed vlan 788** **switchport port-security** switchport nonegotiate switchport port-security maximum 45 switchport port-security aging time 34 switchport port-security violation shutdown switchport port-security mac-address 3456.3456.5678 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet3/31** **deny any host 0100.0ccc.cccc** **deny any host 0100.0ccc.cccd** **deny any host 0100.0ccd.cdd0** **deny any host 0180.c200.0000** **deny any host 1234.3234.3432** **permit any any**	**interface GigabitEtherne4/0/1** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500** **rewrite ingress tag push dot1q 555** **symmetric** **xconnect 192.169.105.20 505 encapsulation** **mpls**

コメント

- U-PE 上の UNI。
- 単一の一致タグが実行されます。
- 書き換え動作 **push** は、555 の外部 VLAN タグをプッシュします。

EVC（疑似回線コア接続、UNI、ポート セキュリティなし、ブリッジ ドメインあり）

設定

- サービス：EVC/Metro イーサネット。
- 機能：疑似回線コア接続、UNI、ブリッジ ドメインを備え、ポート セキュリティを備えていない EVC。
- デバイス設定：
  - N-PE は IOS 12.2(33)SRB3 を備えた Cisco 7600 です。

    インターフェイス：GI2/0/0。
  - U-PE は IOS 12.2(25)EY2 を備えた Cisco 3750ME です。ポート セキュリティはイネーブルです。

    インターフェイス：FA1/14 ～ FA3/23。

コンフィグレット

U-PE	N-PE
vlan 772 exit ! interface FastEthernet3/23 **switchport trunk allowed vlan 500,772** ! interface FastEthernet1/14 no cdp enable no keepalive no ip address switchport trunk allowed vlan 500,772 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet1/14** **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**	**vlan 100** **interface GigabitEtherne2/0/0** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500** **rewrite ingress tag push dot1q 23** **second-dot1q 41 symmetric** **bridge-domain 100 split-horizon** **Interface Vlan100** **no shut** **xconnect 192.169.105.20 101 encapsulation** **mpls**

コメント

- U-PE 上の UNI。
- 単一の一致タグが実行されます。
- 書き換え動作 **push** は 2 つのタグをプッシュします。

EVC（疑似回線コア接続、UNI、および疑似回線トンネリング）

設定

- サービス：EVC/Metro イーサネット。
- 機能：疑似回線、UNI、および疑似回線トンネリングを備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GI4/0/0 <–> GI2/0/0。

コンフィグレット

U-PE	N-PE

（なし）	`pseudowire-class ISC-pw-tunnel-2147`
	`encapsulation mpls`
	`preferred-path interface Tunnel2147`
	`disable-fallback`
	
	`interface GigabitEtherne4/0/0`
	`service instance 1 ethernet`
	`encapsulation dot1q 11 second-dot1q 41`
	`rewrite ingress tag pop 2 symmetric`
	`xconnect pw-class ISC-pw-tunnel-2147`

コメント

- N-PE 上の UNI（CE は直接接続されています）。
- 両方のタグの一致が実行されます。
- 書き換え動作は、内部および外部 VLAN タグの両方をポップします。

EVC（VPLS コア接続、UNI ポート セキュリティ）

設定

- サービス：EVC/Metro イーサネット。
- 機能：VPLS コア接続および UNI ポートセキュリティを備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：GI4/0/1。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。ポート セキュリティはイネーブルです。

    インターフェイス：FA1/14 ～ FA3/23。

コンフィグレット

U-PE	N-PE
vlan 788 exit ! interface FastEthernet3/23 no ip address switchport trunk allowed vlan 783,787-788 ! interface FastEthernet1/14 no cdp enable no keepalive no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan none **switchport trunk allowed vlan 788** switchport port-security switchport nonegotiate switchport port-security maximum 58 switchport port-security aging time 85 switchport port-security violation shutdown switchport port-security mac-address 1252.1254.2544 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet3/31** **deny any host 0100.0ccc.cccc** **deny any host 0100.0ccc.cccd** **deny any host 0100.0ccd.cdd0** **deny any host 0180.c200.0000** **deny any host 1234.3234.3432** permit any any	**l2 vfi attest-226 manual** **vpn id 226** **neighbor 192.169.105.20 encapsulation mpls** **vlan 200** **bridge-domain 200 split-horizon** **interface GigabitEtherne4/0/1** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500** **rewrite ingress tag translate 1-to-1 dot1q** **222 symmetric** **Interface vlan 200** **xconnect vfi attest-226**

コメント

- U-PE 上の UNI。
- 書き換え動作は、着信 VLAN タグ 500 を 222 に変換します。

EVC（VPLS コア接続、UNI ポート セキュリティなし）

設定

- サービス：EVC/Metro イーサネット。
- 機能：VPLS コア接続を備え、UNI ポート セキュリティを備えていない EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GI4/0/1。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FA1/14 ～ FA3/23。

コンフィグレット

U-PE	N-PE
vlan 772 exit ! interface FastEthernet3/23 switchport trunk allowed vlan 500,772 ! interface FastEthernet1/14 no cdp enable no keepalive no ip address switchport trunk allowed vlan 500,772 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet1/14** **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	**l2 vfi attest1-458 manual** **vpn id 452** **neighbor 192.169.105.20 encapsulation mpls** **vlan 200** **bridge-domain 200 split-horizon** **interface GigabitEtherne4/0/1** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500** **rewrite ingress tag translate 1-to-2 dot1q** **222 second-dot1q 41 symmetric** **Interface vlan 200** **xconnect vfi attest1-458**

コメント

- U-PE 上の UNI。
- 書き換え操作は、着信 VLAN タグ 500 を 2 つのタグ（222 および 41）に変換します。

EVC（ローカル コア接続、UNI ポート セキュリティ）

設定

- サービス：EVC/Metro イーサネット。
- 機能：ローカル接続コア接続および UNI ポート セキュリティを備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：GI2/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。ポート セキュリティはイネーブルです。

    インターフェイス：FA1/14 ～ FA3/23。

コンフィグレット

U-PE	N-PE
vlan 788 exit ! interface FastEthernet3/23 no ip address switchport trunk allowed vlan 783,787-788 ! interface FastEthernet1/14 no cdp enable no keepalive no ip address **switchport** **switchport trunk encapsulation dot1q** **switchport mode trunk** switchport trunk allowed vlan none switchport trunk allowed vlan 788 switchport port-security switchport nonegotiate switchport port-security maximum 45 switchport port-security aging time 34 switchport port-security violation shutdown switchport port-security mac-address 4111.4545.1211 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet3/31** **deny any host 0100.0ccc.cccc** **deny any host 0100.0ccc.cccd** **deny any host 0100.0ccd.cdd0** **deny any host 0180.c200.0000** **deny any host 1234.3234.3432** **permit any any**	**Connect Customer_1 GigabitEthernet4/0/1 10** **GigabitEthernet4/0/10 25** **interface GigabitEtherne4/0/1** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500** **rewrite ingress tag push dot1q 555** **symmetric** **interface GigabitEtherne4/0/10** **no shut** **service instance 25 ethernet** **encapsulation dot1q 500 second-dot1q 501** **rewrite ingress tag translate 2-to-1 dot1q** **222 symmetric**

コメント

- U-PE 上の UNI。
- 2 つのタグ一致動作が実行されます。
- 書き換え動作は、2 つのタグを 1 つのタグに変換します。
- 2 つのサービス インスタンスが **connect** コマンドを通じて接続されます。

EVC（ローカル コア接続、UNI、ポート セキュリティなし、ブリッジ ドメイン）

設定

- EVC/Metro イーサネット。
- 機能：ローカル接続コア接続、UNI、およびブリッジ ドメインを備え、ポート セキュリティを備えていない EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GI2/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FA1/14– FA3/23。

コンフィグレット

U-PE	N-PE
vlan 772 exit ! interface FastEthernet3/23 switchport trunk allowed vlan 500,772 ! interface FastEthernet1/14 no cdp enable no keepalive no ip address switchport trunk allowed vlan 500,772 spanning-tree bpdufilter enable mac access-group ISC-FastEthernet3/23 in ! **mac access-list extended** **ISC-FastEthernet1/14** **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	**interface GigabitEtherne2/0/0** **no shut** **service instance 10 ethernet** **encapsulation dot1q 500 second-dot1q 501** **rewrite ingress tag translate 2-to-2 dot1q 222 second-dot1q 41 symmetric** **bridge-domain 200 split-horizon** **interface GigabitEtherne2/0/10** **no shut** **service instance 15 ethernet** **encapsulation dot1q 24** **rewrite ingress tag pop 1 symmetric** **bridge-domain 200 split-horizon**

コメント

- U-PE 上の UNI。
- 書き換え動作は、2 つの着信タグを 2 つの異なるタグにマッピングまたは変換します。
- ここで、サービス インスタンスはブリッジ ドメイン経由で接続されています。

EVC（疑似回線コア接続、ブリッジ ドメイン、SVI 上の疑似回線）

設定

- EVC/Metro イーサネット。
- 機能 : 疑似回線コア接続とブリッジ ドメインを備え、N-PE で SVI 上の疑似回線がイネーブルにされている EVC。
- デバイス設定 :
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス : GigabitEthernet7/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。

    インターフェイス : FastEthernet1/0/10。

コンフィグレット

U-PE	N-PE
vlan 452 exit ! interface FastEthernet1/0/10 no ip address switchport trunk allowed vlan add 452 ! interface FastEthernet1/0/13 no spanning-tree bpdufilter enable switchport no keepalive no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 452 switchport nonegotiate	vlan 3524 exit ! ethernet evc Customer1_253 ! interface GigabitEthernet7/0/0 **service instance 3 ethernet Customer1_253** encapsulation dot1q 452 rewrite ingress tag pop 1 symmetric **bridge-domain 3524 split-horizon** ! **interface Vlan3524** no ip address description BD=T,SVI=T,Flex **xconnect 22.22.22.22 52500 encapsulation mpls** **backup peer 22.22.22.22 52501** no shutdown

コメント

- なし。

EVC（疑似回線コア接続、ブリッジ ドメインなし、SVI 上の疑似回線なし）

設定

- EVC/Metro イーサネット。
- 機能：疑似回線コア接続を備え、ブリッジ ドメインがディセーブルになっており、N-PE で SVI 上の疑似回線がディセーブルになっている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：GigabitEthernet7/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。

    インターフェイス：FastEthernet1/0/10。

コンフィグレット

U-PE	N-PE
vlan 545 exit ! interface FastEthernet1/0/10 no ip address switchport trunk allowed vlan add 545 ! interface FastEthernet1/0/12 no spanning-tree bpdufilter enable switchport no keepalive no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 545 switchport nonegotiate mac access-group ISC-FastEthernet1/0/12 in	ethernet evc Customer1_248 ! interface GigabitEthernet7/0/0 **service instance 2 ethernet Customer1_248** encapsulation dot1q 545 rewrite ingress tag pop 1 symmetric **xconnect 22.22.22.22 52498 encapsulation mpls** **backup peer 22.22.22.22 52499**

コメント

- なし。

EVC（AutoPick Service Instance Name）

設定

- EVC/Metro イーサネット。
- 機能：[AutoPick Service Instance Name] がイネーブルで、[Service Instance Name] 入力フィールドが空欄のままの EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GigabitEthernet7/0/2。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FastEthernet1/0/14。

コンフィグレット

U-PE	N-PE
!	!
vlan 452	vlan 3524
exit	exit
!	!
interface FastEthernet1/0/10	ethernet evc C1_1
no ip address	!
switchport trunk allowed vlan add 452	interface GigabitEthernet7/0/0
!	service instance 3 ethernet C1_1
interface FastEthernet1/0/13	encapsulation dot1q 452
no spanning-tree bpdufilter enable	rewrite ingress tag pop 1 symmetric
switchport	bridge-domain 3524 split-horizon
no keepalive	!
no ip address	interface Vlan3524
switchport	no ip address
switchport trunk encapsulation dot1q	description BD=T,SVI=T,Flex
switchport mode trunk	xconnect 22.22.22.22 52500 encapsulation
switchport trunk allowed vlan 452	mpls
switchport nonegotiate	backup peer 22.22.22.22 52501
mac access-group ISC-FastEthernet1/0/13 in	no shutdown

コメント

- トランスポートのタイプは疑似回線です。
- 自動選択の [Service Instance Name] は、*CustomerName_JobID* の値を取ります。

EVC（AutoPick サービス インスタンス名なし、サービス インスタンス名なし）

設定

- EVC/Metro イーサネット。
- 機能：[AutoPick Service Instance Name] がイネーブルではなく、[Service Instance Name] 入力フィールドが空欄のままの EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GigabitEthernet7/0/2。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FastEthernet1/0/14。

コンフィグレット

U-PE	N-PE
!	!
vlan 566	interface GigabitEthernet7/0/2
exit	**service instance 43 ethernet**
!	encapsulation dot1q 566
interface FastEthernet1/0/14	xconnect 1.1.1.1 453366 encapsulation mpls
no spanning-tree bpdufilter enable	
switchport	
no keepalive	
no ip address	
switchport trunk encapsulation dot1q	
switchport mode trunk	
switchport trunk allowed vlan 566	
switchport nonegotiate	
no shutdown	
mac access-group ISC-FastEthernet1/0/14 in	
!	
interface FastEthernet1/0/18	
no ip address	
switchport trunk allowed vlan 566	
!	
mac access-list extended	
ISC-FastEthernet1/0/14	
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	

コメント

- この例で、ユーザは [AutoPick Service Instance Name] をイネーブルにせず、また [Service Instance Name] 入力フィールドを空欄のままにしています。
- グローバル コマンド **ethernet evc** は生成されませんが、コマンド **service instance 43 ethernet** は生成されます。
- サービス インスタンス名はなく、サービス インスタンス ID は 43 です。

EVC（ユーザ指定のサービス インスタンス名、疑似回線コア接続）

設定

- EVC/Metro イーサネット。
- 機能：疑似回線コア接続およびユーザ指定のサービス インスタンス名を備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GigabitEthernet7/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FastEthernet1/0/10。

コンフィグレット

U-PE	N-PE
!	!
vlan 452	vlan 3524
exit	exit
!	!
interface FastEthernet1/0/10	**ethernet evc ServiceInst**
no ip address	!
switchport trunk allowed vlan add 452	interface GigabitEthernet7/0/0
!	**service instance 3 ethernet ServiceInst**
interface FastEthernet1/0/13	encapsulation dot1q 452
no spanning-tree bpdufilter enable	rewrite ingress tag pop 1 symmetric
switchport	bridge-domain 3524 split-horizon
no keepalive	!
no ip address	interface Vlan3524
switchport	no ip address
switchport trunk encapsulation dot1q	description BD=T,SVI=T,Flex
switchport mode trunk	xconnect 22.22.22.22 52500 encapsulation
switchport trunk allowed vlan 452	mpls
switchport nonegotiate	backup peer 22.22.22.22 52501
mac access-group ISC-FastEthernet1/0/13 in	no shutdown

コメント

- トランスポートのタイプは PSEUDOWIRE です。
- ユーザは、**ServiceInst** をサービス インスタンス名として手動で指定しました。これは、サービス インスタンス ID が 3 のデバイスにプッシュされます。

EVC（ユーザ指定のサービス インスタンス名、ローカル コア接続）

設定

- EVC/Metro イーサネット。
- 機能：ローカル コア接続およびユーザ指定のサービス インスタンス名を備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GigabitEthernet1/0/6、GigabitEthernet1/0/7。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FastEthernet1/0/12、FastEthernet1/0/14。

コンフィグレット

U-PE	N-PE
vlan 45 exit ! interface FastEthernet1/0/12 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 45 ! interface FastEthernet1/0/14 no spanning-tree bpdufilter enable switchport no keepalive no ip address switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 45 switchport nonegotiate no shutdown mac access-group ISC-FastEthernet1/0/14 in ! mac access-list extended ISC-FastEthernet1/0/14 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	**ethernet evc service_int** ! interface GigabitEthernet1/0/6 no shutdown **service instance 5 ethernet service_int** encapsulation dot1q 56 ! interface GigabitEthernet1/0/7 no shutdown **service instance 33 ethernet service_int** encapsulation dot1q 45 ! connect Customer2_195 GigabitEthernet1/0/7 33 GigabitEthernet1/0/6 5

コメント

- トランスポートのタイプは LOCAL です。
- ユーザは **service_int** をサービス インスタンス名として手動で指定しました。これは、サービス インスタンス ID が 5 および 33 のそれぞれのデバイスにプッシュされます。

EVC（ユーザ指定のサービス インスタンス名、VPLS コア接続）

設定

- EVC/Metro イーサネット。
- 機能：VPLS コア接続およびユーザ指定のサービス インスタンス名を備えている EVC。
- デバイス設定：
  - N-PE は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。
    インターフェイス：GigabitEthernet7/0/0。
  - U-PE は、IOS 12.2(25) EY2 を備えた Cisco 3750ME です。
    インターフェイス：FastEthernet1/0/10。

コンフィグレット

U-PE	N-PE
!	l2 vfi vpls-test manual
vlan 452	vpn id 300
exit	neighbor 22.22.22.22 encapsulation mpls
!	!
interface FastEthernet1/0/10	vlan 500
no ip address	!
switchport trunk allowed vlan add 452	ethernet evc ServiceInst
!	!
interface FastEthernet1/0/13	interface GigabitEtherne7/0/0
no spanning-tree bpdufilter enable	service instance 10 ethernet ServiceInst
switchport	encapsulation dot1q 400
no keepalive	rewrite ingress tag pop 1 symmetric
no ip address	bridge-domain 500 split-horizon
switchport	!
switchport trunk encapsulation dot1q	interface vlan500
switchport mode trunk	xconnect vfi vpls-test
switchport trunk allowed vlan 452	
switchport nonegotiate	
mac access-group ISC-FastEthernet1/0/13 in	

コメント

- トランスポートのタイプは VPLS です。
- ユーザは、**ServiceInst** をサービス インスタンス名として手動で指定しました。これは、サービス インスタンス ID が 10 のデバイスにプッシュされます。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、ポイントツーポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：複数のリンクがあるエンドツーエンド回線を備えている疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンクが N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.370。
  - N-PE 2 は、IOS 12.2(33) SRE を備えた Cisco 7600 です。

    インターフェイス：GigabitEthernet4/0/2。

コンフィグレット

N-PE 1（ATM）	N-PE 2（イーサネット）
!	!
interface ATM1/0/0.370 point-to-point	ethernet evc 1-3_51
no atm enable-ilmi-trap	!
pvc 0/370 l2transport	interface GigabitEthernet4/0/2
encapsulation aal5snap	no ip address
xconnect 192.169.105.10 123 pw-class inter-ether	no mls qos trust
!	service instance 103 ethernet 1-3_51
	encapsulation dot1q 370
	rewrite ingress tag pop 1 symmetric
	xconnect 192.169.105.20 123 encapsulation mpls
	!

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、マルチポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：マルチポイント回線を備えている疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。リンク #1 が N-PE 1 の ATM インターフェイス上で終端し、リンク #2 が N-PE 1 のイーサネット インターフェイス上で終端し、リンク #3 が N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：GigabitEthernet7/0/4、ATM6/0/0.100。
  - N-PE 2 は IOS 12.2(33) SRE を備えた Cisco 7600 です。

    インターフェイス：GigabitEthernet7/0/5。

コンフィグレット

N-PE 1（ATM + イーサネット）	N-PE 2（イーサネット）
!	!
vlan 500	vlan 800
exit	exit
!	!
ethernet evc Customer1_166	ethernet evc Customer1_166
!	!
interface GigabitEthernet7/0/4	interface GigabitEthernet7/0/5
no shutdown	no shutdown
service instance 1 ethernet Customer1_166	service instance 1 ethernet Customer1_166
encapsulation dot1q 600	encapsulation dot1q 623
bridge-domain 500 split-horizon	bridge-domain 800 split-horizon
!	!
interface ATM6/0/0.100 point-to-point	interface Vlan800
pvc 200/300	description UT-9
encapsulation aal5snap	xconnect 192.169.105.20 6 pw-class
bridge-domain 500 split-horizon	ISC-pw-tunnel-900
!	
interface Vlan500	
no ip address	
description UT-9	
xconnect 1.1.1.1 6 pw-class	
ISC-pw-tunnel-400	
no shutdown	

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、ローカル コア接続、ポイントツーポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：ポイントツーポイント回線を備えているローカル コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。この回線は、同じローカル N-PE の異なる ATM インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/1、ATM4/1/0、ATM1/0/1.99、ATM4/1/0.98。

コンフィグレット

N-PE 1（ATM）	N/A
! interface ATM1/0/1 no shutdown ! interface ATM4/1/0 no shutdown ! interface ATM1/0/1.99 point-to-point pvc 99/99 l2transport encapsulation aal0 ! interface ATM4/1/0.98 point-to-point pvc 98/98 l2transport encapsulation aal0 ! connect ATM-to-ATM ATM1/0/1 99/99 ATM4/1/0 98/98 !	

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、ローカル コア接続、マルチポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：同じローカル N-PE 上で終端する複数のリンクのローカル コア接続で ATM とイーサネットがインターワーキングを実行する EVC。リンク #1 は ATM インターフェイスで終端し、リンク #2 はイーサネット インターフェイスで終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.99、TenGigabitEthernet6/0/0、TenGigabitEthernet6/0/1。

コンフィグレット

N-PE 1（ATM + イーサネット）	N/A

```
!
vlan 1001
exit
!
interface ATM1/0/0.99 point-to-point
 no atm enable-ilmi-trap
 pvc 99/99
  encapsulation aal5snap
 bridge-domain 1001
 !
!
interface TenGigabitEthernet6/0/0
 no ip address
 no mls qos trust
 service instance 104 ethernet 1-4_60
  encapsulation dot1q 11
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1001
 !
!
interface TenGigabitEthernet6/0/1
 no ip address
 no mls qos trust
 service instance 105 ethernet 1-4_60
  encapsulation dot1q 12
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1001
 !
```

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、ローカル コア接続、マルチポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：ローカル コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。複数のリンクが同じローカル N-PE で終端します。リンク #1 は ATM インターフェイス上で終端し、リンク #2 は ATM インターフェイス上で終端し、リンク #3 は ATM インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM6/0/0.100、ATM6/0/1.101、ATM6/0/2.102。

コンフィグレット

N-PE 1（ATM）	N/A

```
!
vlan 500
exit
!
interface ATM6/0/0.100 point-to-point
pvc 200/300
encapsulation aal5snap
bridge-domain 500
!
interface ATM6/0/1.101 point-to-point
pvc 201/301
encapsulation aal5snap
bridge-domain 500
!
interface ATM6/0/2.102 point-to-point
pvc 202/302
encapsulation aal5snap
bridge-domain 500
!
```

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、ローカル コア接続、ポイントツーポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：ローカル コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。ポイントツーポイント回線は、同じローカル N-PE の異なる ATM インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0、ATM1/0/1。

コンフィグレット

N-PE 1（ATM）	N/A
! interface ATM1/0/0 atm pvp 33 l2transport ! interface ATM1/0/1 atm pvp 222 l2transport ! connect Customer1_208 ATM1/0/0 33 ATM1/0/1 222	

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、エンドツーエンド回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：複数のリンクがあるエンドツーエンド回線の疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンクが N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.370。
  - N-PE 2 は、IOS XR 3.9.0 を備えた Cisco ASR 9000 です。

    インターフェイス：GigabitEthernet0/0/0/4.458。

コンフィグレット

N-PE 1（ATM）	N-PE 2（イーサネット）
!	interface GigabitEthernet0/0/0/4.458
interface ATM1/0/0.370 point-to-point	l2transport
no atm enable-ilmi-trap	encapsulation dot1q 458
pvc 0/370 l2transport	!
encapsulation aal5snap	l2vpn
xconnect 192.169.105.10 123 pw-class inter-ether	xconnect group VPNSC
!	p2p iscind-crs-1--48856
	interface GigabitEthernet0/0/0/4.458
	neighbor 192.168.118.167 pw-id 123
	!
	!
	!

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、マルチポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：複数のリンクがあるエンドツーエンド回線を備えている疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンク（Flex 以外）が N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM4/1/0.8790。
  - N-PE 2 は IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：GigabitEthernet4/0/17.600。

コンフィグレット

N-PE 1（ATM）	N-PE 2（イーサネット）

`interface ATM4/1/0.8790 point-to-point`
`pvc 150/3454 l2transport`
`encapsulation aal5snap`
`xconnect 192.169.105.10 760 pw-class ISC-pw-tunnel-1`
	`interface GigabitEthernet4/0/17.600`
	`encapsulation dot1Q 600`
	`xconnect 192.169.105.20 760 pw-class ISC-pw-tunnel-1`

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、ローカル コア接続、ポイントツーポイント回線）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：ポイントツーポイント回線のローカル コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。この回線は、同じローカル N-PE 1 上で終端します。1 つのリンクは ATM インターフェイスで終端し、別の（Flex 以外）リンクはイーサネット インターフェイスで終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.444。
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：FastEthernet3/39.674。

コンフィグレット

N-PE 1（ATM + イーサネット）	N/A
! interface FastEthernet3/39.674 encapsulation dot1Q 674 ! interface ATM1/0/0.444 point-to-point pvc 44/4444 l2transport encapsulation aal5snap ! connect Customer1_204 ATM1/0/0 44/4444 FastEthernet3/39.674 interworking ethernet	

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、ブリッジ ドメインのあるエンドツーエンド回線、）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：ブリッジ ドメインがイネーブルにされている複数のリンクのあるエンドツーエンド回線の疑似回線コア接続を使用して、ATM とイーサネットがインターワーキングを実行するための EVC。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンクが N-PE 2 の Flex イーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.370。
  - N-PE 2 は、IOS XR 3.9.0 を備えた Cisco ASR 9000 です。

    インターフェイス：GigabitEthernet0/0/0/25.341。

コンフィグレット

N-PE 1（ATM）

```
!
interface ATM1/0/0.370 point-to-point
 no atm enable-ilmi-trap
 pvc 0/370 l2transport
  encapsulation aal5snap
xconnect 10.20.21.1 4531 pw-class
ISC-pw-tunnel-1
```

N-PE 2（イーサネット）

```
interface GigabitEthernet0/0/0/25.341
l2transport
 encapsulation dot1q 341
 rewrite ingress tag push dot1q 430
second-dot1q 349 symmetric
!
l2vpn
 bridge group tml
  bridge-domain CISCO
   interface GigabitEthernet0/0/0/25.341
   !
   neighbor 192.169.105.20 pw-id 32190
   !
  !
 !
!
```

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、ブリッジ ドメインのあるエンドツーエンド回線、）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：複数のリンクがあるエンドツーエンド回線の疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。ブリッジ ドメインはイネーブルにされています。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンク（Flex 以外）が N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.370。
  - N-PE 2 は、IOS XR 3.9.0 を備えた Cisco ASR 9000 です。

    インターフェイス：GigabitEthernet0/0/0/20.712。

コンフィグレット

N-PE 1（ATM）	N-PE 2（イーサネット）

!
 interface ATM1/0/0.370 point-to-point
  no atm enable-ilmi-trap
  pvc 0/370 l2transport
  encapsulation aal5snap
  xconnect 10.20.21.1 4531 pw-class ISC-pw-tunnel-1
  !
	interface GigabitEthernet0/0/0/20.712 l2transport
	  encapsulation dot1q 712
	 !
	 l2vpn
	  bridge group tml
	  bridge-domain CISCO
	  interface GigabitEthernet0/0/0/20.712
	  !
	  neighbor 192.169.105.20 pw-id 1005
	  !
	  !
	 !

コメント

- なし。

EVC（ATM-Ethernet インターワーキング、疑似回線コア接続、エンドツーエンド回線、ブリッジ ドメインなし）

設定

- EVC/ATM-Ethernet インターワーキング。
- 機能：複数のリンクがあるエンドツーエンド回線の疑似回線コア接続で ATM とイーサネットがインターワーキングを実行するための EVC。ブリッジ ドメインはディセーブルにされています。1 つのリンクが N-PE 1 の ATM インターフェイス上で終端し、別のリンクが N-PE 2 のイーサネット インターフェイス上で終端します。
- デバイス設定：
  - N-PE 1 は、IOS 12.2(33) SRB3 を備えた Cisco 7600 です。

    インターフェイス：ATM1/0/0.370。
  - N-PE 2 は、IOS XR 3.9.0 を備えた Cisco ASR 9000 です。

    インターフェイス：GigabitEthernet0/0/0/12.433。

コンフィグレット

N-PE 1（ATM）	N-PE 2（イーサネット）
!	interface GigabitEthernet0/0/0/12.433
interface ATM1/0/0.370 point-to-point	l2transport
no atm enable-ilmi-trap	encapsulation dot1q 433
pvc 0/370 l2transport	rewrite ingress tag push dot1q 43
encapsulation aal5snap	second-dot1q 53 symmetric
xconnect 10.20.21.1 4531 pw-class	!
ISC-pw-tunnel-1 !	l2vpn
	xconnect group ISC
	p2p CISCO
	interface GigabitEthernet0/0/0/12.433
	neighbor 192.169.105.20 pw-id 4531
	!
	!
	!
	!

コメント

- なし。

CHAPTER 4

RAN バックホール サービスの管理

この章では、Prime Provisioning で Radio Access Network（RAN）バックホール サービスを管理するために Prime Provisioning を使用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。

RAN バックホール サービスの概要

Radio Access Network（RAN）の転送は、セル サイトの Base Transceiver Station（BTS）から集約ノードと Base Station Controller（BSC）、BSC の間、および BSC と関連付けられた Mobile Switching Center（MSC）間で、バックホール トラフィック（音声とデータの両方）を管理します。図 4-1 には、RAN バックホール トポロジの例が示されています。

図 4-1　RAN バックホール トポロジの例

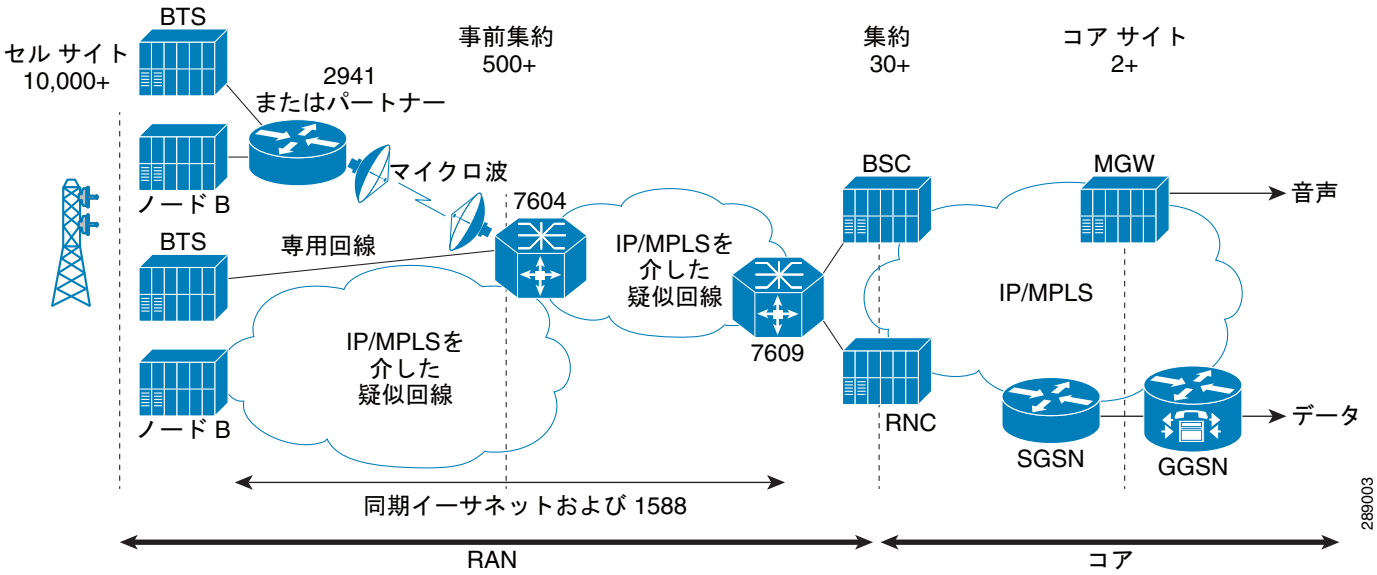
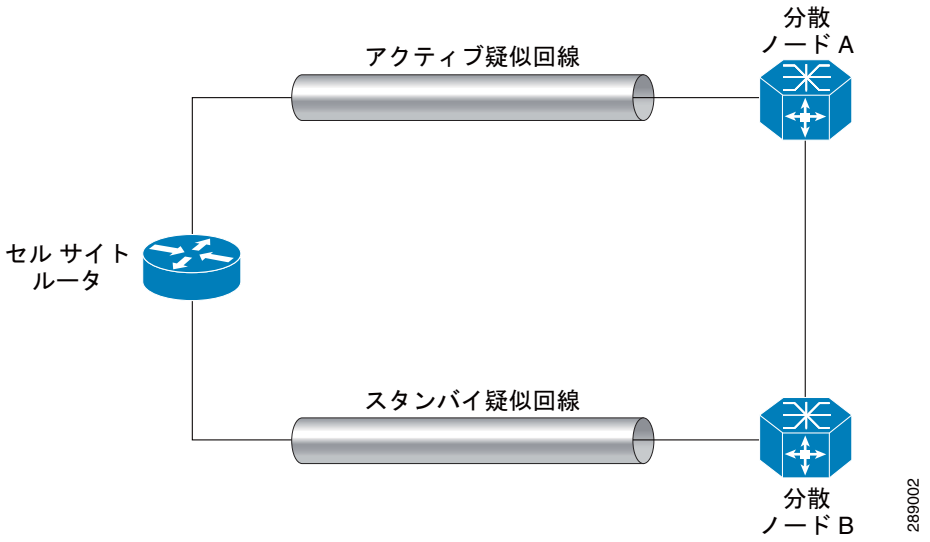


図 4-2 は、Prime Provisioning GUI で RAN バックホール サービスの設定方法を説明する際にこの章で使用するために抜粋されたトポロジ ビューです。

図 4-2　　RAN バックホール トポロジの抜粋



Prime Provisioning はインターネット プロトコル（IP）を使用して、RAN でバックホール トラフィックを転送します。Ethernet Virtual Circuit（EVC）ポリシーとサービス要求を Prime Provisioning で使用して次のサービスをプロビジョニングし、RAN バックホール トラフィック管理をサポートします。

- Circuit Emulation Time Delay Multiple Access（CEM TDM）
- 非同期転送モード（ATM）の疑似回線プロビジョニング

さらに、EVC サービス要求は、CEM と疑似回線クラス オブジェクトを使用して、サービスがプロビジョニングされるすべてのノードで再利用できるように、共通属性をバンドルします。

Prime Provisioning で RAN バックホール サービスを設定および管理するための基本的なワークフローには次のタスクが含まれます。

1. 前提条件を確認し、必要な設定作業を実行する。
2. RAN バックホール ポリシーとサービス要求で使用される CEM または疑似回線クラスを作成する。
3. CEM TDM または ATM ポリシーを作成する。
4. CEM TDM または ATM サービス要求で使用するテンプレートを作成する。
5. CEM TDM または ATM サービス要求を作成する。
6. ネットワーク上のデバイスにサービス要求を展開する。

この章は 2 つの項に分かれており、それぞれが CEM TDM サービスと ATM サービスを説明しています。上記のワークフロー タスクはこれらの各項に記載されています。

前提条件

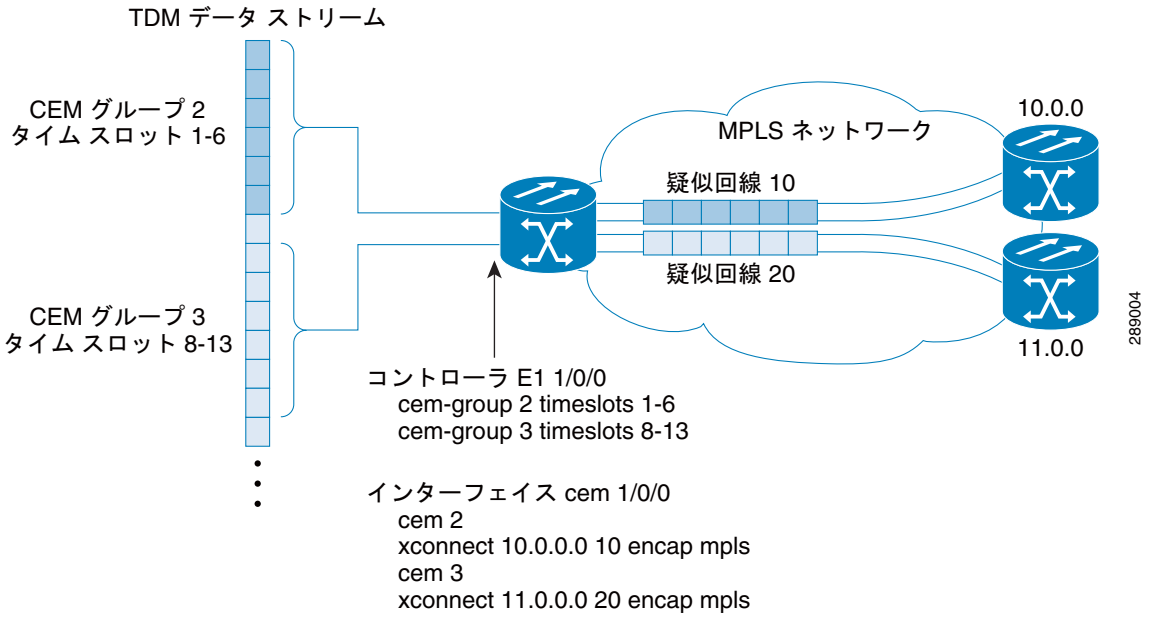
この項では、RAN バックホール サービスを Prime Provisioning 設定する前に把握しておく必要のある制約事項と前提条件について説明します。

CEM TDM ポリシーとサービス要求を作成するには、ターゲット デバイスやネットワーク リンクなどのサービス関連要素を最初に Prime Provisioning に定義する必要があります。通常、これらの要素は 1 回作成します。これらのタスクの対象範囲については、「Prime Provisioning サービスの設定」（P.3-6）を参照してください。また、基本インフラストラクチャ設定とディスカバリ タスクの実行方法については、このマニュアルの他の章を参照してください。この章の情報は、すでにこれらの準備タスクを実行していることを前提としています。

CEM TDM サービスに関する作業

回線エミュレーションは、Circuit Emulation Over Packet（CEoP）共有ポートアダプター（SPA）上で、時分割多重（TDM）データを MPLS パケットにカプセル化するように設定されています。これは、データを CEM 疑似回線を介してリモート プロバイダー エッジ（PE）ルータに送信します。トポロジの例を図 4-3 に示します。

図 4-3　回線エミュレーション（CEM）トポロジの例



この例では、次の点に注意してください。

- TDM 回線は、スロット 1、サブスロット 0（E1 コントローラ 1/0/0）に搭載された SPA のポート 0 に接続されます。
- MPLS ネットワーク経由で TDM データを伝送するために、2 つの疑似回線（PW10 および PW20）を設定します。
- TDM タイム スロット内のデータ用に 2 つの CEM グループ（2 および 3）を設定します。
  - タイム スロット 1 ～ 6 は、疑似回線 10 を介して、10.0.0.0 にあるリモート PE ルータに送信されます。
  - タイム スロット 8 ～ 13 は、疑似回線 20 を介して、11.0.0.0 にある PE ルータに送信されます。

次の転送メカニズムがサポートされています。

- SAToP PWE3：Structure Agnostic TDM over Packet / Pseudowire Edge-to-Edge

- CESoPSN PWE3：Circuit Emulation Service over Packet Switched Network / Pseudowire Edge-to-Edge

この項の残りの部分では、Prime Provisioning で RAN バックホールをサポートするために CEM TDM サービスを実装および管理する場合に必要なすべてのタスクについて説明します。具体的な内容は、次のとおりです。

- 「CEM クラスでの作業」（P.4-4）
- 「CEM TDM ポリシーの作成」（P.4-6）
- 「CEM TDM サービスでのテンプレート型変数の使用」（P.4-10）
- 「CEM TDM サービス要求の管理」（P.4-11）

CEM クラスでの作業

CEM クラス オブジェクトは、CEM インターフェイス パラメータを設定して、CEM インターフェイスのグループに適用できるようにするために使用されます。CEM クラスは、CEM TDM ポリシーまたはサービス要求で使用するように選択できます。CEM クラス オブジェクトは、サービスによって設定されたデバイス上に **cem class** コマンドと、それに関連する設定を設定するために使用されます。

（注）　CEM TDM ポリシーとサービス要求は、疑似回線クラスを使用することもできます。疑似回線クラスの作成および管理に関する情報は、このマニュアルの別の項で説明します。（詳細については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください）。

具体的な内容は、次のとおりです。

- 「CEM クラス オブジェクトの作成」（P.4-4）
- 「CEM クラス オブジェクトの編集」（P.4-5）
- 「CEM クラス オブジェクトの削除」（P.4-5）
- 「CEM クラスのサンプル コンフィグレット」（P.4-6）

CEM クラス オブジェクトの作成

CEM クラスを作成するには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI のトップレベル メニューから、[Inventory] > [Logical Inventory] > [CEM Class] を選択します。

[CEM Class] 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 CEM Class] ウィンドウが表示されます。

ステップ 3　次のように、ウィンドウのフィールドに該当する値を入力します。

- [Name]：CEM クラス オブジェクトの名前。このフィールドは必須です。
- [Description]：CEM クラスの説明。これは任意です。
- [Dejitter Buffer]：CEM コンフィギュレーション モードで、ネットワーク ジッタに使用されるデジッタ バッファのサイズ。範囲は 1 ～ 500 ミリ秒です。この値はオプションです。
- [Payload Size]：CEM コンフィギュレーション モードで使用されるペイロード サイズ。有効な範囲は 32 ～ 1312 バイトです。この値はオプションです。

- [Idle Pattern] : それぞれの損失 CESoPSN データ パケットのコンテンツの置換に使用する日付のパターン。範囲は 16 進数の 0x00 ～ 0xFF です。デフォルト パターンは 0xFF です。

ステップ 4　CEM クラスを作成するには、[Save] をクリックします。

作成操作が成功した場合、確認メッセージが表示され、[CEM Class] ウィンドウが再表示されて、新しい CEM クラスが [Class Name] カラムに表示されます。

CEM クラス オブジェクトの編集

CEM クラスを編集するには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI のトップレベル メニューから、[Inventory] > [Logical Inventory] > [CEM class] を選択します。

[CEM Class] ウィンドウが、Prime Provisioning ですでに作成されているすべての CEM クラスとともに表示されます。

ステップ 2　編集する CEM クラスのチェックボックスをオンにします。

ステップ 3　ウィンドウの右下の [Edit] ボタンをクリックします。

[Edit CEM Class] ウィンドウが表示されます。

ステップ 4　必要に応じて、属性値を変更します。

ステップ 5　[Save] ボタンをクリックして変更を保存します。

編集が成功すると、確認メッセージが表示され、[CEM Class] ウィンドウが再表示されます。

CEM クラス オブジェクトの編集に関する注意事項

- CEM クラスの名前は、作成後に変更できません。このため、CEM クラスの編集中に [Name] フィールドを変更することはできません。他のフィールドはすべて編集可能です。
- サービス要求で使用されている CEM クラスを編集すると、特定のサービス要求が組み込まれます。複数のサービス要求で編集済みの CEM クラスを使用する場合、サービス要求はすべて組み込まれます。「組み込まれる」とは、サービス要求が [Requested] 状態になり、導入の準備ができていることを示します。
- 1 つ以上の CEM TDM のサービス要求に関連付けられた CEM クラスで属性が変更された場合、関連するまたは影響を受けるサービス要求がすべて組み込まれます。GUI にウィンドウが表示され、影響を受けるサービス要求のリストが表示されます。サービス要求のリストから、次のいずれかを実行できます。
  - [Save] ボタンをクリックして、後で導入するためにサービス要求を保存する。
  - [Save and Deploy] ボタンをクリックして、サービス要求を保存する。サービス要求は、[Requested] 状態になり、展開する準備が整います。

CEM クラス オブジェクトの削除

CEM クラスを削除するには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI のトップレベル メニューから、[Inventory] > [Logical Inventory] > [CEM Class] を選択します。

[CEM Class] ウィンドウが、Prime Provisioning ですでに作成されているすべての CEM クラスとともに表示されます。

ステップ 2　削除する CEM クラスのチェックボックスをオンにします。

ステップ 3　ウィンドウの右下の [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　[Delete] ボタンをクリックして、削除を確定します。

削除操作が成功した場合、確認メッセージが表示され、[CEM Class] ウィンドウが再表示されて、削除済みの CEM クラスが [Class Name] カラムから削除された状態で表示されます。

CEM クラス オブジェクトの削除に関する注意事項

- CEM TDM ポリシーまたはサービス要求とともに使用されている CEM クラスは削除できません。

CEM クラスのサンプル コンフィグレット

次に、CEM クラスを作成するために生成されるサンプル コンフィグレットの例を示します。

```
class cem ranCemClass
 payload-size 512
 dejitter-buffer 10
 idle-pattern 0x55
 !
```

次に、CEM クラスが設定にどのように組み込まれるかを示すサンプル コンフィグレットを示します。

```
interface cem 0/0
 no ip address
 cem 0
   cem class mycemclass
   xconnect 10.10.10.10 200 encapsulation mpls
   !
 !
```

CEM TDM ポリシーの作成

この項では、CEM TDM ポリシーを作成する方法について説明します。

サービスをプロビジョニングするには、CEM TDM ポリシーを定義する必要があります。ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。ポリシーは、サービス要求の定義に必要な大部分のパラメータのテンプレートです。ポリシーを定義すると、共通する一連の特性を共有するすべてのサービス要求で使用できます。新しいタイプのサービスまたは異なるパラメータを持つサービスを作成する場合は、常に新しい CEM TDM ポリシーを作成します。

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 ファイルを使用する方法の詳細については、「ポリシーでのテンプレートの使用」（P.9-22）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。

CEM TDM 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] > [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　[Create] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 3　[Policy Type] ドロップダウン リストから [EVC] を選択します。

[Policy Editor] ウィンドウが表示されます。

ステップ 4　EVC ポリシーの [Policy Name] を入力します。

ステップ 5　EVC ポリシーの [Policy Owner] を選択します。

EVC 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：すべてのサービス オペレータがこの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 EVC 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。

ステップ 6　EVC ポリシーの所有者を選択するには、[Select] をクリックします。

ポリシー所有者は、Prime Provisioning の設定中にカスタマーまたはプロバイダーを作成した際に設定しました。所有権がグローバルの場合は、[Select] 機能は表示されません。

ステップ 7　[Circuit-Emulation-TDM] を [Policy Type] として選択します。

ステップ 8　[Next] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 9　次の項である「サービス オプションの設定」（P.4-7）に記載されているステップに進みます。

サービス オプションの設定

CEM TDM ポリシーのサービス オプションを設定するには、次の手順を実行します。

（注）　MPLS Core 接続属性はデフォルトで PSEUDOWIRE に設定され、変更することはできません。

ステップ 1　ドロップダウン リストから [TDM CEM Service Options] の 1 つを選択します。

選択できる基準は、次のとおりです。

- [SAToP_UNFRAMED] : Structure-agnostic TDM over packet。このモードは、T1 または E1 非構造化（非チャネライズド）サービスをパケットスイッチド ネットワークを介してカプセル化するために使用されます。SAToP モードでは、バイトは TDM 回線に到着したとおりに送信されます。

バイトはフレーミングと揃える必要はありません。このモードでは、インターフェイスは、継続的にフレーム化されたビット ストリームと見なされます。すべてのシグナリングはビット ストリームの一部として透過的に伝送されます。

- [CESoPN_TIMESLOT] : Circuit emulation services over packet-switched network。このモードは、T1 または E1 構造化（チャネライズド）サービスを PSN を介してカプセル化するために使用されます。CESoPN は、フレーミングを特定し、ペイロードのみを送信します。DS3 の T1 と T1 の DS0 のチャネライズを行えます。DS0 は同一パケットにバンドルできます。

ステップ 2　ドロップダウン リストから、[CEM Container Type] を選択します。

選択できる基準は、次のとおりです。

- [T1] : T-1 デジタル回線。DS-1（デジタル シグナリングのレベル 1）シグナリング フォーマットを使用して 1.544 Mbps で PSTN ネットワーク上の音声およびデータを送信します。
- [E1] : E-1 デジタル回線。音声またはデータ コール用の 30 64Kbps デジタル チャネル（DS0）、シグナリング用の 64Kbps チャネル、フレーミングおよびメンテナンス用の 64Kbps チャネルを伝送します。

ステップ 3　[Next] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 4　次の項である「[Service] 属性の設定」（P.4-8）に記載されているステップに進みます。

[Service] 属性の設定

CEM TDM ポリシーのサービス属性を設定するには、次の手順を実行します。

ステップ 1　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[Enable PseudoWire Redundancy] 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方法に関する注釈については、付録 C「2 台の N-PE 上でのアクセス リングの終端」、および特に「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）を参照してください。

ステップ 2　サービス要求の作成中に Prime Provisioning に VC ID を自動選択させるには、[AutoPick VC ID] 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フにすると、オペレータは、サービス要求の作成中に VC ID を指定するよう求められます。

使用方法に関する注釈：

- [AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。

ステップ 3　[Next] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 4　次の項である「疑似回線と CEM クラスの使用」（P.4-8）に記載されているステップに進みます。

疑似回線と CEM クラスの使用

CEM TDM ポリシーで使用する疑似回線または CEM クラスを指定するには、次の手順を実行します。

ステップ 1　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR デバイスでの **pw-class** コマンドのプロビジョニングに使用されます。疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning 以前に作成した疑似回線クラスを選択するには、[Select] ボタンをクリックします。
- [Use PseudoWireClass] は IOS デバイスに対してのみ適用できます。

ステップ 2　CEM クラスの選択をイネーブルにするには、[Use CEM Class] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- CEM クラスは、IOS デバイスで **cem class ranCemClass** コマンドをプロビジョニングするために使用されます。CEM クラスのサポートの詳細については、「CEM クラスでの作業」（P.4-4）を参照してください。
- [Use CEM Class] をオンにすると、追加属性の [CEM Class] が GUI に表示されます。Prime Provisioning で以前に作成した CEM クラスを選択するには、[Select] ボタンをクリックします。
- [Use CEM Class] は、IOS デバイスに対してのみ適用できます。

ステップ 3　[Next] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 4　次の項である「CEM TDM ポリシー ワークフローへのユーザ定義フィールドの追加」（P.4-9）に記載されているステップに進みます。

CEM TDM ポリシー ワークフローへのユーザ定義フィールドの追加

[Additional Information] 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ができます。追加情報機能の使用方法の詳細については、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。

次の項である「テンプレートの関連付けのイネーブル化」（P.4-9）に記載されているステップに進みます。

テンプレートの関連付けのイネーブル化

Prime Provisioning テンプレート機能を使用すると、デバイスにフリーフォーマット CLI をダウンロードできます。テンプレートをイネーブルにする場合は、Prime Provisioning で現在サポートされていないコマンドをダウンロードするために、テンプレートとデータ ファイルを作成できます。

（注）　テンプレート変数のサポートは、CEM TDM サービスで使用できます。CEM 関連の変数を含むテンプレートとデータ ファイルの例を使用できます。このテンプレートへのアクセスと使用方法についての詳細は、次の項「CEM TDM サービスでのテンプレート型変数の使用」（P.4-10）を参照してください。

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、（[Finish] をクリックする前に）[Interface Attribute] ウィンドウで [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、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、「ポリシーでのテンプレートの使用」（P.9-22）を参照してください。

ステップ 2　ポリシー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] をクリックして閉じて、[Policy Editor] ウィンドウに戻ります。

ステップ 3　CEM TDM ポリシーを保存するには、[Finish] をクリックします。

CDM TEM ポリシーに基づいてサービス要求を作成するには、「CEM TDM サービス要求の管理」（P.4-11）を参照してください。

CEM TDM サービスでのテンプレート型変数の使用

この項では、Prime Provisioning でサンプルの CEM テンプレートにアクセスして使用する方法について説明します。

CEM テンプレート例のデータ ファイルを作成するには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI で、[Service Design] > [Templates] > [Template Manager] を選択します。

[Template Manager] ウィンドウが表示されます。

ステップ 2　[Templates] ウィンドウでルート フォルダをクリックして展開します。

サブフォルダのリストが、最上部の [Examples] フォルダとともに表示されます。

ステップ 3　[Examples] フォルダをクリックしてフォルダを展開します。

CEM テンプレートを含む複数のサンプル テンプレートが表示されます。

ステップ 4　CEM フォルダをクリックして選択します。

CEM テンプレートは、テーブルの [Data File Name] カラムに事前にロードされた CEMProvisioning データ ファイルとともに [Template] ウィンドウに表示されます。

ステップ 5　[Edit] ボタンをクリックして CEMProvisioning データ ファイルを編集するか、これをオフにして [Create Data File] をクリックし、新しいファイルを作成します。

いずれの場合も、[Data File Editor] ウィンドウが表示されます。このファイルを使用して、CEM TDM サービスをプロビジョニングするために必要なテンプレート変数をマッピングできます。

ステップ 6　テンプレート変数に必要な変更を行った場合、[Save] をクリックして変更を保存します。

ステップ 7　[Close] をクリックして、[Data File Editor] ウィンドウを閉じます。

CEM TDM サービス要求の管理

この項では、CEM TDM のサービス要求を管理するためのワークフローのさまざまなタスクについて説明します。次の事項について説明します。

CEM TDM のサービス要求の作成

CEM TDM サービス要求の作成を開始するには、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。

ステップ 2　[Create] 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 3　[Policy] ドロップダウン リストを使用して、以前に作成したポリシーから CEM TDM ポリシーを選択します（「CEM TDM ポリシーの作成」（P.4-6）を参照）。これは、ポリシー名に EVC が続くことからわかるように、タイプ EVC のポリシーになります。

[EVC Service Request Editor] ウィンドウが表示されます。これは、サービス要求の属性を追加または変更できるワークフローの初期ウィンドウです。新しいサービス要求は、すべての編集可能な機能と編集不可能な機能および事前設定されたパラメータなど、選択したポリシーのプロパティをすべて継承します。

ステップ 4　次の項である「サービス要求の詳細の設定」（P.4-11）に記載されているステップに進みます。

サービス要求の詳細の設定

[Service Request Details] セクションに属性を設定するには、次の手順を実行します。

（注）　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

（注）　[Policy Name] フィールドは読み取り専用です。サービス要求の元になっているポリシーの名前が表示されます。読み取り専用のポリシー名をクリックすると、ポリシー内で設定されているすべての属性値のリストが表示されます。

ステップ 1　Prime Provisioning に VC ID を選択させる場合は、[AutoPick VC ID] 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しない場合は、次のステップで説明されているように、[VC ID] フィールドで ID を指定するよう求めるプロンプトが表示されます。

[AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。この場合は、[VC ID] オプションのテキスト フィールドは編集不可能です。

ステップ 2　[AutoPick VC ID] をオフにした場合は、[VC ID] フィールドに VC ID を入力します。

使用方法に関する注釈：

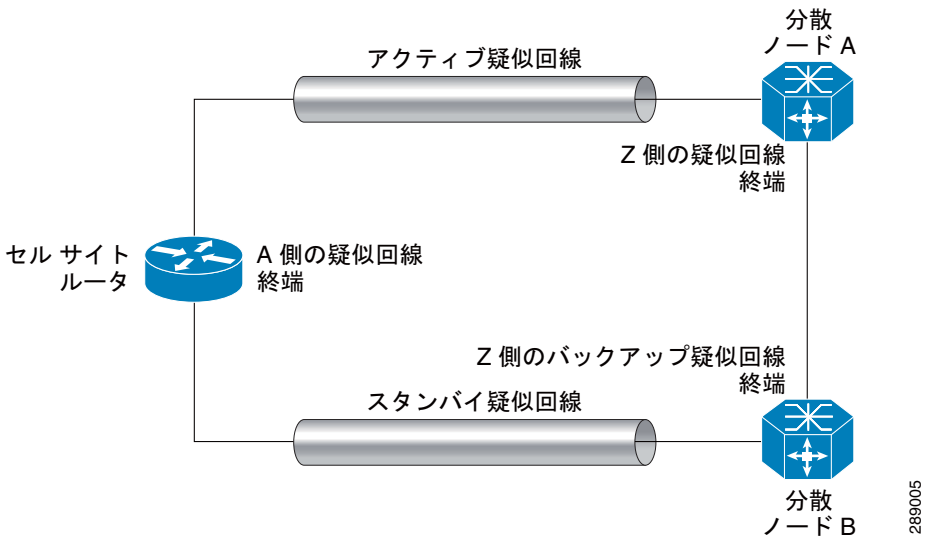
- [VC ID] 値は、VC ID に対応する整数値でなければなりません。
- VC ID を手動で割り当てると、Prime Provisioning は VC ID を調べて、Prime Provisioning の VC ID プール内にそれがあるかどうかを確認します。VC ID がプール内にあっても割り当てられていない場合は、VC ID はサービス要求に割り当てられます。VC ID がプール内にあって、すでに使用中の場合は、Prime Provisioning は別の VC ID を割り当てるよう求めるプロンプトを表示します。VC ID が Prime Provisioning VC ID プールの外にある場合は、Prime Provisioning は、VC ID が割り当てられているかどうかに関する検査を実行しません。オペレータは、VC ID が使用可能であることを確認する必要があります。
- VC ID は、サービス要求の作成中に限り入力できます。サービス要求の編集中は、[VC ID] フィールドは編集不可能です。

ステップ 3　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[PseudoWire Redundancy] 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：

- [PseudoWire Redundancy] がオフの場合、疑似回線の冗長性はサービス要求でプロビジョニングされません。したがって、サービスに対して有効に機能するデバイスは 2 つのみになります。設定例については、図 4-4 を参照してください。一方のデバイスは、疑似回線の「A」側にあり、もう一方は疑似回線の「Z」側にあります。この場合、バックアップ PW VC ID を入力できません。

図 4-4　疑似回線終端の例



- [Pseudowire Redundancy] チェックボックスをオンにすると、サービスに有効に機能するデバイスは 3 台になります。一方のデバイスは、疑似回線の「A」側にあり、もう一方のデバイスは「Z」側にあります。この場合、バックアップ PW VC ID 属性を使用して「Z」側のバックアップ疑似回線を設定できます。
- このオプションの使用方法に関する注釈については、付録 C「2 台の N-PE 上でのアクセス リングの終端」、および特に「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）を参照してください。

ステップ 4　設定に問題がなければ、[Backup PW VC ID] フィールドにバックアップ疑似回線の VC ID を入力します。

バックアップ VC ID の動作は、プライマリ疑似回線の VC ID の動作と同じです。

ステップ 5　ドロップダウン リストから、[CEM Container Type] を選択します。

選択できる基準は、次のとおりです。

- [T1]：T-1 デジタル回線。DS-1（デジタル シグナリングのレベル 1）シグナリング フォーマットを使用して 1.544 Mbps で PSTN ネットワーク上の音声およびデータを送信します。
- [E1]：E-1 デジタル回線。音声またはデータ コール用の 30 64Kbps デジタル チャネル（DS0）、シグナリング用の 64Kbps チャネル、フレーミングおよびメンテナンス用の 64Kbps チャネルを伝送します。

使用方法に関する注釈：

- CEM コンテナ タイプが T1 に設定されている場合、フレーミング タイプ属性は GUI に動的に表示されます。これは、次の手順で説明されているように設定できます。

ステップ 6　ドロップダウン リストから [Framing Type] を選択します。

選択できる基準は、次のとおりです。

- [SDH]：Synchronous Digital Hierarchy（同期デジタル階層）。
- [SONET]：Synchronous Optical Networking。

これらは、Synchronous Data Transmission Over Fiber Optic Network の標準に関連します。これらのプロトコルの詳細については、このユーザ ガイドでは説明しません。

ステップ 7　CEM クラス オブジェクトの選択をイネーブルにするには、[Use CEM Class] 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：

- CEM クラスはサービス要求レベルで編集できます。したがって CEM クラスは、サービス要求のポリシーの 1 セットから変更することもできます。CEM クラスを変更しない場合、ポリシーで指定されたものがサービス プロビジョニングのために維持されます。
- CEM クラスは、IOS デバイスで **cem class ranCemClass** コマンドをプロビジョニングするために使用されます。CEM クラスのサポートの詳細については、「CEM クラスでの作業」（P.4-4）を参照してください。
- [Use CEM Class] をオンにすると、追加属性の [CEM Class] が GUI に表示されます。Prime Provisioning で以前に作成した CEM クラスを選択するには、[Select] ボタンをクリックします。
- [Use CEM Class] は、IOS デバイスに対してのみ適用できます。

ステップ 8　次の項である「デバイスの選択」（P.4-14）に記載されているステップに進みます。

デバイスの選択

[EVC Service Request Editor] ウィンドウの [Devices] セクションを使用して、N-PE へのリンクを設定することができます。Prime Provisioning では、CEM TDM プロビジョニング用に追加されたデバイスは、N-PE ロール ベースのデバイスと見なされます。デバイスを選択した後、コントローラを選択し、デバイスの他の属性を設定します。

図 4-4 に示されている設定例は、ここでも使用されます。

次のステップを実行します。

ステップ 1　[Select Device] リンクをクリックして、疑似回線終端ポイントの「A」側を選択します。

[Select PE Device] ウィンドウが表示されます。

（注）　「A」ノードでサポートされているデバイス タイプには、該当する CEoP および SPA ライン カードを持つ MWR 2941-DC および 760X シリーズのデイバスが含まれています。

ステップ 2　適切なデバイスを選択し、[Save] をクリックします。

ステップ 3　[Controller] カラムで、デバイスのドロップダウン リストから目的のコントローラを選択します。

使用方法に関する注釈：

- ドロップダウン リストに表示されるコントローラは、上記で指定された [CEM Container Type] 属性の値によって異なります。
- [CEM Container Type] が [TI] の場合、T1 コントローラのみがリストに組み込まれます。コンテナ タイプが [E1] の場合、E1 コントローラのみがリストに表示されます。
- 選択したデバイスで特定タイプのコントローラがない場合、ドロップダウン リストは空になります。
- また、[CEM Container Type] が [TI] の場合、追加の [Framing Type] 属性の値によってコントローラのリストが変更されます。たとえば、[Framing Type] が [SONET] である場合、SONET コントローラがコントローラ リストに表示されます。次に、リストから SONET コントローラを選択して [Edit] をクリックすると、SONET コントローラの属性ウィンドウが開きます。[Framing Type] が [SDH] である場合、リストから SONET コントローラを選択して [Edit] をクリックすると、SDH コントローラの属性ウィンドウが開きます。

ステップ 4　「A」側の終端装置のコントローラを選択したら、[Link Attributes] カラムの [Edit] リンクをクリックしてコントローラ属性を設定します。

[EVC Service Request Editor - Standard UNI Details] ウィンドウが表示されます。これには、いずれかの T1/E1 コントローラ属性のリストが表示されます。

ステップ 5　「A」側のターミナル デバイスの T1/E1 コントローラの属性の設定

- [CEM Group ID] : コントローラの下の [CEM Group ID] は、コントローラと同じスロット / サブスロット / ポート情報を持つ CEM インターフェイスを作成します。これが取れる数は、E1 または T1 回線のどちらであるかによって異なります。0 ～ 23 の任意の数字。
- [Clock Source] : INTERNAL または LINE。デフォルトは INTERNAL です。
- [Time-Slot Range] : T1 コントローラの場合は 1 ～ 31 の値で、E1 コントローラの場合は 1 ～ 24 の値です。

（注）　ポリシーの [TDM CEM Service Options] 属性が CESoPN_TIMESLOT に設定されていた場合にのみ、[Time-Slot Range] 属性が表示されます。このため、属性が SAToP_UNFRAMED に設定されていた場合は表示されません。

- [Use PseudoWireClass]：サービス要求に既存の疑似回線クラスを関連付けるには、このチェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、疑似回線クラスを選択できます。サービス要求から疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。
- [Use Backup PseudoWireClass]：（この属性は [Pseudowire Redundancy] 属性がオンになっている場合にのみ使用できます）。既存の疑似回線クラスをバックアップ疑似回線クラスとしてサービス要求に関連付けるには、チェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、バックアップ疑似回線クラスを選択できます。サービス要求から疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。この機能は、サービス要求ウィンドウの [Pseudowire Class] での選択と似ています。[Use Backup PseudowireClass] 属性は「A」ターミナルにのみ適用できます。「Z」および「Z - バックアップ」ターミナルには適用できません。

ステップ 6　「A」ターミナル デバイスの T1/E1 コントローラに属性を設定した後、[OK] をクリックします。

[EVC Service Request Editor] ウィンドウが再表示されます。

ステップ 7　「A」ターミナル デバイスに対して実行した手順と同じ手順に従って、「Z」を選択し、該当する場合は「Z - バックアップ」ターミナル デバイスとそれらのコントローラを選択します。

SONET コントローラが、「Z」および「Z - バックアップ」ターミナル デバイスの [Controller] ドロップダウン リストに組み込まれます。

ステップ 8　これらの終端装置のコントローラを選択したら、[Link Attributes] カラムの [Edit] リンクをクリックしてコントローラ属性を設定します。

[Standard UNI Details] ウィンドウが表示され、SONET コントローラの属性が表示されます。

ステップ 9　SONET コントローラの属性を設定します。

このウィンドウに表示される SONET 属性は CEM コンテナ タイプ、SONET コントローラ フレーミング タイプ、管理ユニット グループ（AUG）マップ、チャネライゼーション モードによって異なります。これについては、表 4-1 で概説されています。

表 4-1　CEM コンテナ タイプおよび SONET コントローラの属性

CEM コンテナ タイプ	SONET コントローラのフレーミングのシーケンス	AUG マッピング	チャネライゼーション モード
E1	SDH	Au-4	C-12
T1	SDH	Au-3	C-11
T1	SONET	N/A	STS-1

参考のために、使用可能な属性のスーパーセットを次に示します。GUI に実際に表示されるものは、GUI で以前に選択したものによって異なります。

- [CEM Group ID]：コントローラの下の [CEM Group ID] は、コントローラと同じスロット/サブスロット/ポート情報を持つ CEM インターフェイスを作成します。これが取れる数は、E1 または T1 回線のどちらであるかによって異なります。0 ～ 23 の任意の数字。
- [Clock Source]：INTERNAL または LINE。デフォルトは INTERNAL です。

- [AUG-Mapping] : SDH フレーミングが選択されている場合に、管理ユニット グループ（AUG）マッピングを設定します。au-3 または au-4。
- [Channelization Mode] : TDM チャネライゼーションを指定するために使用されるモード。c-11、c-12、または sts-1。
- [au3 Number] : 1 ～ 3 の範囲の数字。これは、AU-.3 にマッピングされた E1 回線の特定の管理ユニット タイプ 3（AU-3）を設定するために使用されます。
- [sts-1 Number] : 同期転送信号を識別するために使用される番号。1 ～ 3 の数字。
- [sts-1 Mode] : 同期転送信号。STS-1 モードの動作として、VT-15 を指定します。
- [tug-2 Number] : トリビュタリ ユニット グループ タイプ 2（TUG-2）。1 ～ 7 の任意の数字、または数字の範囲。TUG-2 番号の範囲を指定するには、1-5 のように、値の間にダッシュを使用します。2,4 のように値の間にカンマを使用して、TUG-2 を個別に指定できます。ユーザがテキスト ボックスに値を設定する必要があります。デフォルト値はありません。
- [tug-3 Number] : トリビュタリ ユニット グループ タイプ 3（TUG-3）。1 ～ 7 の任意の数字、または数字の範囲。
- [VTG Number] : T1 を伝送する仮想トリビュタリ グループ。1 ～ 7 の任意の数字、または数字の範囲。
- [T1 Line Number] : サービスを設定する必要のある T1 番号を指定します。1 ～ 4 の数字。
- [E1 Number] : サービスを設定する必要のある E1 番号を指定します。1 ～ 3 の数字。
- [Time Slot] : コンテナのタイプ（E1 または T1）に応じて、1 ～ 24、または 1 ～ 31 の数字。
- [Time-Slot Range] : T1 コントローラの場合は 1 ～ 31 の数字で、E1 コントローラの場合は 1 ～ 24 の数字です。

（注）　ポリシーの [TDM CEM Service Options] 属性が CESoPN_TIMESLOT に設定されていた場合にのみ、[Time-Slot Range] 属性が表示されます。このため、属性が SAToP_UNFRAMED に設定されていた場合は表示されません。

- [Use PseudoWireClass] : サービス要求に既存の疑似回線クラスを関連付けるには、このチェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、疑似回線クラスを選択できます。サービス要求から疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。

ステップ 10　SONET コントローラ値を設定してから、[OK] をクリックします。

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

ステップ 11　必要であれば、[Swap Terminals] ドロップダウン リストを使用して、ターミナルに関連するデバイスの順序を変更します。

この選択は、設定に基づきます。

- Swap A - Z
- Swap A - Z Backup
- Swap Z- Z Backup

スワップ操作を実行するためのオプションの 1 つを選択します。デバイスは、選択内容に基づいて [Select Devices] カラムで並べ替えられます。

使用方法に関する注釈：

- [Swap Terminals] ボタンは、サービス要求を最初に作成する場合にのみ表示されます。後でサービス要求を編集する場合、このボタンは表示されず、その時点でスワップ操作を実行することはできません。
- [Swap A - Z Backup] および [Swap Z - Z Backup] オプションは、[Pseudowire Redundancy] 属性がオンになっている場合にのみ使用できます。
- デバイスとターミナルがスワップされる場合、コントローラを [Controller] カラムでリセットする必要があります。

ステップ 12　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、サービス要求を作成します。

属性が欠落しているか、設定が間違っている場合、Prime Provisioning に警告が表示されます。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「CEM TDM のサービス要求の変更」（P.4-17）の項を参照してください。CEM TDM サービス要求の保存に関する追加情報については、「CEM TDM のサービス要求の保存」（P.4-18）を参照してください。

CEM TDM のサービス要求の変更

リンクまたはサービス要求の他の設定を変更する必要がある場合は、CEM TDM サービス要求を変更できます。

サービス要求を変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

[Service Request Manager] ウィンドウが表示され、Prime Provisioning で使用可能なサービス要求が示されます。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

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

ステップ 4　必要に応じて、属性を変更します。

ステップ 5　テンプレートまたはデータ ファイルを接続回線に追加するには、「CEM TDM の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」（P.4-17）の項を参照してください。

ステップ 6　CEM TDM サービス要求の編集が終了したら、[Save] をクリックします。

CEM TDM サービス要求の保存に関する追加情報については、「CEM TDM のサービス要求の保存」（P.4-18）を参照してください。

CEM TDM の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

Prime Provisioning では、アプリケーションによって管理されるデバイスで使用可能なすべての CLI コマンドの設定はサポートされません。そのようなコマンドをデバイス上で設定するために、Prime Provisioning Template Manager 機能を使用できます。テンプレートは、デバイス ロール単位でポリシー レベルで関連付けることができます。サービス要求レベルでのテンプレートの上書きは、ポリシーレベルの設定でオペレータに許可されている場合は行うことができます。

サービス要求でテンプレートとデータ ファイルを関連付けるには、[Service Request Editor] ウィンドウで任意のリンクを選択して、ウィンドウの下部にある [Template] ボタンをクリックします。

（注）　関連付けられたポリシーでテンプレート機能が使用可能になっていない場合は、[Template] ボタンは選択できません。

[SR Template Association] ウィンドウが表示されます。このウィンドウでは、デバイス単位レベルでテンプレートを関連付けることができます。[SR Template Association] ウィンドウには、リンクを構成するデバイス、デバイス ロール、およびデバイスに関連付けられているテンプレートとデータ ファイルが一覧表示されます。この場合は、テンプレートまたはデータ ファイルはまだ設定されていません。

テンプレートとデータ ファイルをサービス要求に関連付ける方法の詳細については、「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。

CEM TDM のサービス要求の保存

CEM TDM サービス要求を保存するには、次の手順を実行します。

ステップ 1　サービス要求の属性の設定が終了したら、[Save] をクリックして、サービス要求を作成します。

サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウが表示されます。新しく作成された CEM TDM サービス要求が [REQUESTED] の状態で追加されます。

ただし、何らかの理由で（たとえば、選択した値が範囲外である）サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

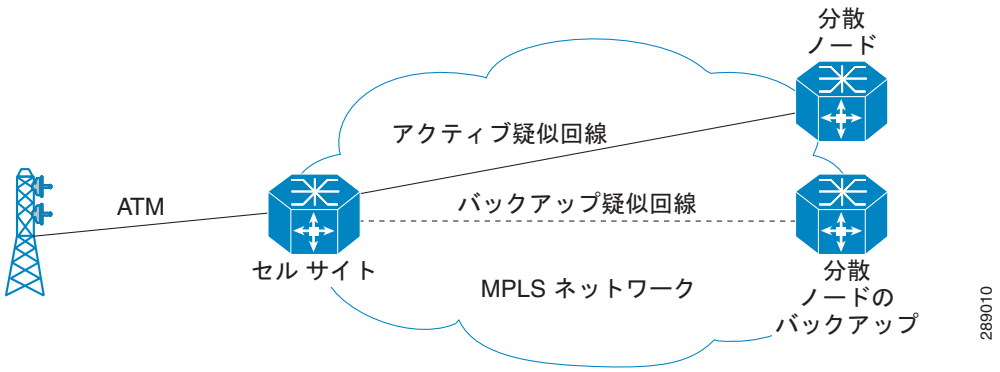
ステップ 2　CEM TDM サービス要求を展開する準備ができたら、「サービス要求の展開」（P.8-10）を参照してください。

CEM TDM サービスのサンプル コンフィグレットについては、「RAN バックホール サービスのサンプル コンフィグレット」（P.4-33）を参照してください。

ATM サービスでの作業

RAN バックホール サービスは ATM（ATM/IMA）仮想チャネル接続（VCC）または相手先固定パス（PVP）回線の逆多重化で設定できます。データは、リモート プロバイダー エッジ（PE）ルータに ATM 疑似回線で送信されます。ATM エンドポイントで疑似回線を作成する場合、IMA インターフェイスを選択して、その下に相手先固定接続（PVC）を作成できます。また、対応する IMA インターフェイスを作成できるコントローラを作成することもできます。トポロジの例を図 4-5 に示します。

図 4-5　ATM トポロジの例



次の転送メカニズムがサポートされています。

- ATM IMA VCC PWE3：ATM Inverse Multiplexing for ATM / Virtual Channel Connection / Pseudowire Edge-to-Edge。
- ATM IMA PVP PWE3：ATM Inverse Multiplexing for ATM / Permanent Virtual Path / Pseudowire Edge-to-Edge。

この項では、Prime Provisioning で ATM サービスを管理して RAN バックホールをサポートするためのワークフローにおけるさまざまなタスクについて説明します。具体的な内容は、次のとおりです。

- 「疑似回線クラスでの作業」（P.4-19）
- 「ATM ポリシーの作成」（P.4-19）
- 「ATM サービスでのテンプレート型変数の使用」（P.4-22）
- 「テンプレートを使用した ATM/IMA インターフェイスの作成」（P.4-23）
- 「ATM サービス要求の管理」（P.4-26）

疑似回線クラスでの作業

疑似回線クラスは、クラス オブジェクトに関連するさまざまな属性を設定するために使用されます。疑似回線クラスでは、カプセル化、トランスポート モード、フォールバック オプションの設定、および疑似回線を転送できるトラフィック エンジニアリング トンネルの選択がサポートされます。疑似回線クラスは、後で ATM ポリシーまたはサービス要求で使用されます。

（注）　疑似回線クラスの作成および管理に関する情報は、このマニュアルの別の項で説明します。「疑似回線クラスの作成および変更」（P.3-16）を参照してください。

ATM ポリシーの作成

この項では、ATM ポリシーの作成方法について説明します。

サービスをプロビジョニングするには、ATM ポリシーを定義する必要があります。ポリシーは、類似したサービス要件を持つ 1 つ以上のサービス要求で共有できます。ポリシーは、サービス要求の定義に必要な大部分のパラメータのテンプレートです。ポリシーを定義すると、共通する一連の特性を共有するすべてのサービス要求で使用できます。新しいタイプのサービスまたは異なるパラメータを持つサービスを作成する場合は、常に新しい ATM ポリシーを作成します。

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の使用」（P.9-22）を参照してください。ポリシーでのテンプレートおよびデータ ファイルの使用方法の詳細については、上記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。

ATM 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] > [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　[Create] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 3　[Policy Type] ドロップダウン リストから [EVC] を選択します。

[Policy Editor] ウィンドウが表示されます。

ステップ 4　EVC ポリシーの [Policy Name] を入力します。

ステップ 5　EVC ポリシーの [Policy Owner] を選択します。

EVC 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：すべてのサービス オペレータがこの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 EVC 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。

ステップ 6　EVC ポリシーの所有者を選択するには、[Select] をクリックします。

ポリシー所有者は、Prime Provisioning の設定中にカスタマーまたはプロバイダーを作成した際に設定しました。所有権がグローバルの場合は、[Select] 機能は表示されません。

ステップ 7　[Policy Type] として [ATM] を選択します。

ステップ 8　[Next] をクリックします。

[Create New EVC Policy] ウィンドウが表示されます。

ステップ 9　次の項である「ATM インターフェイス属性の設定」（P.4-20）に記載されているステップに進みます。

ATM インターフェイス属性の設定

この項では、ATM ポリシーの ATM インターフェイス属性を設定する方法について説明します。

ATM インターフェイス属性を設定するには、次のステップを実行します。

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

選択できる基準は、次のとおりです。

- [VP]：仮想パス モード。これはデフォルトです。
- [VC]：仮想回線モード。このオプションを選択すると、GUI に [ATM Encapsulation] 属性がデフォルト値 AAL0 とともに表示されます。[ATM Encapsulation] は変更できません。

ステップ 2　[Next] をクリックします。

[Policy Editor] ウィンドウが表示され、[Service Attributes] セクションが表示されます。

ステップ 3　次の項である「[Service] 属性の設定」（P.4-21）に記載されているステップに進みます。

[Service] 属性の設定

サービス属性を設定するには、次の手順を実行します。

ステップ 1　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[Enable PseudoWire Redundancy] チェックボックスをオンにします。

ステップ 2　サービス要求の作成中に Prime Provisioning に VC ID を自動選択させるには、[AutoPick VC ID] 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フにすると、オペレータは、サービス要求の作成中に VC ID を指定するよう求められます。

使用方法に関する注釈：

- [AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。

ステップ 3　[Next] をクリックします。

[Policy Editor] ウィンドウが表示され、[Pseudowire] セクションが表示されます。

ステップ 4　次の項である「疑似回線クラスの使用」（P.4-21）に記載されているステップに進みます。

疑似回線クラスの使用

ATM ポリシーで使用される疑似回線クラスを指定するには、次の手順を実行します。

ステップ 1　疑似回線クラスの選択をイネーブルにするには、[Use PseudoWireClass] チェックボックスをオンにします。

デフォルトでは、この属性はオフです。

使用方法に関する注釈：

- 疑似回線クラス名は、IOS XR での **pw-class** コマンドのプロビジョニングに使用されます。IOS XR デバイスの疑似回線クラス サポートに関する追加情報については、「疑似回線クラスの作成および変更」（P.3-16）を参照してください。
- [Use PseudoWireClass] をオンにすると、追加の属性 [PseudoWireClass] が GUI に表示されます。Prime Provisioning で以前に作成した疑似回線クラスを選択するには、[Edit] ボタンをクリックします。
- [Use PseudoWireClass] は、IOS デバイスのみに適用できます。

ステップ 2　[Next] をクリックします。

[Policy Editor] ウィンドウが表示されます。

ステップ 3　次の項である「ATM ポリシー ワークフローへのユーザ定義フィールドの追加」（P.4-22）に記載されているステップに進みます。

ATM ポリシー ワークフローへのユーザ定義フィールドの追加

[Additional Information] 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ができます。追加情報機能の使用方法の詳細については、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。

次の項である「テンプレートの関連付けのイネーブル化」（P.4-22）に記載されているステップに進みます。

テンプレートの関連付けのイネーブル化

Prime Provisioning テンプレート機能を使用すると、デバイスにフリーフォーマット CLI をダウンロードできます。テンプレートをイネーブルにする場合は、Prime Provisioning で現在サポートされていないコマンドをダウンロードするために、テンプレートとデータ ファイルを作成できます。

（注）　テンプレート変数のサポートは、ATM ポリシーおよびサービスで使用できます。ATM 関連の変数を含むテンプレートとデータ ファイルの例を使用できます。このテンプレートへのアクセスと使用方法についての詳細は、「ATM サービスでのテンプレート型変数の使用」（P.4-22）の項を参照してください。

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、（[Finish] をクリックする前に）[Policy Editor] ウィンドウで [Next] ボタンをクリックします。

[Policy Editor] ウィンドウが表示され、[Template Information] セクションが表示されます。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、「ポリシーでのテンプレートの使用」（P.9-22）を参照してください。

ステップ 2　ポリシー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 Information] ウィンドウで [Finish] をクリックして閉じ、[Policy Editor] ウィンドウに戻ります。

ステップ 3　ATM ポリシーを保存するには、[Finish] をクリックします。

ATM ポリシーに基づいてサービス要求を作成するには、「ATM サービス要求の管理」（P.4-26）を参照してください。

ATM サービスでのテンプレート型変数の使用

この項では、Prime Provisioning でサンプルの ATM テンプレートにアクセスして使用する方法について説明します。

ATM テンプレート例のデータ ファイルを作成するには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI で、[Service Design] > [Templates] > [Template Manager] を選択します。

[Template Manager] ウィンドウが表示されます。

ステップ 2　[Templates] ウィンドウでルート フォルダをクリックして展開します。

サブフォルダのリストが、最上部の [Examples] フォルダとともに表示されます。

ステップ 3　[Examples] フォルダをクリックしてフォルダを展開します。

ATM テンプレートを含む複数のサンプル テンプレートが表示されます。

ステップ 4　ATM フォルダをクリックして選択します。

ATM テンプレートは、テーブルの [Data File Name] カラムに、事前にロードされた ATMData データ ファイルとともに [Template] ウィンドウに表示されます。

ステップ 5　[Edit] ボタンをクリックして ATMData データ ファイルを編集するか、これをオフにして [Create Data File] をクリックし、新しいファイルを作成します。

いずれの場合も、[Data File Editor] ウィンドウが表示されます。このファイルを使用して、ATM サービスをプロビジョニングするために必要なテンプレート変数をマッピングできます。

ステップ 6　テンプレート変数に必要な変更を行った場合、[Save] をクリックして変更を保存します。

ステップ 7　[Close] をクリックして、[Data File Editor] ウィンドウを閉じます。

テンプレートを使用した ATM/IMA インターフェイスの作成

ATM/IMA インターフェイスは、プロビジョニングする必要があるデバイスで作成されます。これらのインターフェイスが以前に手動でデバイスに作成されていない場合、テンプレートを使用してデバイス コンソールで作成できます。ATM/IMA インターフェイスをデバイス コンソールを介してデバイスに作成したら、デバイスのコンフィギュレーションの収集タスクを実行する必要があります。コンフィギュレーションの収集後、Prime Provisioning インベントリ（リポジトリ）には、新しく作成された ATM/IMA インターフェイスからデータが取り込まれます。これらのインターフェイスは、ATM サービスのプロビジョニングに使用できるようになります。

テンプレートとデータ ファイルの作成およびデバイスへのダウンロード

（注）　次の手順は大まかに説明されており、Prime Provisioning でテンプレートとデータファイルを使用するための基本的な実務知識が必要です。テンプレートおよびデータ ファイルを作成するために必要な手順に関する詳細情報が必要な場合は、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

次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　[Template Manager] ツリーで、[Example] フォルダをクリックして展開します。

ステップ 3　次のように IMA テンプレートを作成し、保存します。

ステップ 4　[Create Template] ボタンをクリックして、IMA テンプレートを作成します。

[Template Editor] ウィンドウが表示されます。

ステップ 5　次を入力します。

- [Template Name]（必須）：たとえば、「IMA MWR 2941」など、任意の名前を選択します。
- [Description]（任意）。
- [Body]（必須）：組み込む必要のあるコンフィギュレーション テキスト、Velocity Template Language（VTL）ディレクティブ、および変数を入力します。次に例を示します。

```
controller $container $slot/$sub-slot
    clock source $option
    ima-group $ima
```

それぞれの説明は次のとおりです。

- **container** は **E1** または **T1** のいずれかの値に指定できるストリング タイプです。
- **slot** および **sub-slot** はそれぞれスロットとサブスロットを表します。
- **option** の値は、**internal** または **line** のいずれかの値に指定できるストリング タイプです。
- **ima** の値は、最小値が 0 で最大値が 23 の整数タイプの値です。

ステップ 6　[Save] をクリックして、テンプレートを保存します。

ステップ 7　前の手順で定義したように、該当する値を使用して適切なデータ ファイルを作成します。

この例では、デバイス コンソールを使用してデバイスを選択し、次のようにデータ ファイルを指定します。

ステップ 8　[Inventory] > [Device Tools] > [Device Console] を選択します。

[Choose Operation] ウィンドウが表示されます。

ステップ 9　[Download Template] を選択し、[Next] をクリックします。

[Download Template] ウィンドウが表示されます。

ステップ 10　デバイスを追加するには、[Add] をクリックします。

ステップ 11　表示される [Device Selection] ウィンドウで、選択する各デバイスのチェックボックスをオンにします。

ステップ 12　[Select] をクリックします。

追加されたデバイスが表示された [Download Template] ウィンドウに戻ります。

ステップ 13　[Next] をクリックします。

ウィンドウが更新され、デバイス グループを追加できるようになります。

ステップ 14　[Next] をクリックします。

ウィンドウが更新され、ダウンロードするテンプレートを選択できるようになります。

ステップ 15　[Select] ボタンをクリックします。

[Add/Remove Template] ウィンドウが表示されます。

ステップ 16　[Add] をクリックしてテンプレートを追加するか、[Remove] をクリックしてテンプレートを削除します。

[Add] をクリックすると、ツリー形式のテンプレート選択肢を含む [Template Datafile Chooser] ウィンドウが表示されます。ツリー内のフォルダとサブフォルダをナビゲートして、前に作成した ATM/IMA テンプレートを探します。

ステップ 17　必要なテンプレートを選択した後、[OK] をクリックします。

ステップ 18　前に作成したデータ ファイルを選択し、[Accept] をクリックします。

更新された情報が表示されている [Download Template] ウィンドウに戻ります。

ステップ 19　[Next] をクリックします。

[Template Summary] セクションがウィンドウに表示されます。

ステップ 20　[Upload Config After Download] と [Retrieve device attributes] のチェックボックスをオンにします。

これらのチェックボックスをオンにすると、テンプレートのダウンロードが送信されたときに、デバイスでコンフィギュレーションの収集が実行されます。これにより、Prime Provisioning のインベントリとリポジトリで、テンプレートが追加されたデバイスの設定が更新されます。

（注）　また、次の項「インベントリへの ATM/IMA インターフェイスの追加」（P.4-25）で説明されているように、収集を個別のタスクとして実行することもできます。

ステップ 21　[Finish] をクリックして、ダウンロードを実行します。

ステータスが示されたメッセージが表示されます。

ステップ 22　[Done] をクリックします。

インベントリへの ATM/IMA インターフェイスの追加

デバイスに対して別個にコンフィギュレーションの収集タスクを実行して、テンプレートを使用して以前にダウンロードした ATM/IMA インターフェイスからインベントリにデータを取り込むことができます。この項では、ネットワーク内の物理デバイスに接続して、デバイス情報を収集し、リポジトリにデータを取り込む方法について説明します。

次のステップを実行します。

ステップ 1　[Operate] > [Tasks] > [Task Manager] を選択します。

[Choose Operation] 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。

ステップ 3　[Collect Config] を選択します。

[Create Task] ウィンドウが表示されます。

ヒント　このタスクのデフォルトの [Name] と [Description] を変更する場合は、タスク ログでより簡単に特定することができます。

ステップ 4　[Next] をクリックします。

[Collect Config Task] ウィンドウが表示されます。

ステップ 5　タスクに関連付けられたデバイスを選択するには、[Devices] パネルで [Select] をクリックします。

[Select Device] ウィンドウが表示されます。

ステップ 6　目的のデバイスをオンにして選択し、[Select] をクリックします。

[Collect Config Task] ウィンドウが再表示されます。

ステップ 7　タスクに関連付けられたデバイス グループを選択するには、[Groups] パネルで [Select] をクリックします。

利用可能なデバイス グループのリストが表示されます。

ステップ 8　目的のデバイス グループをオンにして選択し、[Select] をクリックします。

[Collect Config Task] ウィンドウが再表示されます。

ステップ 9　必要であれば、スケジュールとタスクの所有者を設定します。

ステップ 10　[Submit] をクリックします。

[Tasks] ウィンドウが表示されます。

ステップ 11　[Task Name] カラムでタスクを選択し、[Details] をクリックして詳細情報を表示します。

コンフィギュレーション収集タスクの結果、以前にデバイスにダウンロードされたテンプレートを使用して作成された ATM/IMA インターフェイスが、Prime Provisioning インベントリおよびリポジトリのデバイス設定で更新されます。

ATM サービス要求の管理

この項では、RAN バックホール サービスをサポートする ATM サービス要求の管理に関連するワークフローのさまざまなタスクについて説明します。次の事項について説明します。

- 「ATM サービス要求の作成」（P.4-26）
- 「サービス要求の詳細の設定」（P.4-27）
- 「MCPT タイマー値の設定」（P.4-28）
- 「デバイスの選択」（P.4-29）
- 「ATM サービス要求の変更」（P.4-31）
- 「ATM 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」（P.4-32）
- 「ATM サービス要求の作成」（P.4-26）

ATM サービス要求の作成

ATM サービス要求の作成を開始するには、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。

ステップ 2　[Create] 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 3　[Policy] ドロップダウン リストを使用して、以前に作成したポリシーから ATM ポリシーを選択します（「ATM ポリシーの作成」（P.4-19）を参照）。これは、ポリシー名に EVC が続くことからわかるように、タイプ EVC のポリシーになります。

[EVC Service Request Editor] ウィンドウが表示されます。これは、サービス要求の属性を追加または変更できるワークフローの初期ウィンドウです。新しいサービス要求は、すべての編集可能な機能と編集不可能な機能および事前設定されたパラメータなど、選択したポリシーのプロパティをすべて継承します。

このウィンドウ内の属性は、接続回線間の疑似回線接続を表します。疑似回線接続によって、X Connect（つまり、クロスコネクト）を使用して 2 つのカスタマー サイト間のポイントツーポイント接続を作成することができます。

ステップ 4　次の項である「サービス要求の詳細の設定」（P.4-27）に記載されているステップに進みます。

サービス要求の詳細の設定

[Service Request Details] セクションに属性を設定するには、次の手順を実行します。

（注）　[Job ID] フィールドと [SR ID] フィールドは読み取り専用です。初めてサービス要求を作成する場合は、フィールドには値 [NEW] が表示されます。既存のサービス要求を変更する場合、フィールドの値は、Prime Provisioning データベースがサービス要求の編集フロー内に保持するそれぞれの ID を示します。

（注）　[Policy Name] フィールドは読み取り専用です。サービス要求の元になっているポリシーの名前が表示されます。読み取り専用のポリシー名をクリックすると、ポリシー内で設定されているすべての属性値のリストが表示されます。

ステップ 1　Prime Provisioning に VC ID を選択させる場合は、[AutoPick VC ID] 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しない場合は、次のステップで説明されているように、[VC ID] フィールドで ID を指定するよう求めるプロンプトが表示されます。

[AutoPick VC ID] をオンにすると、Prime Provisioning は、Prime Provisioning によって管理される VC ID リソース プールから疑似回線用に VC ID を割り当てます。この場合は、[VC ID] オプションのテキスト フィールドは編集不可能です。

ステップ 2　[AutoPick VC ID] をオフにした場合は、[VC ID] フィールドに VC ID を入力します。

使用方法に関する注釈：

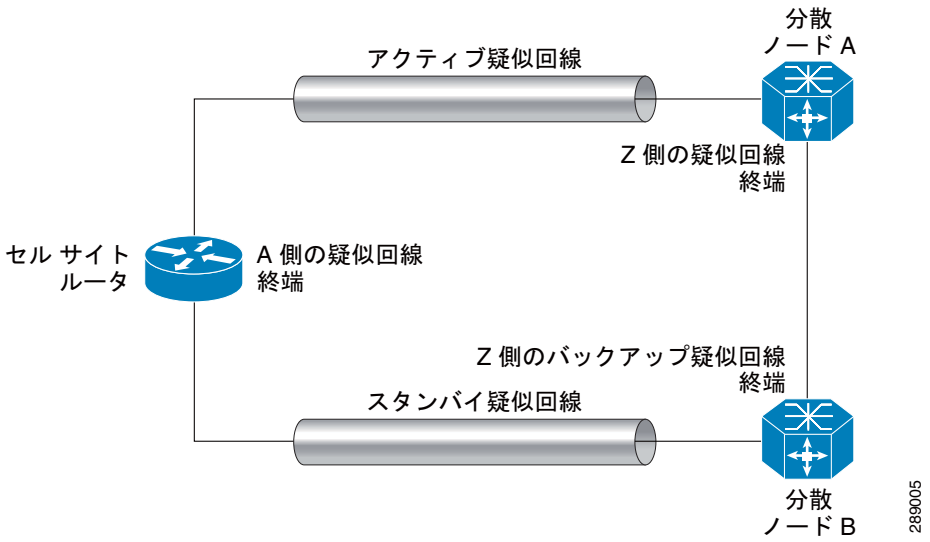
- [VC ID] 値は、VC ID に対応する整数値でなければなりません。
- VC ID を手動で割り当てると、Prime Provisioning は VC ID を調べて、Prime Provisioning の VC ID プール内にそれがあるかどうかを確認します。VC ID がプール内にあっても割り当てられていない場合は、VC ID はサービス要求に割り当てられます。VC ID がプール内にあって、すでに使用中の場合は、Prime Provisioning は別の VC ID を割り当てるよう求めるプロンプトを表示します。VC ID が Prime Provisioning VC ID プールの外にある場合は、Prime Provisioning は、VC ID が割り当てられているかどうかに関する検査を実行しません。オペレータは、VC ID が使用可能であることを確認する必要があります。
- VC ID は、サービス要求の作成中に限り入力できます。サービス要求の編集中は、[VC ID] フィールドは編集不可能です。

ステップ 3　特定の条件下で疑似回線の冗長性（代替の終端デバイス）をイネーブルにするには、[PseudoWire Redundancy] 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：

- [PseudoWire Redundancy] がオフの場合、疑似回線の冗長性はサービス要求でプロビジョニングされません。したがって、サービスに対して有効に機能するデバイスは 2 つのみになります。設定例については、図 4-6 を参照してください。一方のデバイスは、疑似回線の「A」側にあり、もう一方は疑似回線の「Z」側にあります。この場合、バックアップ PW VC ID **を入力できません。**

図 4-6　疑似回線終端の例



- [Pseudowire Redundancy] チェックボックスをオンにすると、サービスに有効に機能するデバイスは 3 台になります。一方のデバイスは、疑似回線の「A」側にあり、もう一方のデバイスは「Z」側にあります。この場合、バックアップ PW VC ID 属性を使用して「Z」側のバックアップ疑似回線を設定できます。
- このオプションの使用方法に関する注釈については、付録 C「2 台の N-PE 上でのアクセス リングの終端」、および特に「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）を参照してください。

ステップ 4　設定に問題がなければ、[Backup PW VC ID] フィールドにバックアップ疑似回線の VC ID を入力します。

バックアップ VC ID の動作は、プライマリ疑似回線の VC ID の動作と同じです。

ステップ 5　次の項である「MCPT タイマー値の設定」（P.4-28）に記載されているステップに進みます。

MCPT タイマー値の設定

[EVC Service Request Editor] ウィンドウの [Setting MCPT Timer Values] セクションを使用して、マルティーニのセル パッキング タイマーの値を設定することができます。MCPT タイマーは相手先固定接続（PVC）または相手先固定パス（PVP）に接続できます。パッキング可能なセルの最大数に達する前に、関連付けられている MCPT タイマーが終了した場合、そのパケットはそれまでにパッキングされたセル数で送信されます。MCPT タイマーは ATM サービスで使用されるデバイスに対してリンク属性を設定するときに指定します。

次のステップを実行します。

ステップ 1　MCPT タイマーに適切な値を入力します。

- [MCPT Timer 1]：500 ～ 10000 マイクロ秒の任意の値を設定します。
- [MCPT Timer 2]：1000 ～ 10000 マイクロ秒の任意の値を設定します。
- [MCPT Timer 3]：1500 ～ 10000 マイクロ秒の任意の値を設定します。

ステップ 2　次の項である「デバイスの選択」（P.4-29）に記載されているステップに進みます。

デバイスの選択

[EVC Service Request Editor] ウィンドウの [Devices] セクションを使用して、N-PE へのリンクを設定することができます。Prime Provisioning では、回線エミュレーション プロビジョニング用に追加されたデバイスは、N-PE ロール ベースのデバイスと見なされます。ATM デバイスを選択した後、各 ATM または ATM/IMA インターフェイスは [Interface] ドロップダウン リストで入力されます。

図 4-6 に示されている設定例は、ここでも使用されます。

次のステップを実行します。

ステップ 1　[Select Device] リンクをクリックして、疑似回線終端ポイントの「A」側を選択します。

[Select PE Device] ウィンドウが表示されます。

ステップ 2　適切なデバイスを選択し、[Save] をクリックします。

ステップ 3　[Interfaces] カラムで、デバイスのドロップダウン リストから目的のインターフェイスを選択します。

使用方法に関する注釈：

- 「A」側の終端ポイントのドロップダウン リストに表示されるインターフェイスは、ATM または ATM/IMA インターフェイスです。

ステップ 4　「A」側の終端装置のインターフェイスを選択したら、[Link Attributes] カラムの [Edit] リンクをクリックしてインターフェイス属性を設定します。

[ATM UNI Details] ウィンドウが表示されます。ここに、インターフェイス属性のリストが表示されます。

ステップ 5　「A」側のターミナル デバイスのインターフェイス属性を設定します。

（注）　ウィンドウ内の属性は、[Transport Mode] 属性の値が VP（PVP サービス）または VC（PVC サービス）のどちらに設定されているかによって動的に変わります。設定に応じて、次の該当するサブステップを参照してください。

a. 「A」側の終端が PVP サービスである場合、次の属性がウィンドウに表示されます。

- [Transport Mode]：PVP 転送タイプ。この場合、VP はドロップダウン リストに表示されます。
- [ATM VPI]：仮想パス識別子。0 ～ 255 の数字。
- [Maximum no. of cells to be packed]：パケットにパックされる（セルパッキング）セルの最大数。2 ～ 28 の数字。
- [Use MCPT Timer]：使用する MCPT タイマーの数。1、2、または 3。
- [Use PseudoWireClass]：サービス要求に既存の疑似回線クラスを関連付けるには、このチェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、疑似回線クラスを選択できます。サービス要求から疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。
- [Use Backup PseudoWireClass]：（この属性は [Pseudowire Redundancy] 属性がオンになっている場合にのみ使用できます）。既存の疑似回線クラスをバックアップ疑似回線クラスとしてサービス要求に関連付けるには、チェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、バックアップ疑似回線クラスを選択できます。サービス要求から

疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。この機能は、サービス要求ウィンドウの [Pseudowire Class] での選択と似ています。[Use Backup PseudowireClass] 属性は「A」ターミナルにのみ適用できます。「Z」および「Z - バックアップ」ターミナルには適用できません。

b. 「A」側の終端が PVC サービスである場合、次の属性がウィンドウに表示されます。

- [Transport Mode] : PVC 転送タイプ。この場合、VC はドロップダウン リストに表示されます。
- [Sub-Interface #] : 指定された ATM SPA の所定のポートに、指定されたポイントツーポイントのサブインターフェイスを作成します。サブインターフェイスの範囲は 1 ～ 2147483647 です。
- [ATM VPI] : 仮想パス識別子。0 ～ 255 の数字。
- [ATM VCI] : 仮想回線 ID。1 ～ 65535 の数字。
- [Maximum no. of cells to be packed] : パケットにパックされる（セルパッキング）セルの最大数。2 ～ 28 の数字。
- [Use MCPT Timer] : 使用する MCPT タイマーの数。1、2、または 3。
- [Use PseudoWireClass] : サービス要求に既存の疑似回線クラスを関連付けるには、このチェックボックスをオンにします。GUI に表示される [Select] ボタンを使用して、疑似回線クラスを選択できます。サービス要求から疑似回線クラスの関連付けを解除するには、このチェックボックスをオフにします。

ステップ 6　「A」ターミナル デバイスのインターフェイスに属性を設定した後、[OK] をクリックします。

[EVC Service Request Editor] ウィンドウが再表示されます。

ステップ 7　「A」ターミナル デバイスに対して実行した手順と同じ手順に従って、「Z」を選択し、該当する場合は「Z - バックアップ」ターミナル デバイスを選択して、それらのインターフェイスを設定します。

使用方法に関する注釈：

- ATM インターフェイスが、「Z」および「Z - バックアップ」ターミナル デバイスの [Interface] ドロップダウン リストに組み込まれます。
- [Pseudowire Redundancy] チェックボックスが（前にワークフローで）[EVC Service Request Editor] ウィンドウでオンになっている場合、「A」および「Z」ターミナル デバイスに対してリンク属性が設定されているときは、「Z - バックアップ」ノードを選択して設定できます。
- 「A」ターミナル デバイスの場合と同様に、「Z」および「Z - バックアップ」ターミナル デバイスのインターフェイス属性は、ATM サービスのタイプ（PVP または PVC）によって異なります。

ステップ 8　これらのターミナル デバイスのインターフェイスを選択したら、[Link Attributes] カラムの [Edit] リンクをクリックしてインターフェイス属性を設定します。

ステップ 9　必要であれば、[Swap Terminals] ドロップダウン リストを使用して、ターミナルに関連するデバイスの順序を変更します。

この選択は、設定に基づきます。

- Swap A - Z
- Swap A - Z Backup
- Swap Z- Z Backup

スワップ操作を実行するためのオプションの 1 つを選択します。デバイスは、選択内容に基づいて [Select Devices] カラムで並べ替えられます。

使用方法に関する注釈：

- [Swap Terminals] ボタンは、サービス要求を最初に作成する場合にのみ表示されます。後でサービス要求を編集する場合、このボタンは表示されず、その時点でスワップ操作を実行することはできません。
- [Swap A - Z Backup] および [Swap Z - Z Backup] オプションは、[Pseudowire Redundancy] 属性がオンになっている場合にのみ使用できます。
- デバイスとターミナルがスワップされる場合、インターフェイスを [Interfaces] カラムでリセットする必要があります。

ステップ 10　インターフェイス属性を設定してから、[OK] をクリックします。

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

ステップ 11　[EVC Service Request Editor] ウィンドウで属性の設定が完了したら、ウィンドウの下部にある [Save] ボタンをクリックして、設定を保存し、ATM サービス要求を作成します。

属性が欠落しているか、設定が間違っている場合、Prime Provisioning に警告が表示されます。（Prime Provisioning によって提供される情報に基づいて）必要な修正または更新を行って、[Save] ボタンをクリックします。

EVC サービス要求の変更については、「ATM サービス要求の変更」（P.4-31）の項を参照してください。ATM サービス要求の保存に関する追加情報については、「ATM サービス要求の保存」（P.4-32）を参照してください。

ATM サービス要求の変更

リンクまたはサービス要求の他の設定を変更する必要がある場合は、ATM サービス要求を変更できます。

サービス要求を変更するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

[Service Request Manager] ウィンドウが表示され、Prime Provisioning で使用可能なサービス要求が示されます。

ステップ 2　サービス要求のチェックボックスをオンにします。

ステップ 3　[Edit] をクリックします。

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

ステップ 4　必要に応じて、属性を変更します。

ステップ 5　テンプレートまたはデータ ファイルを接続回線に追加するには、「ATM 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」（P.4-32）の項を参照してください。

ステップ 6　ATM サービス要求の編集が終了したら、[Save] をクリックします。

ATM サービス要求の保存に関する追加情報については、「ATM サービス要求の保存」（P.4-32）を参照してください。

ATM 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

Prime Provisioning では、アプリケーションによって管理されるデバイスで使用可能なすべての CLI コマンドの設定はサポートされません。そのようなコマンドをデバイス上で設定するために、Prime Provisioning Template Manager 機能を使用できます。テンプレートは、デバイス ロール単位でポリシー レベルで関連付けることができます。サービス要求レベルでのテンプレートの上書きは、ポリシーレベルの設定でオペレータに許可されている場合は行うことができます。

サービス要求でテンプレートとデータ ファイルを関連付けるには、[Service Request Editor] ウィンドウで任意のリンクを選択して、ウィンドウの下部にある [Template] ボタンをクリックします。

（注）　関連付けられたポリシーでテンプレート機能が使用可能になっていない場合は、[Template] ボタンは選択できません。

[SR Template Association] ウィンドウが表示されます。このウィンドウでは、デバイス単位レベルでテンプレートを関連付けることができます。[SR Template Association] ウィンドウには、リンクを構成するデバイス、デバイス ロール、およびデバイスに関連付けられているテンプレートとデータ ファイルが一覧表示されます。この場合は、テンプレートまたはデータ ファイルはまだ設定されていません。

テンプレートとデータ ファイルをサービス要求に関連付ける方法の詳細については、「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。

ATM サービス要求の保存

ATM サービス要求を保存するには、次の手順を実行します。

ステップ 1　サービス要求の属性の設定が終了したら、[Save] をクリックして、サービス要求を作成します。

サービス要求の作成が正常に完了すると、[Service Request Manager] ウィンドウが表示されます。新しく作成された ATM サービス要求が [REQUESTED] の状態で追加されます。

ただし、何らかの理由で（たとえば、選択した値が範囲外である）サービス要求の作成が失敗した場合は、エラー メッセージで警告されます。そのような場合は、エラーを修正して、サービス要求を再度保存する必要があります。

ステップ 2　ATM サービス要求を展開する準備ができたら、「サービス要求の展開」（P.8-10）を参照してください。

ATM サービスのサンプル コンフィグレットについては、「RAN バックホール サービスのサンプル コンフィグレット」（P.4-33）を参照してください。

RAN バックホール サービスのサンプル コンフィグレット

この項では、Prime Provisioning での RAN バックホール サービス 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ます。具体的な内容は、次のとおりです。

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）　太字で示してある CLI が最も関連するコマンドです。

SAToP PW3 を使用した CEM TDM

設定

- サービス：RAN バックホール。
- 機能 : この項では、セル サイト ルータと 2 つの分配ノード（A および B）での CEM TDM SAToP PW3 サービス用に生成されるサンプル コンフィグレットについて説明します。
- デバイス設定 :
  - セル サイト ルータは、IOS イメージを持つ MWR 2941-DC ルータです。

    コントローラ：E1 0/0

    インターフェイス：CEM 0/0
  - 分散ノード A は IOS イメージを持つ 760X シリーズ デバイスです。

    コントローラ：SONET 3/0/0

    インターフェイス：CEM 3/0/0
  - 分散ノード B は IOS イメージを持つ 760X シリーズ デバイスです。

    コントローラ：SONET 3/0/0

    インターフェイス：CEM 3/0/0

コンフィグレット

セル サイト ルータ

```
pseudowire-class c76a3-1
 encapsulation mpls
!
pseudowire-class c76a3-2
 encapsulation mpls
!
controller E1 0/0
 clock source internal
 cem-group 0 unframed
!
interface CEM0/0
 no ip address
 cem 0
  xconnect 10.0.0.1 2090102001 pw-class c76a3-1
   backup peer 10.0.0.4 2090403001 pw-class c76a3-2
```

分散ノード A	分散ノード B

pseudowire-class c76a3-1
 encapsulation mpls
 preferred-path interface Tunnel211
!
controller SONET 3/0/0
 ais-shut
 framing sdh
 clock source line
 aug mapping au-4
 !
 au-4 1 tug-3 2
  mode c-12
 tug-2 1 e1 1 description m29a2-3(CEM0/0)
  tug-2 1 e1 1 cem-group 100 unframed
!
interface CEM3/0/0
 no ip address
 cem 100
  xconnect 10.0.0.1 2090102001 pw-class c76a3-1 sequencing both
	pseudowire-class c76a3-2
	 encapsulation mpls
	 preferred-path interface Tunnel340
	!
	controller SONET 3/0/0
	 ais-shut
	 framing sdh
	 clock source line
	 aug mapping au-4
	 !
	 au-4 1 tug-3 2
	  mode c-12
	 tug-2 1 e1 1 description m29a2-3(CEM0/0)
	  tug-2 1 e1 1 cem-group 100 unframed
	  tug-2 1 e1 1 framing unframed
	!
	interface CEM3/0/0
	 cem 100
	  xconnect 10.0.0.4 2090403001 pw-class c76a3-2 sequencing both

コメント

- なし。

CESoPSN を使用する CEM TDM

設定

- サービス：RAN バックホール。
- 機能：この項では、セル サイト ルータと 2 つの分散ノード（A および B）での CEM TDM CESoPSN サービス用に生成されるサンプル コンフィグレットについて説明します。
- デバイス設定：
  - セル サイト ルータは、IOS イメージを持つ MWR 2941-DC ルータです。

    コントローラ：E1 0/4

    インターフェイス：CEM 0/4
  - 分散ノード A は IOS イメージを持つ 760X シリーズ デバイスです。

    コントローラ：SONET 3/0/0

    インターフェイス：CEM 3/0/0
  - 分散ノード B は IOS イメージを持つ 760X シリーズ デバイスです。

    コントローラ：SONET 3/0/0

    インターフェイス：CEM 3/0/0

コンフィグレット

セル サイト ルータ

```
pseudowire-class c76a3-1
 encapsulation mpls
!
pseudowire-class c76a3-2
 encapsulation mpls
!
controller E1 0/4
 clock source internal
 cem-group 0 timeslots 1-7
!
interface CEM0/4
 cem 0
  xconnect 10.0.0.1 3090102001 pw-class c76a3-1
   backup peer 10.0.0.4 3090403001 pw-class c76a3-2
```

分散ノード A	分散ノード B

pseudowire-class c76a3-1
 encapsulation mpls
 preferred-path interface Tunnel211
!
controller SONET 3/0/0
 ais-shut
 framing sdh
 clock source line
 aug mapping au-4
 !
 au-4 1 tug-3 2
  mode c-12
 tug-2 2 e1 2 description m29a2-3(CEM0/4 cem 0)
  tug-2 2 e1 2 cem-group 104 timeslots 1-7
 !
 interface CEM3/0/0
  cem 104
  xconnect 10.0.0.1 3090102001 pw-class c76a3-1 sequencing both
	pseudowire-class c76a3-2
	 encapsulation mpls
	 preferred-path interface Tunnel340
	!
	controller SONET 3/0/0
	 ais-shut
	 framing sdh
	 clock source line
	 aug mapping au-4
	 !
	 au-4 1 tug-3 2
	  mode c-12
	tug-2 2 e1 2 description m29a2-3(CEM0/4 cem 0)
	  tug-2 2 e1 2 cem-group 104 timeslots 1-7
	!
	interface CEM3/0/0
	 cem 104
	  xconnect 10.0.0.4 3090403001 pw-class c76a3-2 sequencing both

コメント

- なし。

ATM/IMA PVP サービス

設定

- サービス：RAN バックホール。
- 機能：この項では、セル サイト ルータと 2 つの分散ノードでの ATM PVP サービス用に生成されるサンプル コンフィグレットについて説明します。
- デバイス設定：
  - セル サイト ルータは、IOS イメージを持つ MWR 2941-DC ルータです。

    コントローラ：E1 0/12、E1 0/13

    インターフェイス：ATM0/IMA2
  - 分散ノード A は IOS イメージを持つ 760X シリーズ デバイスです。

    インターフェイス：ATM 3/1/1
  - 分散ノード B は IOS イメージを持つ 760X シリーズ デバイスです。

    インターフェイス：ATM 3/1/1

コンフィグレット

セル サイト ルータ

```
pseudowire-class c76a3-1
 encapsulation mpls
!
pseudowire-class c76a3-2
 encapsulation mpls
!
controller E1 0/12
 framing NO-CRC4
 clock source internal
 ima-group 2 scrambling-payload
!
controller E1 0/13
 framing NO-CRC4
 clock source internal
 ima-group 2 scrambling-payload
!
interface ATM0/IMA2
 no ip address
 ima version 1.0
 ima group-id 2
 atm mcpt-timers 1000 5000 10000
 atm pvp 9 l2transport
  cell-packing 28 mcpt-timer 3
  xconnect 10.0.0.1 4090102003 pw-class c76a3-1
   backup peer 10.0.0.4 4090403003 pw-class c76a3-2
 no atm ilmi-keepalive
```

分散ノード Z	分散ノード Z のバックアップ

pseudowire-class c76a3-1
 encapsulation mpls
 preferred-path interface Tunnel211
!
interface ATM3/1/1
 no ip address
 atm mcpt-timers 1000 5000 10000
 atm pvp 9 l2transport
  cell-packing 28 mcpt-timer 3
  xconnect 10.0.0.1 4090102003 pw-class c76a3-1
 no atm enable-ilmi-trap
	pseudowire-class c76a3-2
	 encapsulation mpls
	 preferred-path interface Tunnel340
	!
	interface ATM3/1/1
	 no ip address
	 atm mcpt-timers 1000 5000 10000
	 atm pvp 9 l2transport
	  cell-packing 28 mcpt-timer 3
	  xconnect 10.0.0.4 4090403003 pw-class c76a3-2
	 no atm enable-ilmi-trap

コメント

- なし。

ATM/IMA VCC サービス

設定

- サービス：RAN バックホール。
- 機能：この項では、セル サイト ルータと 2 つの分散ノードでの ATM VCC サービス用に生成されるサンプル コンフィグレットについて説明します。
- デバイス設定：
  - セル サイト ルータは、IOS イメージを持つ MWR 2941-DC ルータです。

    コントローラ：E1 0/8、E1 0/9

    インターフェイス：ATM0/IMA0、ATM0/ IMA0
  - 分散ノード A は IOS イメージを持つ 760X シリーズ デバイスです。

    インターフェイス：ATM 3/1/0
  - 分散ノード B は IOS イメージを持つ 760X シリーズ デバイスです。

    インターフェイス：ATM 3/1/0

コンフィグレット

セル サイト ルータ

```
pseudowire-class c76a3-1
 encapsulation mpls
!
pseudowire-class c76a3-2
 encapsulation mpls
!
controller E1 0/8
 framing NO-CRC4
 clock source internal
 ima-group 0 scrambling-payload
!
controller E1 0/9
 framing NO-CRC4
 clock source internal
 ima-group 0 scrambling-payload
!
interface ATM0/IMA0
 ima version 1.0
 ima group-id 0
 atm mcpt-timers 1000 5000 10000
!
interface ATM0/IMA0.1 point-to-point
 snmp trap link-status
 pvc 9/34 l2transport
  cbr 255
  encapsulation aal0
  cell-packing 28 mcpt-timer 3
  xconnect 10.0.0.1 4090102001 pw-class c76a3-1
   backup peer 10.0.0.4 4090403001 pw-class c76a3-2
```

分散ノード Z	分散ノード Z のバックアップ

pseudowire-class c76a3-1
 encapsulation mpls
 preferred-path interface Tunnel211
!
interface ATM3/1/0
 atm mcpt-timers 1000 5000 10000
!
interface ATM3/1/0.9001 point-to-point
 description m29a2-3 - ATM0/IMA0
 no atm enable-ilmi-trap
 pvc 9/34 l2transport
  cell-packing 28 mcpt-timer 3
  encapsulation aal0
  xconnect 10.0.0.1 4090102001 pw-class c76a3-1
	pseudowire-class c76a3-2
	 encapsulation mpls
	 preferred-path interface Tunnel340
	!
	interface ATM3/1/0
	 atm mcpt-timers 1000 5000 10000
	!
	interface ATM3/1/0.9001 point-to-point
	 description m29a2-3 - ATM0/IMA0
	 no atm enable-ilmi-trap
	 pvc 9/34 l2transport
	  cell-packing 28 mcpt-timer 3
	  encapsulation aal0
	  xconnect 10.0.0.4 4090403001 pw-class c76a3-2

コメント

- なし。

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）、バーチャル 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

具体的な内容は、次のとおりです。

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

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。

a. [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。

b. [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 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 から出ることはできません（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 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と、この VPN を使用していて、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、MVRFCE 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。

a.　[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。

b.　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] 属性はディセーブルになります。

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。

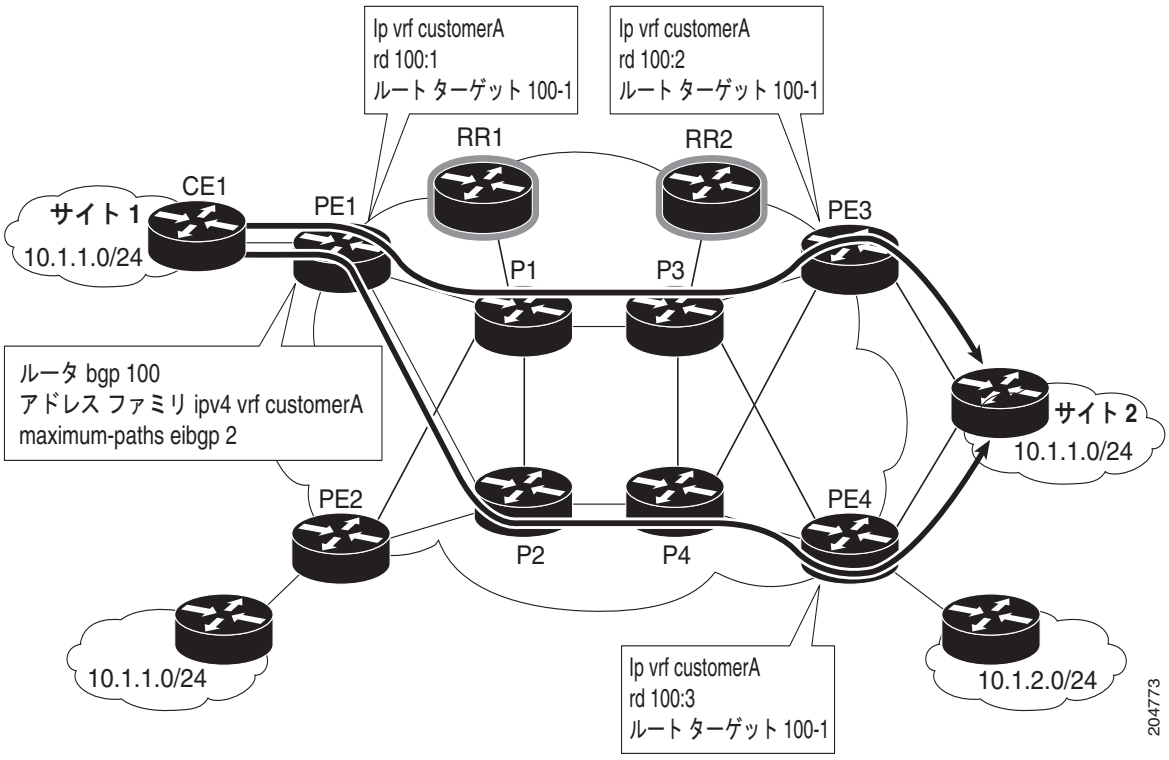
ステップ 3　固有 RD 割り当て機能が必要な場合は、[Unique Route Distinguisher] チェックボックスをオンにします。

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 *vrfName:RD* 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 *vrfName:RD* を使用します。
2	pe2	False	V24:33	Prime Provisioning は、デフォルトの *vrfName:RD* 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 *vrfName:RD* を作成します。この PE（pe3）では、この *vrfName:RD* は設定されていません。
4	pe3	True	V25:34	Prime Provisioning は SR #3 の *vrfName:RD* 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 *vrfName:RD* 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 *vrfName:RD* 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 *vrfName:RD* 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 *vrfName:RD* 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 *vrfName:RD* を使用します。これは、この PE に対する新規 *vrfName:RD* 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 *vrfName:RD* を使用します。これは、この PE に対する新規 *vrfName:RD* 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 *vrfName:RD* を使用します。これは、この PE に対する新規 *vrfName:RD* 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

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] 状態に移行します。

IP アドレシング 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と、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、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。

（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 VPF 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す。

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す。

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る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。

a. [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。

b. [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。

c. 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殊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

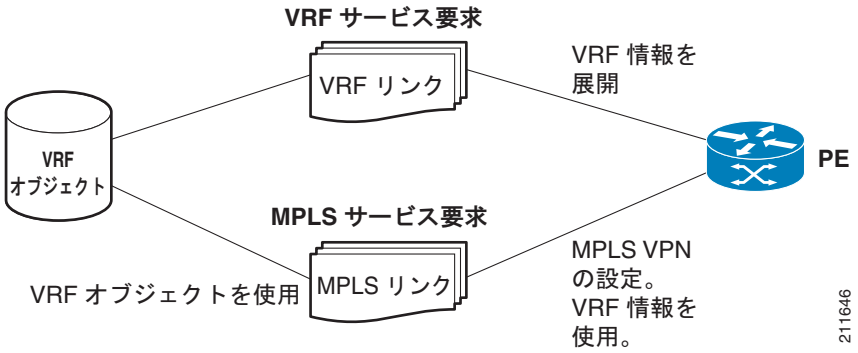
すでに展開された VRF オブジェクトは、MPLS VPN サービス要求およびサービス ポリシー内で使用できます。

（注）　独立 VRF の関連付けは、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。

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。
- MPL 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は削除しません。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します。

（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。

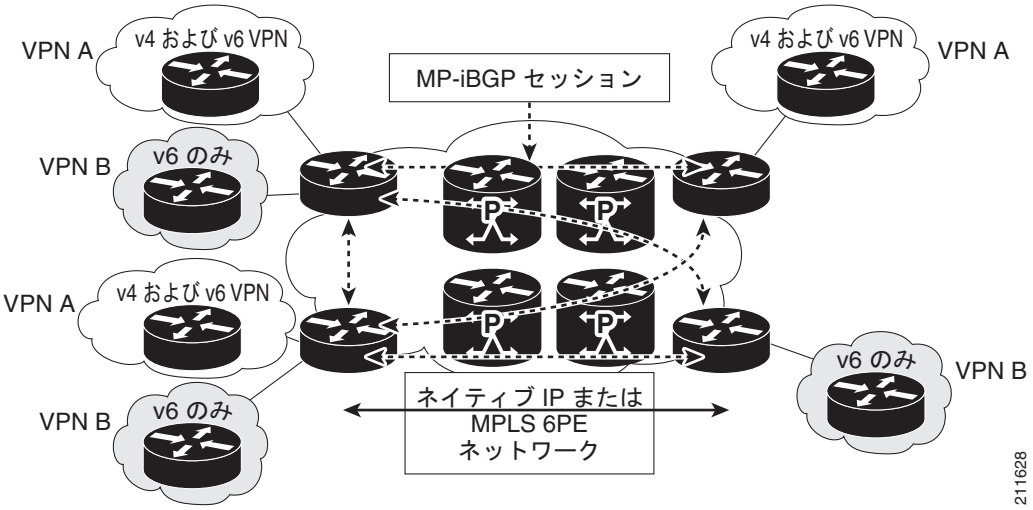
IPv6 VPN プロバイダー エッジ ルータ（6VPE）

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ズされます。

- 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、リポジトリ内に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 のアンナンバード方式は、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ンバード 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（MVRFCE; 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 ファイルの使用方法の詳細については、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。一部の場合、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
- MVRFCE 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 管理においての 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 管理においての 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 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 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 アンナンバード 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す。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。

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 プレフィックスブランチ オフィスにアドバタイズする代わりに、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 フィードがあるなど）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 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している必要があります。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。MVRFCE 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] オプションの使用方法を示すサンプル 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、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 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。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 ProvisioningPrime 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方法を示すサンプル 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ときに外部 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ッディングが発生し、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。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。

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]、[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

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. 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

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。

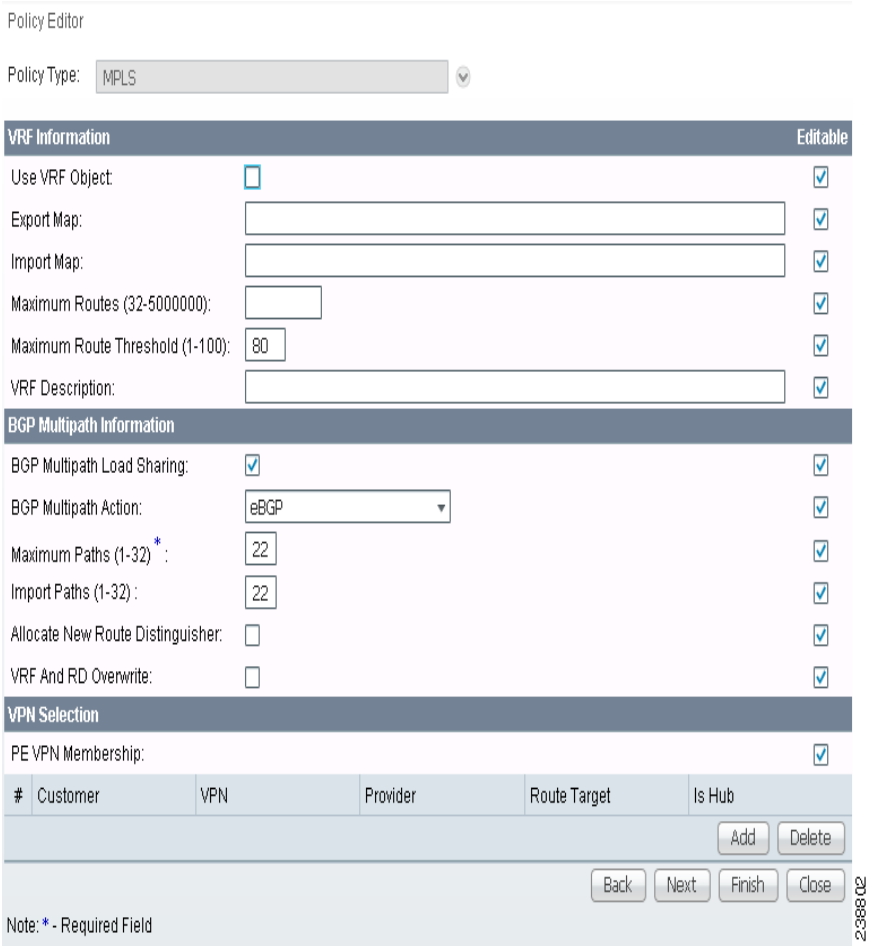
[MPLS Policy VRF and VPN Membership] ダイアログボックスが表示されます。続行するには、「VRF および VPN の情報の定義」（P.5-76）を参照してください。

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



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と、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 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。

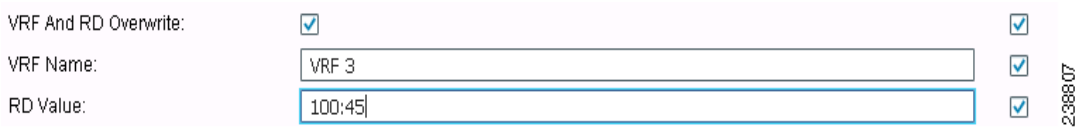
（注）　VPN の作成時に固有ルート識別子機能をイネーブルにした場合、[Allocate New Route Distinguisher] オプションはディセーブルです。詳細については、「VPN の固有ルート識別子のイネーブル化」（P.5-12）を参照してください。

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、絶対に必要な場合に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



a.　[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。

b.　[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] 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す。

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。この機能の使用方法の詳細については、「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。

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ときは、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

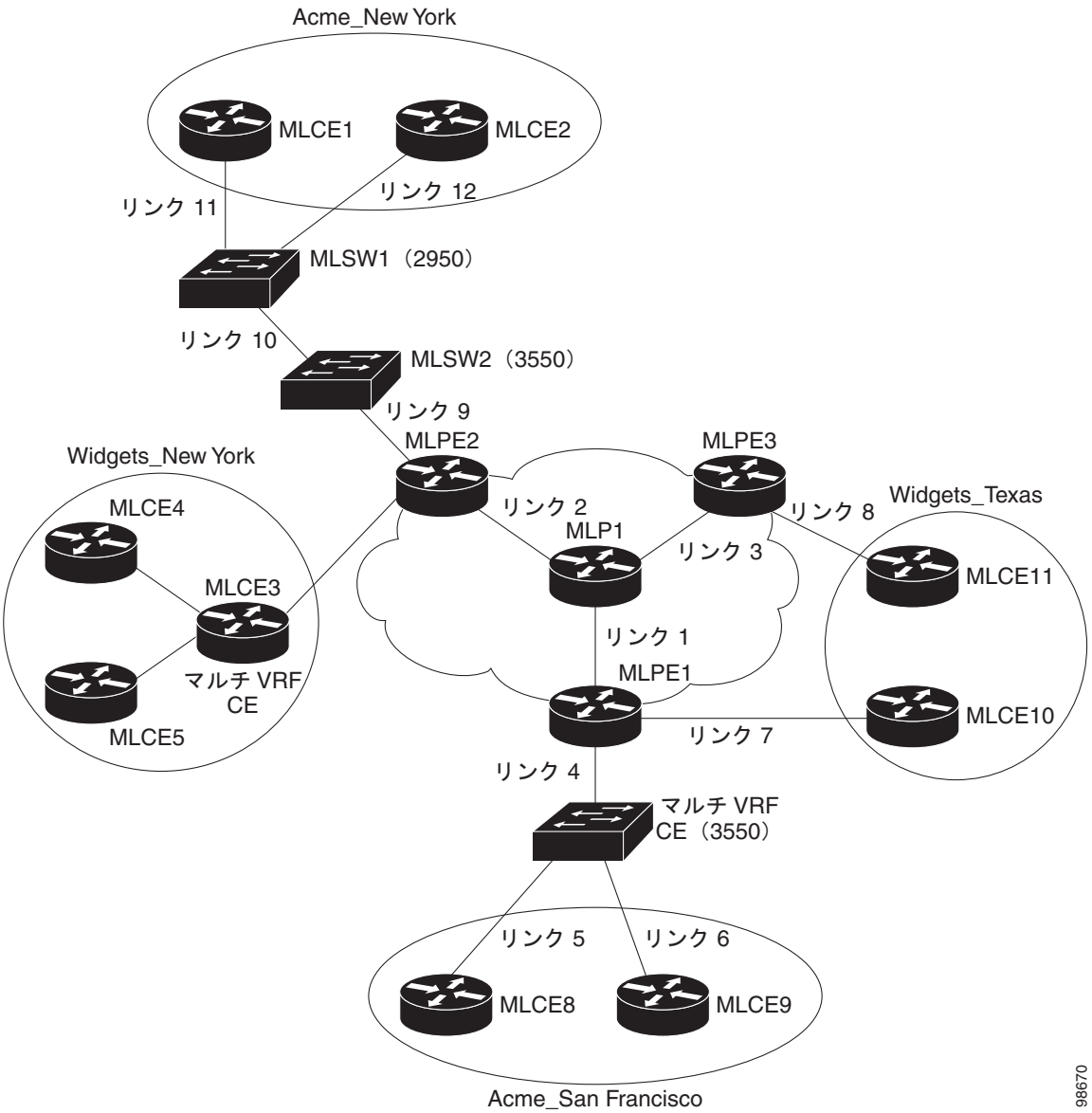
マルチ VRF の例では、サービス プロバイダーは、カスタマー サイト Widgets_NY（ニューヨーク）の CE（mlce4）とカスタマー サイト Widgets_NY（ニューヨーク）にあるマルチ VRFCE（mlce3）間に MPLS サービスを作成する必要があります。

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



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。

a. [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。

b. [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。

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 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/lnkbndl.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、MVRFCE 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。

a. [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 番めの 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、MVRFCE 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 番めの 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の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のあるすべての 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のあるルーティング 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のある 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 ターゲットのタギングを変更します。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 タギング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 上にないかどうかを確認し、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、MVRFCE 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ネーブル化」（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方法の例を示します。

```
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　デフォルトのままで、[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　デフォルトのままで、[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　デフォルトのままで、[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の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のあるすべての 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す。

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 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のあるルーティング プロトコル値があれば編集してます。

（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のある 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。

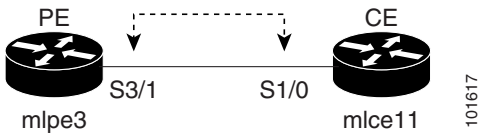
Prime Provisioning は、標準 PE-CE と MVRFCE PE-CE という、2 つの MPLS VPN サービス ポリシー タイプをサポートします。次のシナリオでは、標準 PE-CE ポリシー タイプに焦点を当てます。

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。

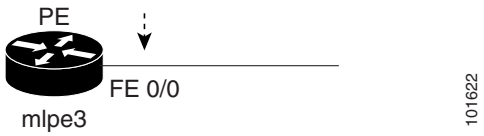
図 5-9　CE が存在する PE から CE へのリンク



[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

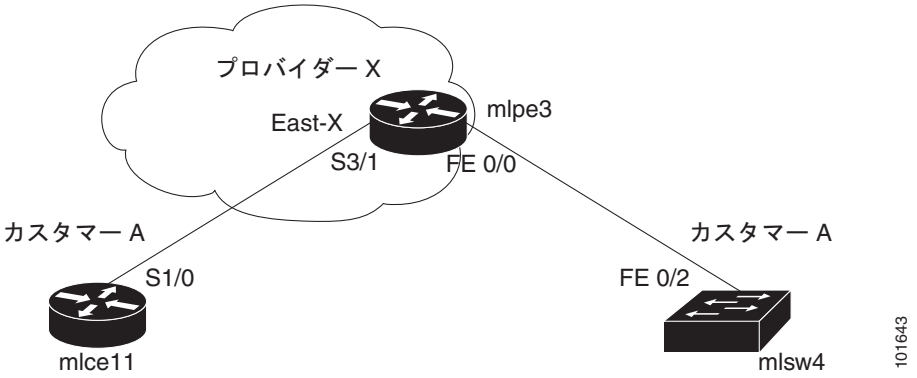


図 5-11 のネットワーク トポロジは、1 つのサービス プロバイダー（プロバイダー X）と 1 つのカスタマー（カスタマー A）のラボ環境を示しています。1 つのリージョン（East-X）と 1 つの PE（mlpe3.cisco.com）があります。各カスタマー デバイス（1 個の CE と 1 個の CLE）は、サイト（mlce11-Site および mlce4-Site）を表しています。

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

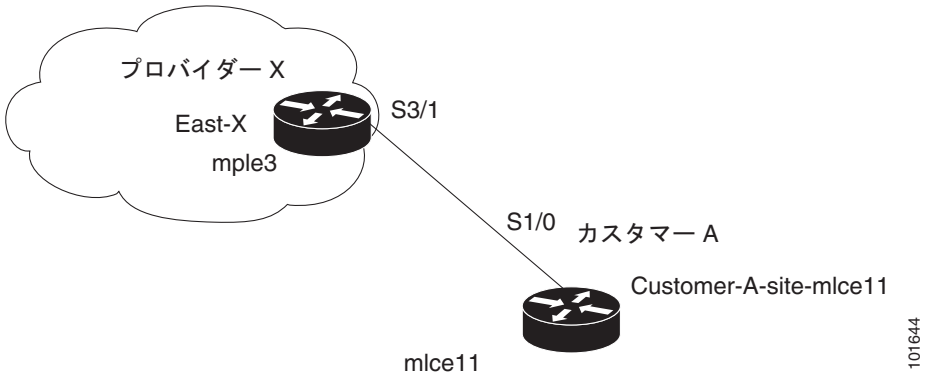
ここでは、次の項目について説明します。

- 「PE-CE サービス ポリシーの概要」（P.5-106）
- 「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）

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



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 番めの 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 番めの 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ることが示されます。

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。

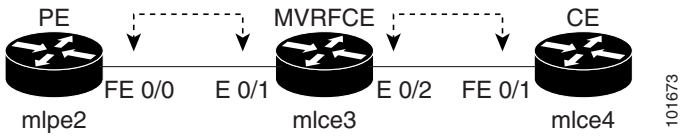
- PE
- マルチ VRF CE
- CE

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。

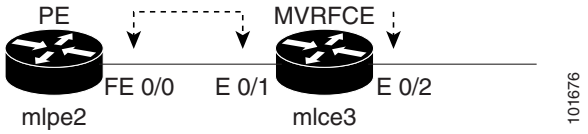
図 5-13　MVRFCE PE-CE リンク



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。

図 5-14　CE を使用しない MVRFCE PE-CE リンク



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

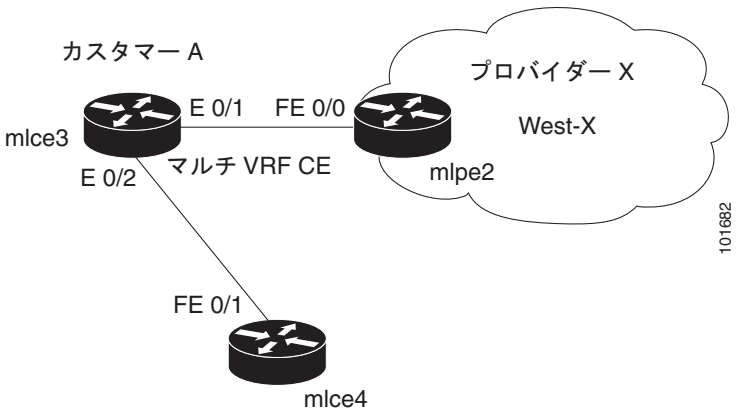


図 5-15 のネットワーク トポロジは、1 つのサービス プロバイダー（プロバイダー X）と 1 つのカスタマー（カスタマー A）のラボ環境を示しています。1 つのリージョン（West-X）と 1 つの PE（mlpe2.cisco.com）があります。各カスタマー デバイス（1 個の MVRFCE と 1 個の CE）は、サイト（mlce3-Site および mlce4-Site）を表しています。

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。

MVRFCE-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 MVRFCE 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

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

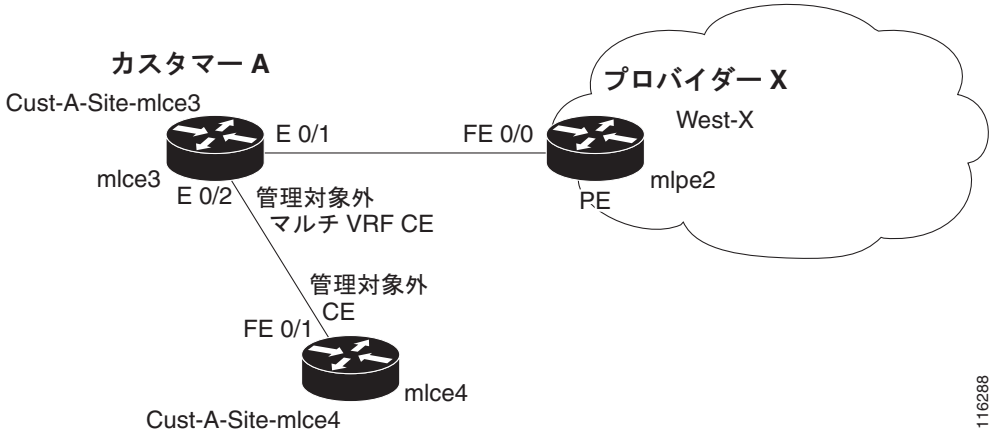


図 5-16 のネットワーク トポロジは、サービス プロバイダー（**プロバイダー X**）と 1 人のカスタマー（**カスタマー A**）を示しています。プロバイダーには、1 つのリージョン（**West-X**）と 1 個の PE（**mlpe2**）が含まれています。カスタマーには、1 個の MVRFCE（**mlce3**）と 1 個の CE（**mlce4**）が含まれています。これらの CPE は両方とも管理対象外です。

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。

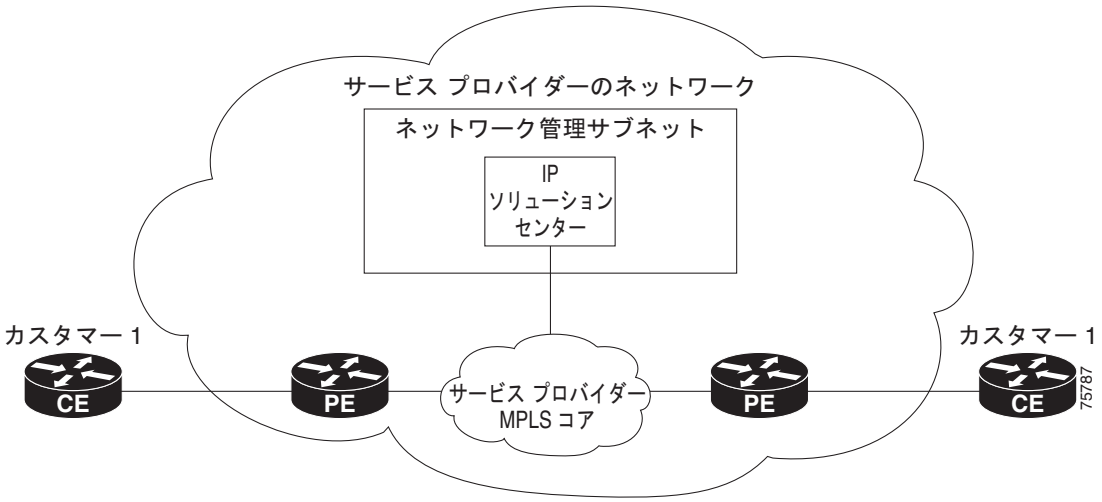
管理対象外のカスタマー エッジ ルータ

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、ルータに自動的には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いため、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、プロバイダーとカスタマー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。

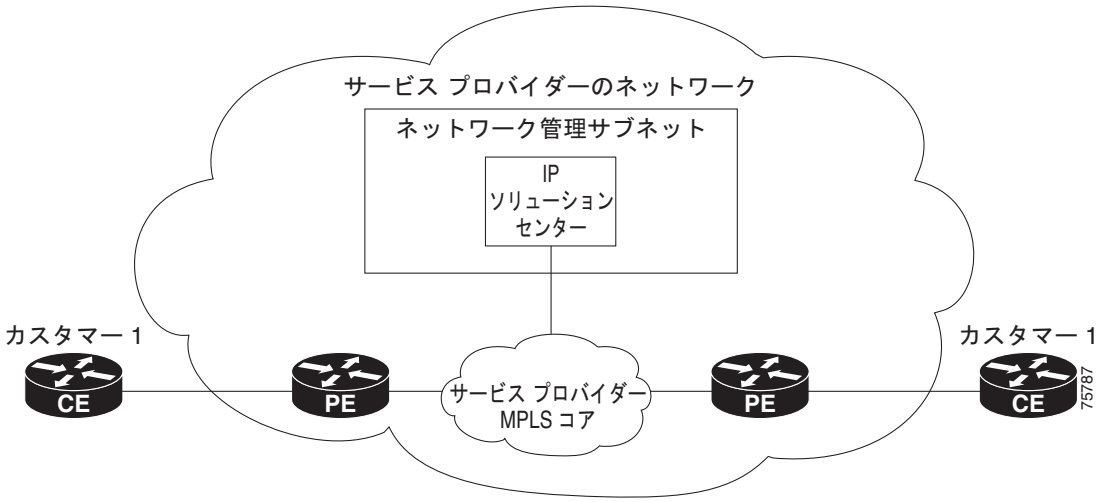
次の項では、管理対象 CE の環境を管理するために必要な概念と問題について説明します。

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 にアクセスできる必要があります。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 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

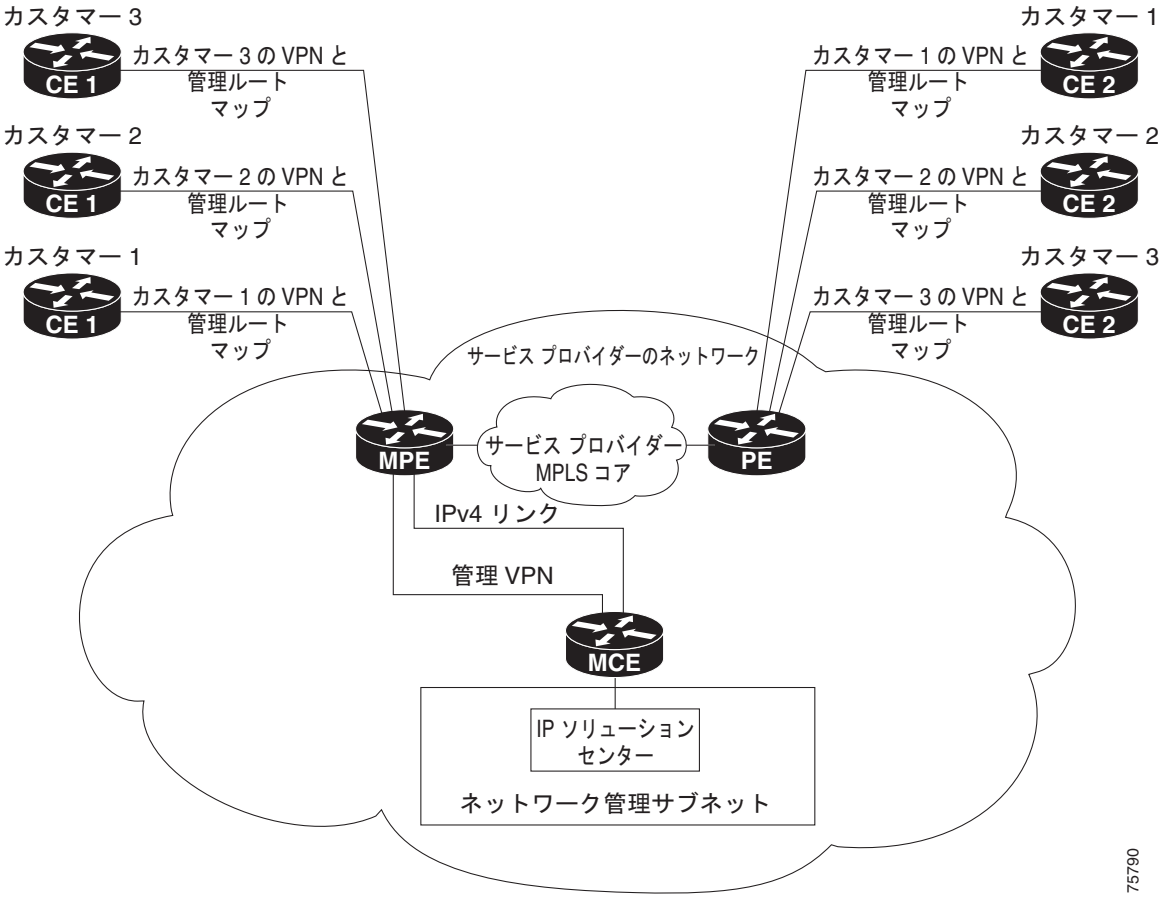
  アウトオブバンド手法では、MCE にネットワークのすべての CE への IPv4 接続（つまり、MPLS VPN 接続ではない）と PE があります（「アウトオブバンド手法」（P.5-132）を参照）。このため、*アウトオブバンド*ではプロバイダーの管理トラフィックを伝送する別個のリンクが PE 間に示されます。

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 リンクはパラレル 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



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 リンクはパラレル 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 の間に別のパラレル非 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。

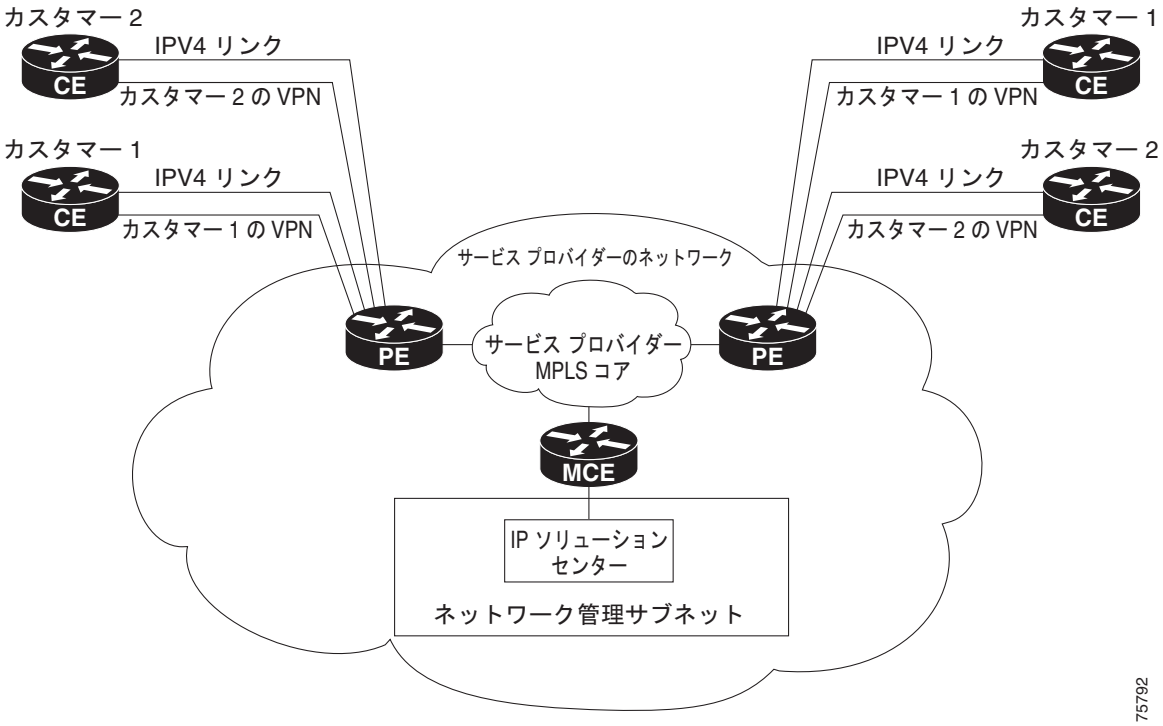
管理 VPN 手法を実装する利点は、次のとおりです。

- 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。

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。

a. [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。

b. [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。

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 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 番めの 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の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のあるすべての 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のあるルーティング 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のあるすべての 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ー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ーラブルで効率的な 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。

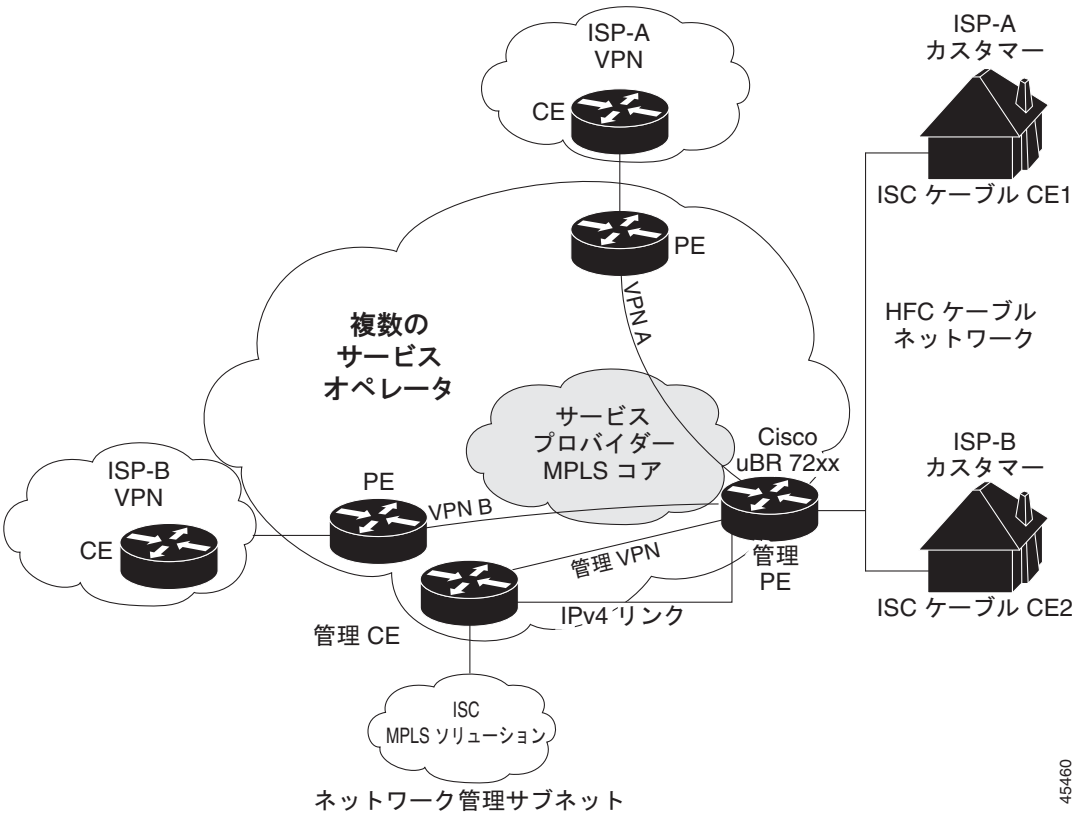
各 PE ルータは 1 つ以上の VRF テーブルを維持します。パケットが特定の VRF に関連付けられたインターフェイスから直接到着すると、PE は適切な VRF テーブルでパケットの IP 宛先アドレスを検索します。MPLS VPN は BGP と IP アドレス解決の組み合わせを使用してセキュリティを保証します。

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力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



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 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のあるすべての 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のあるルーティング 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のある 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の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のあるすべての 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のあるルーティング 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のある 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のある 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

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

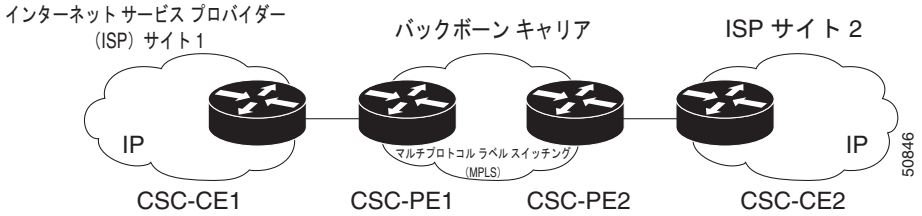
CSC サービスは、IOS XR デバイスでの BGP PE-CE ルーティング プロトコルに適用されます。

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　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。

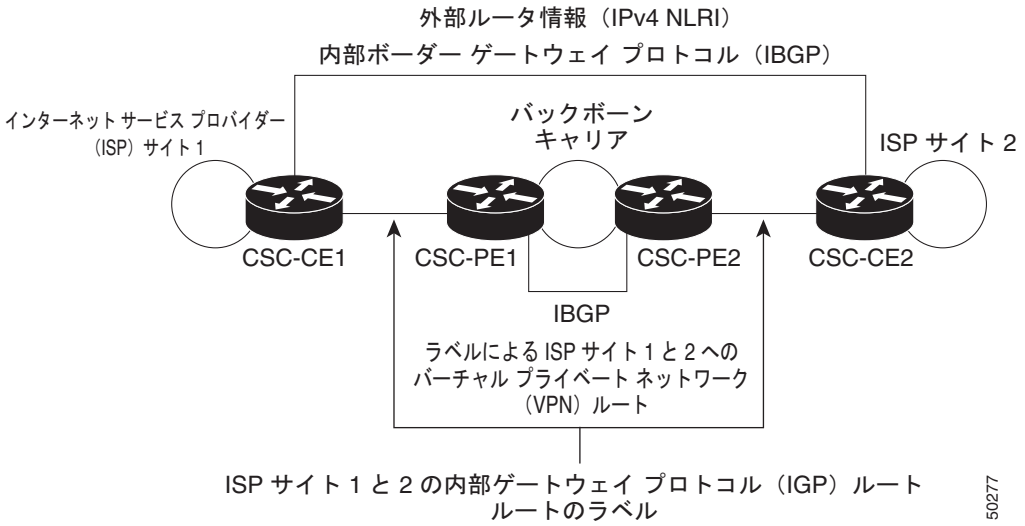
- 内部ルートは、ISP 内のいずれかのルータに進みます。
- 外部ルートはインターネットに進みます。

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が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 キャリアへのパケット転送を一貫した方法で行うことができます。MPLS により、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

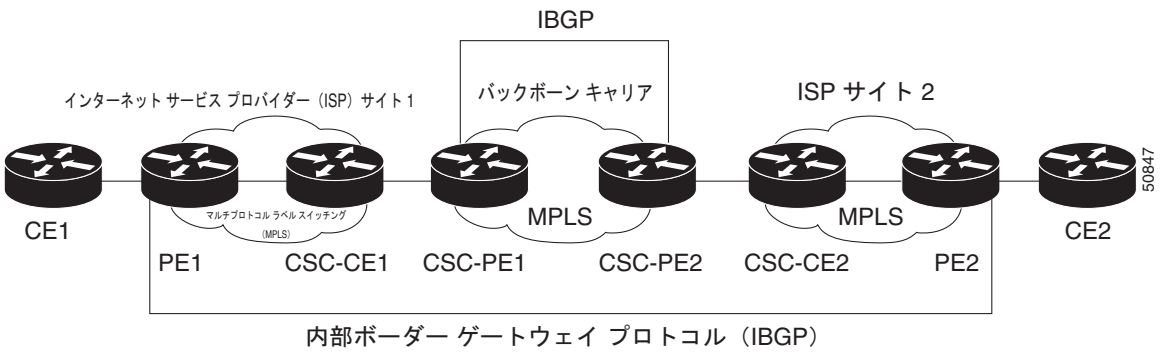
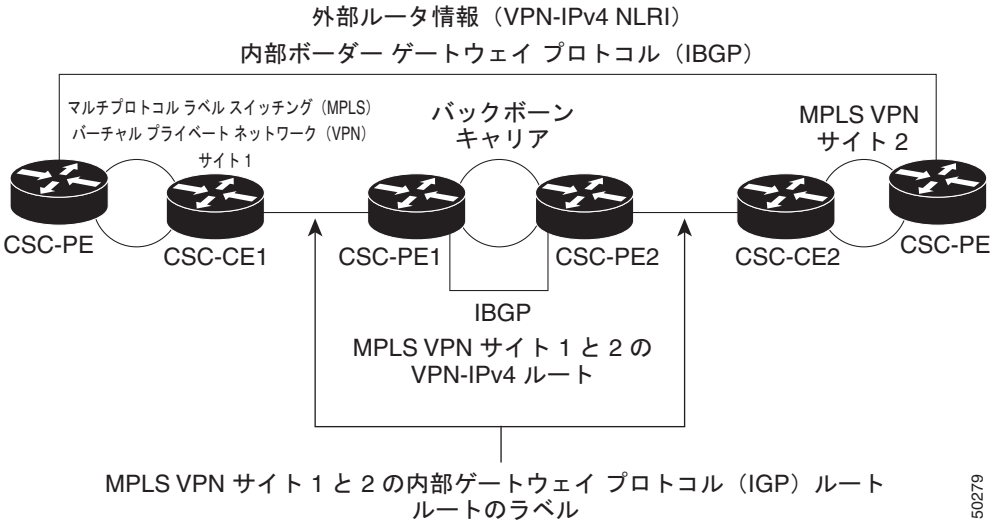


図 5-25 には、MPLS VPN サービス プロバイダーであるカスタマー キャリアと情報を交換するバックボーン キャリアが示されています。

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 ルータとの間には、ルーティング プロトコルが必要です。ルーティング プロトコルにより、カスタマー キャリアは IGP ルーティング情報をバックボーン キャリアと交換できます。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 の代わりになります。BGP を使用して、ルートおよび MPLS ラベルを配布できます。2 つではなく単一のプロトコルを使用すると、設定およびトラブルシューティングが簡単になります。

BGP は、2 つの ISP を接続する場合の優先ルーティング プロトコルです。主な理由は、そのルーティング ポリシーと拡張性です。ISP では、通常、2 つのプロバイダー間で BGP を使用します。この機能を使用すると、これらの ISP は BGP を使用できます。

BGP（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）

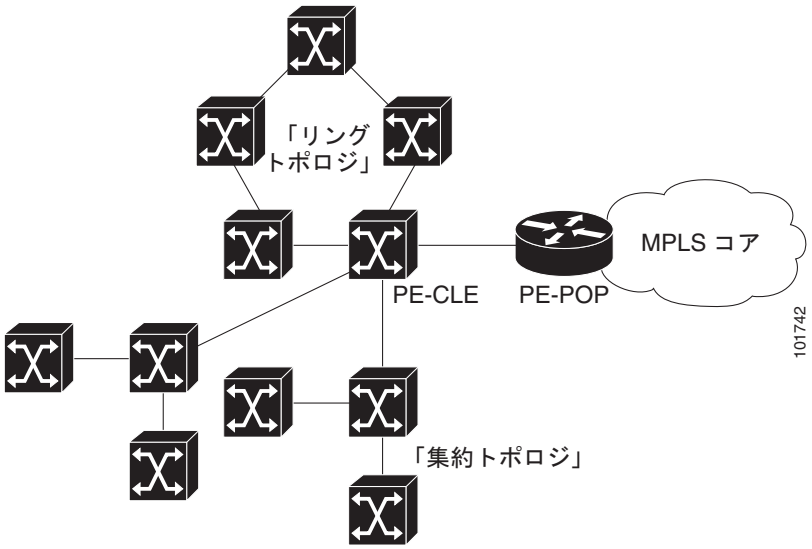
リング トポロジの概要

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

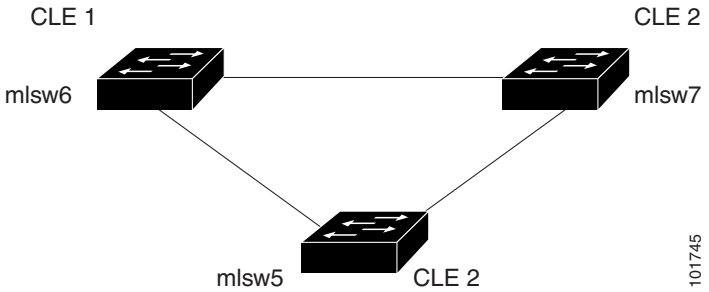


3 つの PE-CLE リングの作成

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 mlsw5、mlsw6、および mlsw7 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。

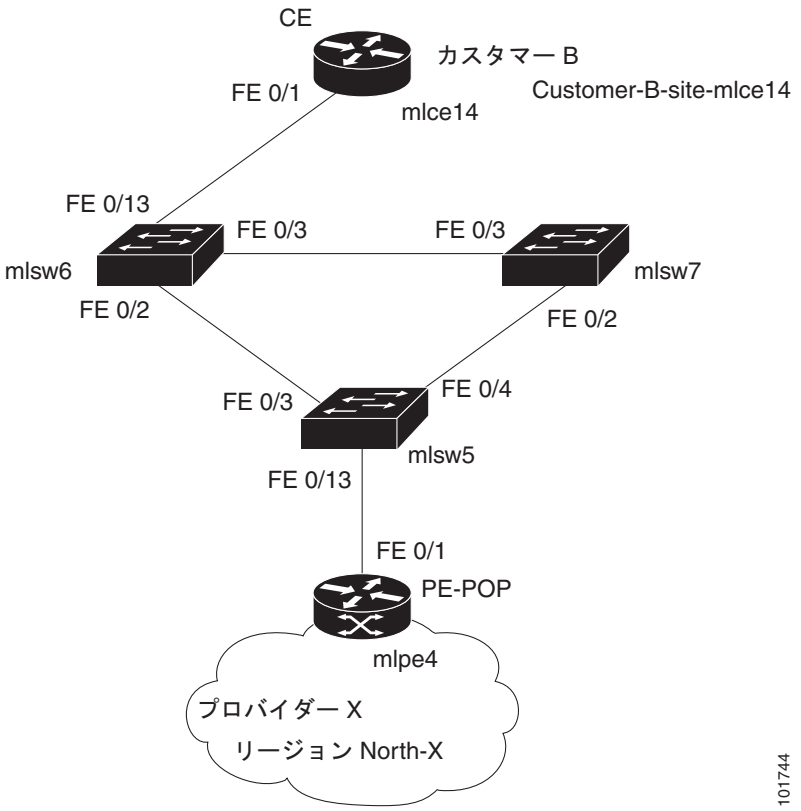
[NPC Rings] ウィンドウが表示されます。

「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



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。

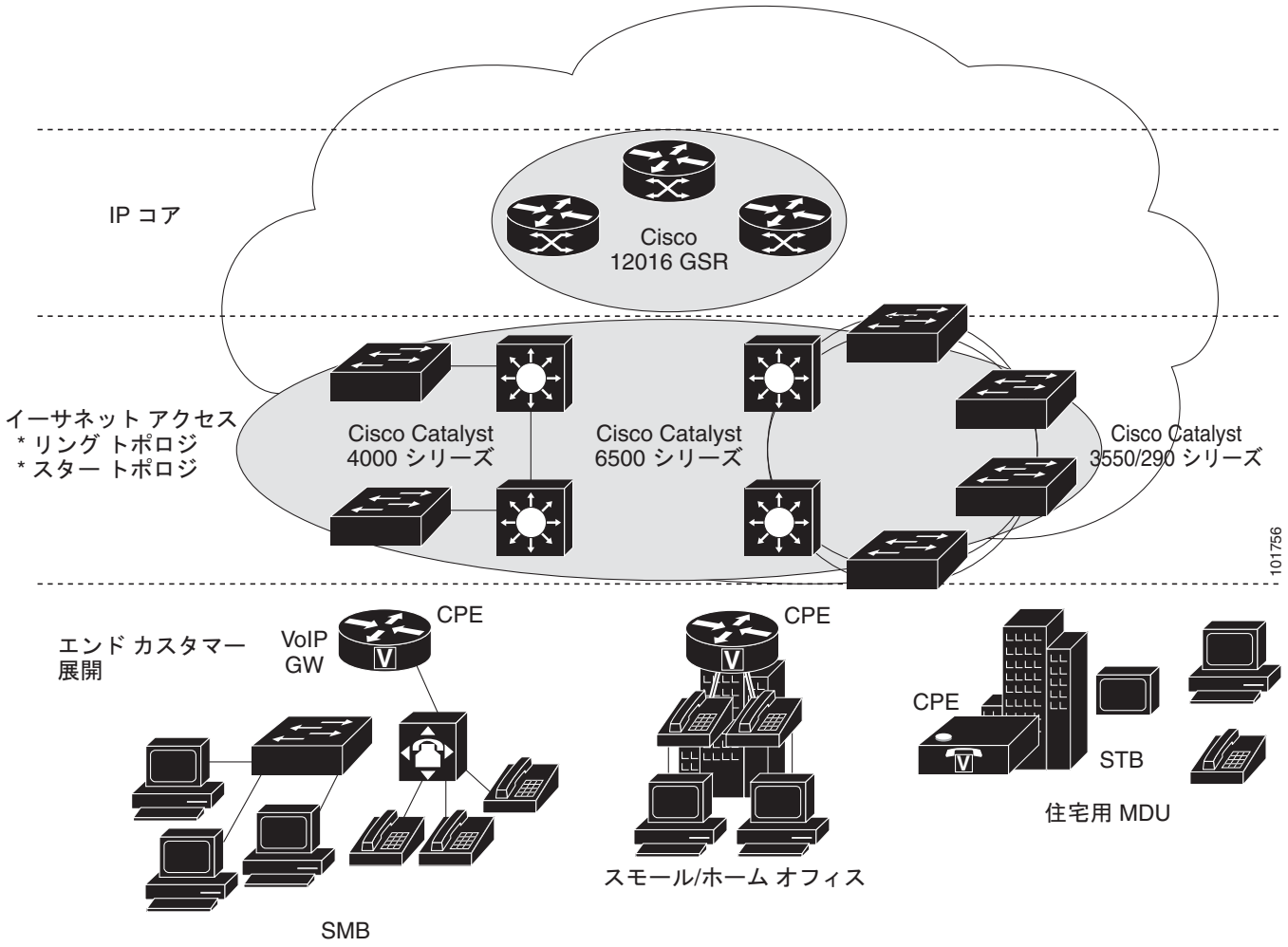
Ethernet-To-The-Home（ETTH）

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なります。

- 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。

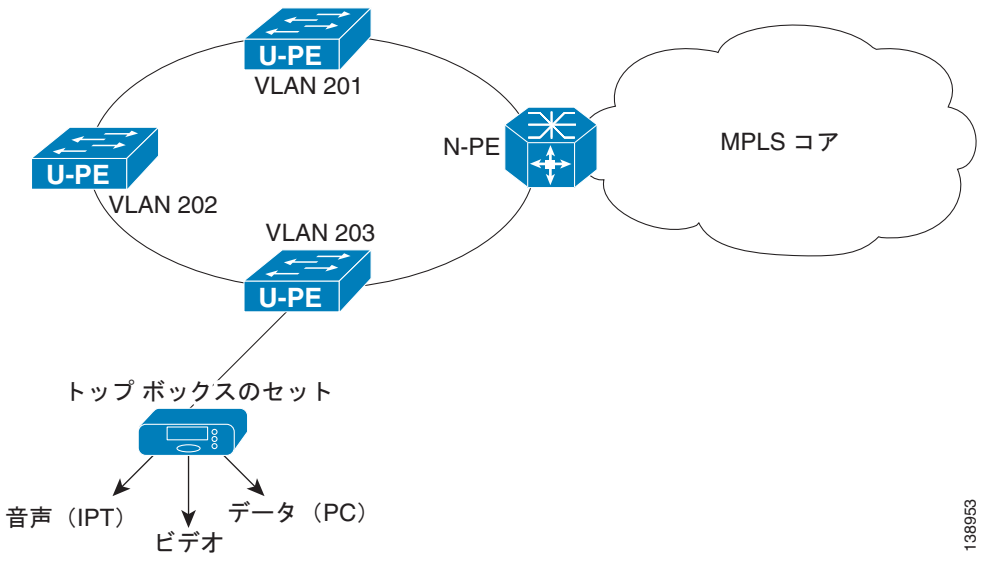
（注）　MPLS VPN サービス要求での VRF および VPN 属性の設定に関する詳細については、「MPLS サービス要求での VRF および VPN 属性の定義」（P.5-91）を参照してください。

[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



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。

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のリストに関する情報を含む、自律システム間のネットワーク到達可能性情報を交換することです。自律システムは、EGBP 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ます。異なる自律システム内のピアは、eBGP セッションを介して通信しますが、これらのピアは iBGP ピアである場合と同様にルート情報を交換できます。

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。

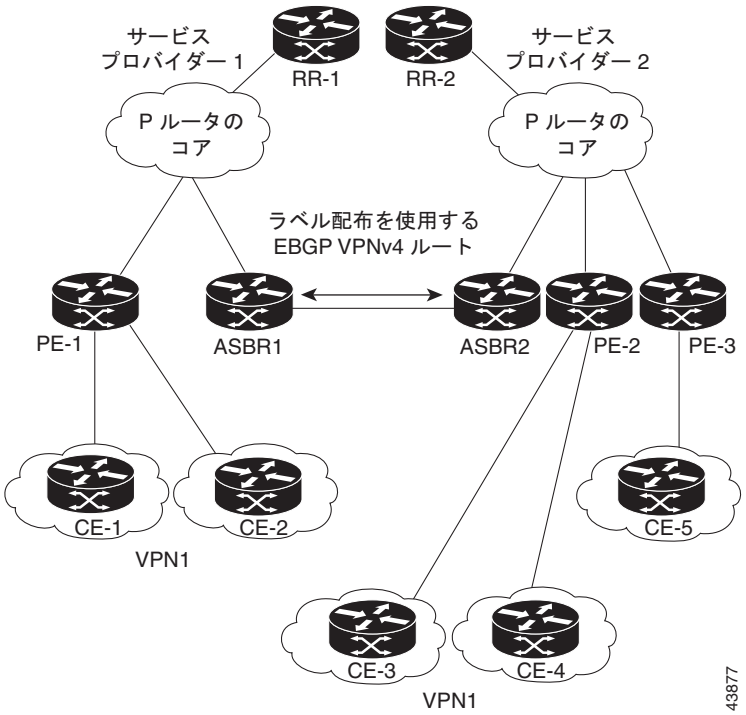
- IBGP メッシングを最適化するための連合が可能

  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 経由で伝播する必要があります。

eBGP VPN-IPv4 ネイバー ホスト ルートを伝播するには、**redistribute connected subnets** コマンドを使用します。eBGP VPN-IPv4 ネイバー ホスト ルートは、ネイバーがアップ状態になったときにルーティング テーブルに自動的にインストールされます。このことは、異なる自律システム内の PE ルータ間でラベル スイッチド パスを確立するために重要です。

VPN ルーティング情報の交換

自律システムは、接続を確立するために VPN ルーティング情報（ルートとラベル）を交換します。自律システム間の接続を制御するために、PE ルータおよび eBGP ボーダー エッジ ルータはラベル転送情報ベース（LFIB）を保持します。LFIB では、VPN 情報の交換中に PE ルータおよび eBGP 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。

図 5-32 に、自律システム間における VPN のルートおよびラベル情報の交換について示します。自律システムでは、次の注意事項を使用して VPN ルーティング情報を交換します。

*ルーティング情報*には次の内容が含まれています。

- 宛先ネットワーク（N）
- 配布元ルータに関連付けられたネクストホップ フィールド
- ローカル MPLS ラベル（L）

RD1: route distinguisher は、VPN-IPv4 ルートを VPN サービス プロバイダー環境でグローバルに一意にするための宛先ネットワーク アドレスの一部です。

ASBR は、IBGP ネイバーに VPN-IPv4 NLRI を送信する場合に、ネクスト ホップを変更するように設定されています（next-hop-self）。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 5-32　　2 つの自律システム間のルートとラベルの交換

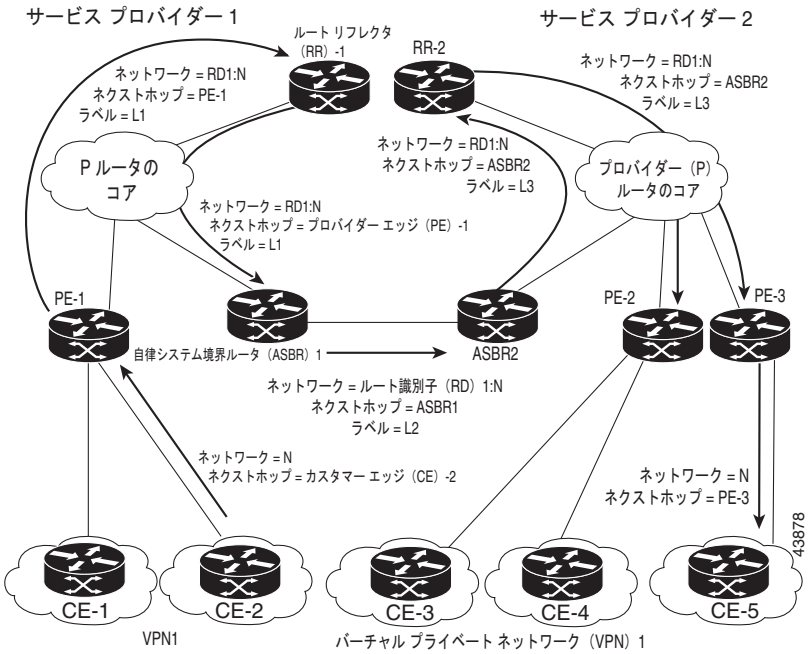


図 5-33 に、自律システム間における VPN のルートおよびラベル情報の交換について示します。唯一の違いは、ASBR2 が **redistribute connected** コマンドを使用して設定されていることです。これにより、ホスト ルートがすべての PE に伝播されます。ASBR2 はネクストホップ アドレスを変更するように設定されていないため、**redistribute connected** コマンドに必要となります。

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

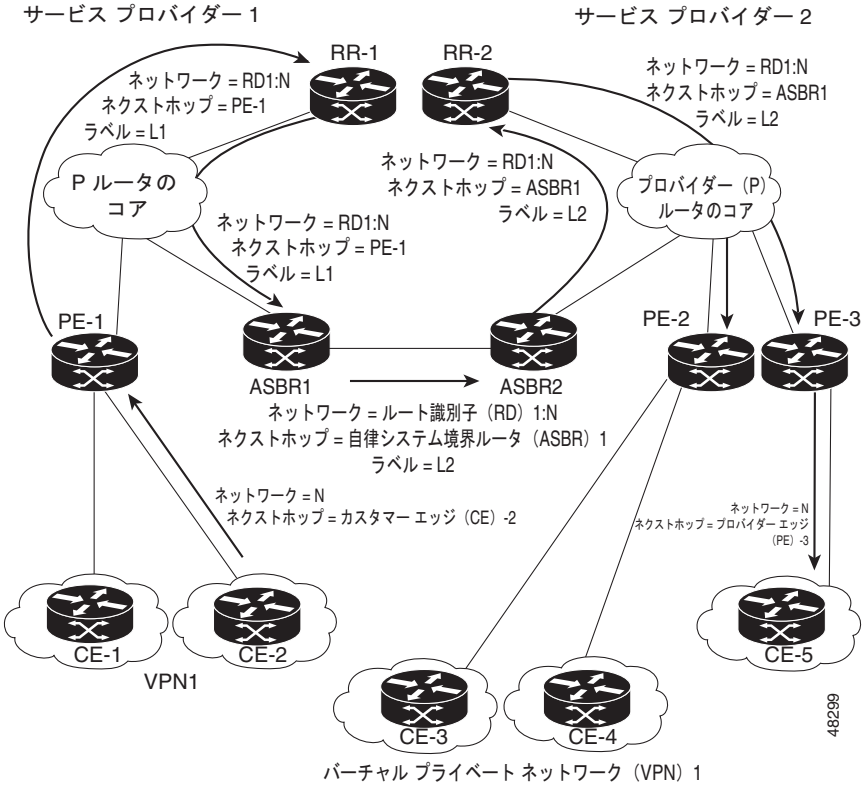


図 5-34 には、プロバイダー間ネットワークにおいて、次のパケット転送方法を使用して自律システム間でパケットが転送されるようすが示されています。

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ダイナミック ラベル スイッチングを使用します。

各自律システムでは、標準的なマルチレベル ラベリングを使用して、自律システム 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 番めのラベル（*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

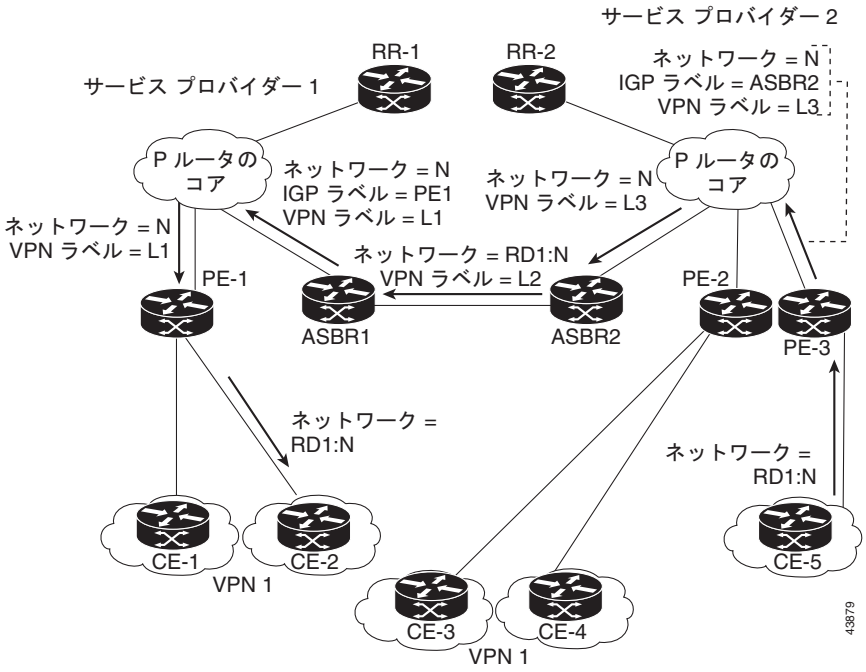
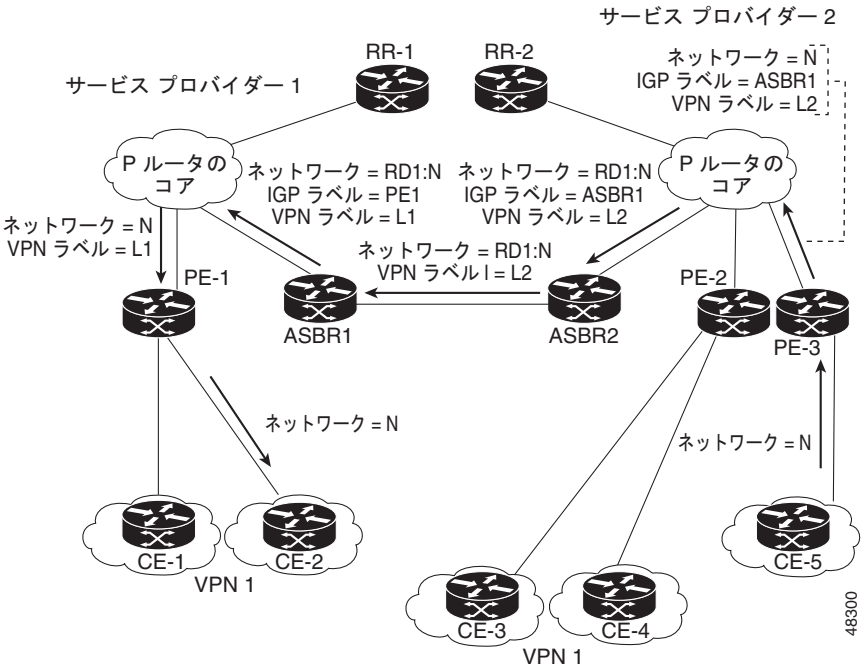


図 5-35 に、同じパケット転送方法を示します。ただし、今回は、eBGP ルータ（ASBR1）で新しいラベルが再割り当てされずにパケットが転送されます。

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。

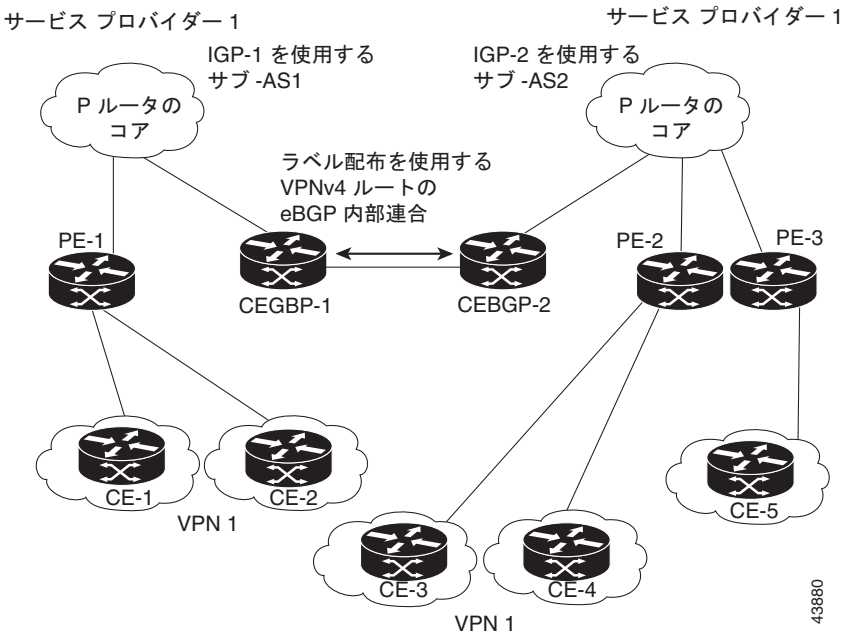
次の 2 つの方法で、異なるサブ自律システムに連合を設定できます。

- 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す。
- 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。

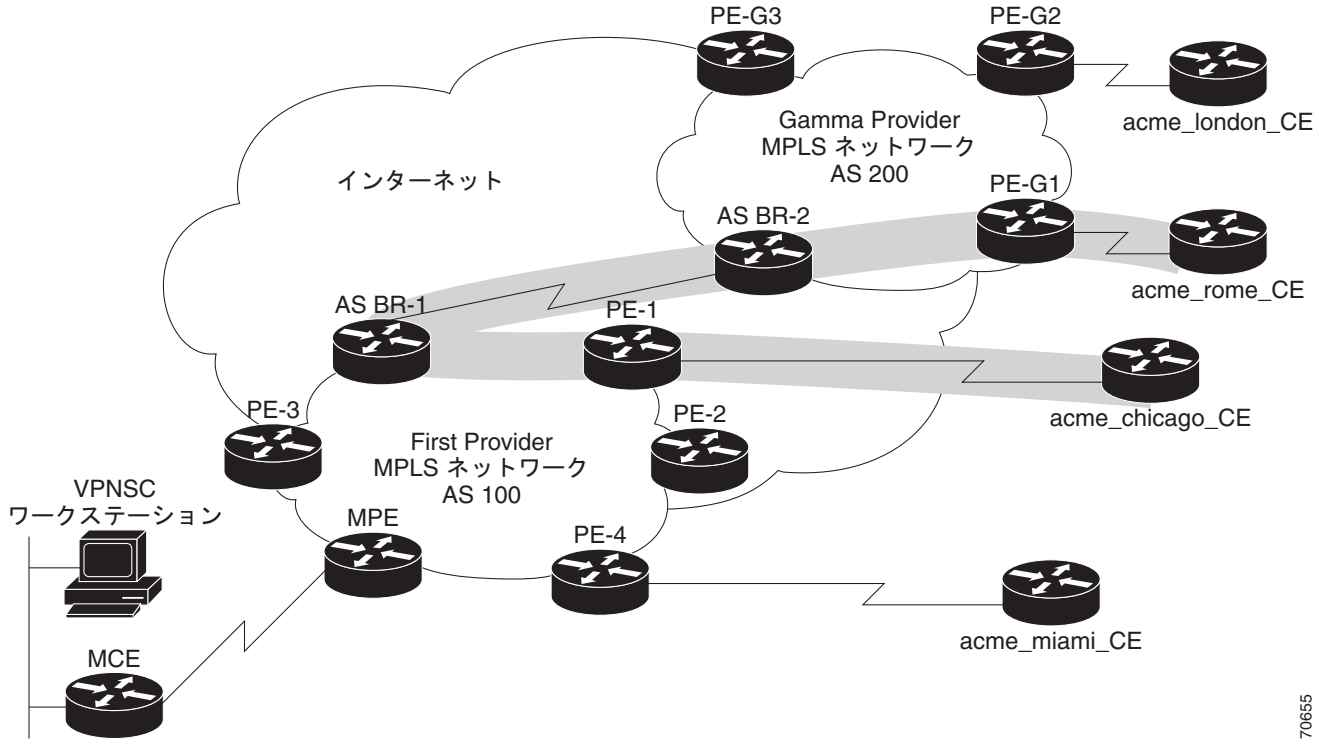
Prime Provisioning を使用した複数の自律システムのスパニング

「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 からのトラフィックが 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の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（*VPNv4* 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 番めのテンプレート 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ます。次の事項について説明します。

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
!	!	!
vlan 3101	vlan 3101	ip vrf V5:VPN_sample
exit	exit	rd 100:1502
!	!	route-target import
interface FastEthernet0/13	interface FastEthernet0/14	100:1602
no ip address	no ip address	route-target import
switchport	switchport	100:1603
switchport trunk	switchport trunk encapsulation	route-target export
encapsulation dot1q	dot1q	100:1602
switchport mode trunk	switchport mode trunk	maximum routes 100 80
switchport trunk allowed	switchport trunk allowed vlan	!
vlan 1,3101	1,3101	interface FastEthernet2/8
!	!	no shutdown
interface Vlan3101	interface FastEthernet0/4	!
description By VPNSC: Job	no keepalive	interface
Id# = 13	no ip address	FastEthernet2/8.3101
ip address 10.19.19.10	switchport	description
255.255.255.252	switchport trunk encapsulation	FastEthernet2/8.3101 dot1q
no shutdown	dot1q	vlan id=3101. By VPNSC:
	switchport mode trunk	Job Id# = 13
	switchport trunk allowed vlan	encapsulation dot1Q 3101
	3101	ip vrf forwarding
	switchport nonegotiate	V5:VPN_sample
	cdp enable	ip address 10.19.19.9
	no shutdown	255.255.255.252
	mac access-group	no shutdown
	ISC-FastEthernet0/4 in	!
	!	router bgp 100
	mac access-list extended	address-family ipv4 vrf
	ISC-FastEthernet0/4	V5:VPN_sample
	deny any host 0100.0ccc.cccc	redistribute connected
	deny any host 0100.0ccc.cccd	redistribute static
	deny any host 0100.0ccd.cdd0	exit-address-family
	deny any host 0180.c200.0000	
	permit any any	

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

```
!
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
```

PE

```
!
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 10
neighbor 10.19.19.42 activate
neighbor 10.19.19.42 allowas-in 2
redistribute connected
redistribute static
exit-address-family
```

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

```
!
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
```

PE

```
!
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
```

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
! 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	! 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

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>
              <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>
                <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>
              <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>
          <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>
                      <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
!	!
interface FastEthernet0/0.158	ip vrf V15:MPLS-1
description FastEthernet0/0.158 dot1q vlan	rd 100:6812
id=158. By VPNSC: Job Id# = 239	route-target import 100:7000
encapsulation dot1Q 158	route-target import 100:7001
ip address 10.1.1.98 255.255.255.252	route-target export 100:7000
no shutdown	!
!	interface GigabitEthernet2/0/15.158
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0.158	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

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す。
  - *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 vpnv4 unicast
 !
 address-family vpnv6 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>
            </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>
```

```
                    <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>
              </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_Verve1 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_Verve1 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_Verve1 address-family ipv4
 rp-address 115.101.110.122 list1
!
router pim vrf V18:VPN_Verve1 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_Verve1
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_Verve1
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_Verve1 address-family ipv6
mdt default 224.10.0.4
mdt mtu 8003
interface GigabitEthernet0/1/0/1.2589
enable
router pim vrf V18:VPN_Verve1 address-family ipv4 rp-address 115.101.110.122 list1
router pim vrf V18:VPN_Verve1 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_Verve1</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_Verve1</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_Verve1</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>
      </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>
    <RemoteAS>
      <AS_XX>0</AS_XX>
      <AS_YY>100</AS_YY>
    </RemoteAS>
  </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す。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>
                  <VRFNeighbor>
                    <Naming>
                      <NeighborAddress>
                        <IPV6Address>25::9</IPV6Address>
```

```
                    </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>
         <VRFTable>
            <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>
                        <Naming>
                           <AF>IPv6Unicast</AF>
                        </Naming>
```

```
            <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>
      </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>
            <VRFTable>
              <VRF>
                <Naming>
                  <VRFName>V67:apr26-vpn2</VRFName>
                </Naming>
                <VRF_AFTable>
                  <VRF_AF>
                    <Naming>
                      <VRF_AFType>IPv4</VRF_AFType>
                    </Naming>
                    <AutoSummary/>
                  </VRF_AF>
                  <VRF_AF>
```

```
                    <Naming>
                      <VRF_AFType>IPv6</VRF_AFType>
                    </Naming>
                    <AutoSummary/>
                  </VRF_AF>
                </VRF_AFTable>
              </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>
```

```
                    <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>
                  <DefaultMetric>
                    <BW>1509</BW>
                    <Delay>1842</Delay>
                    <Reliability>196</Reliability>
                    <Load>187</Load>
                    <MTU>1657</MTU>
```

```
                    </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>
              <BGP>
```

```
            <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>
                    <RouteTarget>
```

```
                    <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>
   <VRFName>V1:VPN_June22</VRFName>
  </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/mpls 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

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 を使用するように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間の関係は、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 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 を作成するときに、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 FastEtherent0/15
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らなくなります。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す。

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 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す。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す。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ければ、[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。

CHAPTER 6

MPLS トランスポート プロファイル サービスの管理

この章では、Prime Provisioning、マルチプロトコル ラベル スイッチング（MPLS）のトランスポート プロファイル（TP）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。

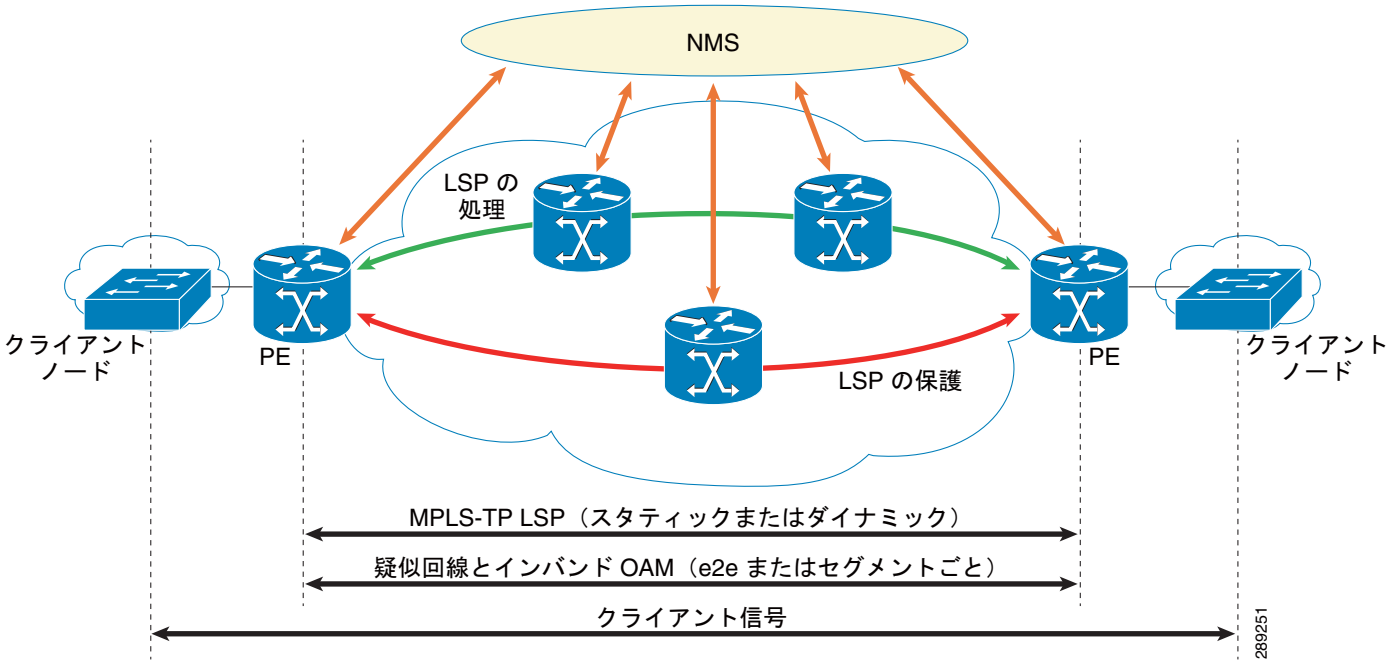
具体的な内容は、次のとおりです。

はじめに

MPLS-TP は、ダイナミック MPLS コアに対するトランスポート サービスです（Prime Provisioning によって管理されます）。

MPLS-TP の現在の実装で、MPLS-TP トンネルは、MPLS-TP 対応ネットワーク内の 2 つの任意のノード間でプロビジョニングできます。プロビジョニングされたトンネルには、1 つまたは 2 つのパス、現用および任意の保護ラベル スイッチド パス（LSP）を割り当てることができます。通常のユースケースで、Prime Provisioning は、最短パスに基づいて MPLS-TP 対応リンクを選択するパス選択アルゴリズムを使用して、現用パスと保護パスを自動的に計算し、トンネルが通過するエンドポイントおよびすべてのノードでトンネルをプロビジョニングします。

図 6-1　MPLS-TP 対応ネットワーク



前提条件と制限事項

現在のリリースの Prime Provisioning には、一般的なシステムの推奨事項を含め、*『Cisco Prime Provisioning 6.3 Installation Guide』*で説明する一定の前提条件および制限事項があります。

Internet Explorer 8（IE8）は SVG の表示をサポートしないため、IE8 では、計算されたパスがグラフィカルに表示されないことに注意してください（「MPLS-TP サービス要求の作成」（P.6-9）を参照）。IE9 がサポートされるまで、パスのテキストによるサマリーを使用して、IE8 でパスを確認できます。

動作しているデバイスに対して実行した変更は、Prime Network に反映されるまでに時間がかかることがあります。

ポーリングは、（最低）15 分ごとに、Prime N によって実行されます。1 ～ 15 分の間に、ポーリングは何度も実行されます。各ポーリングでは、さまざまなデータ（トンネル、ラベル、リンクなど）が収集されます。1 回のポーリングではすべての情報が収集されないため、Prime N で、トンネルの更新、ラベルの更新、リンクの更新を反映するのにかかる時間は異なります。

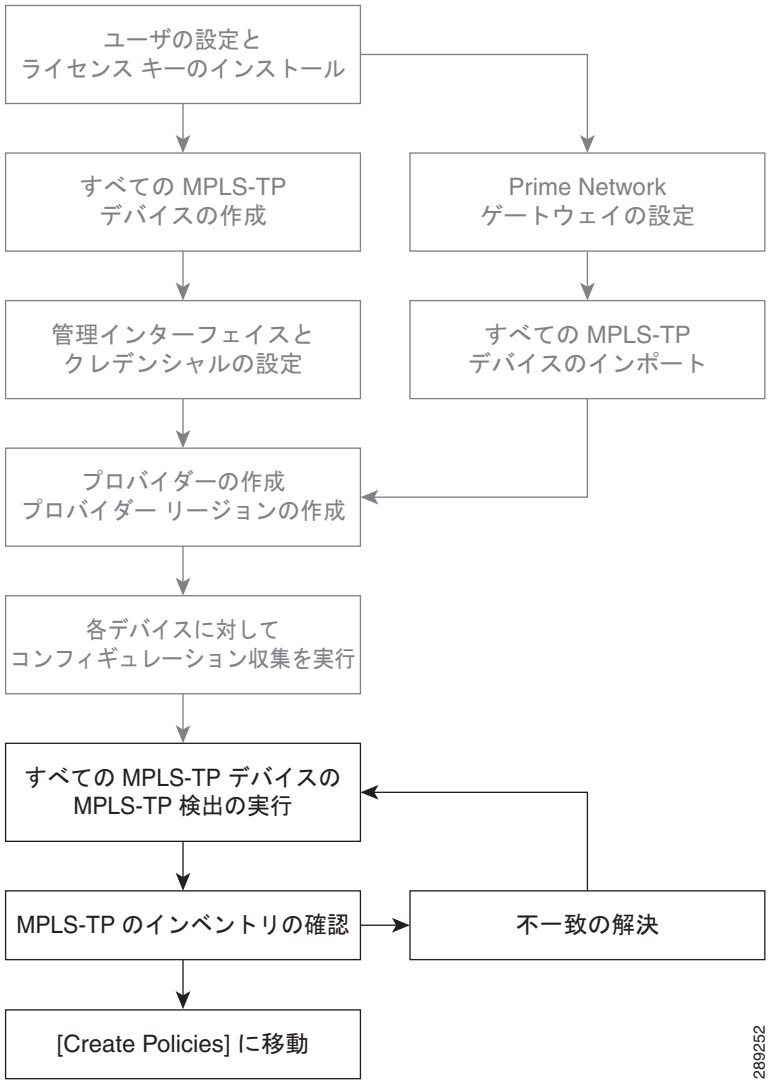
サポートされるデバイスと OS については、*『Cisco Prime Provisioning 6.3 Supported Devices』*を参照してください。

事前設定処理

事前設定処理により、システムが MPLS-TP ネットワーク情報を収集し、選択されたネットワークで MPLS-TP 設定を展開することを可能にする主要なパラメータが設定されます。

図 6-2 には、事前設定処理の異なる手順が示されています。

図 6-2　事前設定処理



事前設定処理を開始する前に、デバイスの MPLS-TP ID として使用される IP アドレスに、管理ステーションから正常にアクセスできることを確認することにより、ネットワーク デバイスで MPLS-TP をイネーブルにする必要があります（このステップは MPLS-TP によってサポートされていません）。これについては、「その他の MPLS-TP 事前設定の要件」（P.6-4）で説明します。

新しいユーザの設定およびライセンス キーのインストールについては、*『Cisco Prime Provisioning Administrator’s Guide 6.3』*で説明されています。その他のステップについては、「デバイスおよびデバイス グループを設定する方法」（P.2-1）および「インベントリ - ディスカバリ」の付録（Collect Config step）を参照してください。

このため、Prime Provisioning ユーザは、Prime Network でデバイスを変更した後に、MPLS-TP ディスカバリを実行するまで、しばらく待つ必要があります。

（注）　Prime Provisioning を Prime Central と統合する場合は、Prime Network 証明書を Prime Provisioning Trust Store にインポートする必要があります。これについては、「Prime Provisioning トラスト ストアへの Prime Network 証明書のインポート」（P.13-14）で説明されています。

特定の MPLS-TP ユーザ ロールについては、以下を参照してください。

MPLS-TP に固有なステップは次のとおりです。

1. MPLS-TP **ディスカバリ タスクの実行**：タスク マネージャを使用して、特定の MPLS-TP プロバイダーの MPLS-TP ネットワークを検出し、プライマリ トンネルとバックアップ トンネルを作成するために、リポジトリに入力します。（「MPLS-TP ディスカバリの実行」（P.6-5）を参照）。
2. MPLS-TP **インベントリの確認**：MPLS-TP ディスカバリ タスクが正常に完了したことを確認します。これは、いくつかの方法で実行できます。（「MPLS-TP ディスカバリ結果の確認」（P.6-6）を参照）。

MPLS-TP のセットアップおよびインストール

Prime Provisioning を設定する前に、Prime Provisioning ソフトウェアをインストールする必要があります。これを行うには、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください。

新規 Prime Provisioning ユーザを設定する場合は、MPLS-TP ロールを持つユーザを 1 つ以上作成する必要があります。MPLS-TP ロールについては、「MPLS-TP のユーザ ロール」（P.6-4）で説明されています。で説明されています。ユーザ ロールを作成するためのステップバイステップの手順については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* を参照してください。

Prime Provisioning ライセンス オプションなどのライセンス情報と、ライセンスのインストールに必要な手順については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* を参照してください。

MPLS-TP のユーザ ロール

Prime Provisioning は、現在 2 つの MPLS-TP ロール、MPLS TPRole および MPLS TPServiceOpRole をサポートしています。この 2 つユーザ ロールは、Prime Provisioning の他のロールと同様に動作します（MPLS にある MPLSRole および MPLSServiceOpRole など）。

これらのユーザ ロールには、次の権限があります。

- MPLSTPRole：インベントリを管理するフル権限（MPLS-TP ポリシーおよびサービス要求の作成、更新、削除、および展開）
- MPLSTPServiceOpRole：MPLS-TP サービス要求を展開する権限

ロールの使用方法については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* を参照してください。

その他の MPLS-TP 事前設定の要件

MPLS-TP プロビジョニングを実行する前に、次の追加の設定ステップを実行します。

ステップ 1　デバイスでの MPLS-TP の有効化：

- すべてのデバイスに共通のグローバル ID を選択します（AS 番号など）。
- 各デバイスにデバイス ID を割り当てます。
- MPLS-TP 関連タイマーを設定します。

ステップ 2　スタティックに定義された MPLS ラベルの範囲を、MPLS-TP トンネルおよびスタティック疑似配線で使用されるように設定します。

ステップ 3　MPLS-TP トポロジのリンクを形成するインターフェイスを選択するために、MPLS-TP リンクをイネーブルにします。

- 各インターフェイスの ID を指定します。
- 任意で各インターフェイスの帯域幅プールを設定します。

ステップ 4　MPLS-TP トンネルの監視に使用する BFD クラスを作成します。

MPLS-TP ディスカバリの実行

Prime Network とともに（または）IP-NGN スイート内に展開された場合、Prime Provisioning は、IOS および IOS-XR デバイスからの MPLS-TP ディスカバリをサポートします。Prime Provisioning は、Prime Provisioning DCPL プロパティの **Inventory Import** で Prime Network ゲートウェイの詳細を設定することにより、Prime Network と「組み合わせる」ことができます。

スタンドアロン モード（Prime Network との統合なし）の Prime Provisioning は、IOS デバイスからの CDP ベース MPLS-TP ディスカバリをサポートしていますが、これは非推奨です。

MPLS-TP ディスカバリを実行するための前提条件として、すべてのデバイスが存在し、コンフィギュレーション収集タスクを実行する必要があります（「インベントリ - ディスカバリ」の付録「Collect Config step」を参照）。Prime Provisioning DCPL プロパティで Prime Network ゲートウェイの詳細を設定します。DCPL プロパティの設定の詳細については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* を参照してください。

MPLS-TP 対応デバイスは、次のように、Prime Provisioning インベントリに追加し、または作成する必要があります。

- Prime Provisioning で直接デバイスを作成します。

または

- Prime Provisioning のデバイス作成ページで提供される「インポート」機能を使用します（このページでは、Prime Network からデバイスをインポートできます）。

MPLS-TP ネットワークは、MPLS-TP **ディスカバリ** タスクを使用して検出されます。これによって、自動的な方法でネットワーク トポロジがリポジトリに入力されます。必要なステップについては、この項で説明します。

（注）　MPLS-TP ディスカバリでは、MPLS-TP ルーティング図（Service Request Editor、[Review Routing] アコーディオン）で、機能 MPLS-TP リンクだけが更新されます。

MPLS-TP ディスカバリ プロセスは、稼働中のネットワークから次の要素を検出します。

- TP 対応リンク
- MPLS スタティック ラベル プール
- MPLS スタティック ラベル プールの使用

- BFD テンプレート
- TP ルータ ID
- TP グローバル ID

可能な場合は、ディスカバリ プロセスは、リポジトリとネットワークの一貫性が維持しようとします。たとえば、取り外されたリンクを削除します。これが不可能な場合は（リンクが使用中の場合など）、ログ メッセージが記録されます。

ここでは、次の内容について説明します。

- 「MPLS-TP ディスカバリ タスクの作成」（P.6-6）
- 「MPLS-TP ディスカバリ タスクの作成」（P.6-6）
- 「MPLS-TP ディスカバリ結果の確認」（P.6-6）

MPLS-TP ディスカバリ タスクの作成

MPLS-TP ネットワーク上で MPLS-TP ディスカバリ タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

[Task Manager] ウィンドウが表示されます。

ステップ 2　[Create] > [MPLS-TP Discovery] を選択し、新しいタスクを作成します。

[Create Task] ウィンドウが表示されます。

ステップ 3　自動生成された名前と説明テキストに必要な変更を加え、[Next] をクリックします。

[MPLS-TP Discovery] ウィンドウが表示されます。

ステップ 4　MPLS-TP ネットワークの検出に使用するデバイスを選択します。

ステップ 5　[Submit] をクリックします。

ディスカバリ プロセスが開始されます。

ステップ 6　MPLS-TP ディスカバリ タスクが完了すると、結果が次の場所にあるログに記載されます。

[Operate] > [Task Logs]

デバイス作成の直後に MPLS-TP ディスカバリ タスクを実行するには、次の場所に移動します。

[Inventory] > [Devices] > [Create] >[Cisco Device]

[Create Cisco Router] ウィンドウで、[MPLS-TP] チェックボックスをオンにします。

これにより、リンクおよびリソース プールが [MPLS-TP Details] ウィンドウに表示されるはずです。このウィンドウには、[Inventory] > [Devices] > [MPLS-TP Details] ページからアクセスできます。

MPLS-TP ディスカバリ結果の確認

MPLS-TP ディスカバリを実行した後に、さまざまな方法で結果を表示できます。

ログの表示

MPLS-TP **ディスカバリ** タスクが完了した後に、生成されたログを表示できます。このサマリー ログには、MPLS-TP ネットワークで発生した変更が一覧表示されます。ディスカバリは、現用または保護 LSP がもはや存在していないか、変更された場合に影響を受ける SR とともに、ログを更新します。これは、ノードの挿入/削除またはリンク番号だけの変更の結果として発生することがあります。

ログを表示するには、タスク マネージャの該当するタスクを選択して、[Logs] をクリックします。

リンク、プール、および MPLS-TP のグローバル ID とルータ ID の確認

リンクおよびプールのステータスを確認するには、[MPLS-TP Details page at Inventory] > [Devices] > [MPLS-TP Details] に移動します。

特定のデバイスの MPLS-TP グローバル ID およびルータ ID は、[Inventory] > [Devices] > [Edit] に移動することによって、確認できます。

MPLS-TP ラベルの同期

MPLS-TP ラベルの同期タスクでは、ラベル情報を更新します。MPLS-TP ラベルは、手動プロビジョニングによって同期しなくなることがあります。したがって、MPLS-TP トポロジ情報全体ではなく、単独でラベル情報を頻繁に更新することを推奨します。

MPLS-TP ディスカバリと同様に、MPLS-TP ラベルの同期タスクは、次のウィンドウから実行できます。

- [Task Manager] ウィンドウ
- [Device Inventory] ウィンドウ
- [Device Creation] ウィンドウ

MPLS-TP ポリシーの作成

MPLS-TP ポリシーは、サービス要求を正常に作成および展開するために必要です。これは、デバイスに必要な設定のテンプレートとして機能します。

MPLS-TP ポリシーを作成するには、次のステップを実行します。

ステップ 1　次のいずれかを選択します。

a. [Service Design] > [Policy Manager]

[Policy Manager] ウィンドウで、[Create] をクリックします。

b. [Service Design] > [Create Policy]

いずれの場合も、[Policy Type] ドロップダウンが表示されます。

ステップ 2　下矢印をクリックして、[Policy Types] ドロップダウン リストを開き、[MPLS-TP Tunnel] を選択します。

[Policy Information] アコーディオンが開きます。

ステップ 3　アコーディオン 1 – [Policy Information] に記入します。

[Policy Name] に入力し、任意で [Description] に入力します。Policy Editor の必須フィールドは、[Policy Name] だけです。

ステップ 4　[Next] をクリックします。

[Policy Information] アコーディオンが閉じ、次のアコーディオンが開きます。

ステップ 5　アコーディオン 2 – [Tunnel Characteristics] に記入します。

各フィールドの横のドロップダウンを使用して、[Service Request Editor] ウィンドウ内に各属性を表示する方法を設定します。

- [Editable] では、属性が表示され、変更が許可されます。
- [Visible] では、属性が表示されますが、編集できません。
- [Hidden] では、属性は表示されません。

Service Request Editor で編集可能にする必要があるフィールドに対しては、必ず [Editable] を選択してください。

shutdown コマンドでトンネルをプロビジョニングする必要があるかどうかを示すには、[State] フィールドを使用します。

パスの保護で、Prime Provisioning に新しいトンネルの代替保護パスを自動生成させるには、[Protection] ボックスを選択したままにしてください。

[Diversity Options] ドロップダウン メニューでは、次のいずれかのオプションを選択します。

- [Node Diversity Required]：一意のノードでの保護が見つからない場合、パス計算は失敗します。
- [Node Diversity Desired]：共通ノードのパスが返されることを許可します。
- [Link Diversity Only]：現用パスと保護パスが、同じリンクを通過することを許可しません。

ステップ 6　アコーディオン 3 – [Tunnel End-points] に記入します。

前のアコーディオンと同様に、Service Request Editor で [Editable]、[Visible]、および [Hidden] にする必要があるフィールドを必ず指定します。

必要に応じてフィールドに記入し、ドロップダウンを使用して、送信元ノードと宛先ノードおよび BFD テンプレートを選択します。

（注）　BFD の属性が IOS-XR デバイスで設定されている場合は、[BFD] フィールドで、Global-BFD テンプレートを指定する必要があります。

送信元デバイスと宛先デバイスで使用可能な BFD テンプレートのリストから、必要な BFD テンプレートを選択します。有効な BFD テンプレート名の長さは最大 31 文字です。

グローバル ID およびルータ ID については、「グローバル ID およびルータ ID」（P.6-8）を参照してください。

ステップ 7　ポリシーを作成するには、[Finish] をクリックします。

新しいポリシーが、ポリシー マネージャでトンネルのリストに表示されます。

グローバル ID およびルータ ID

グローバル ID とルータ ID は、検出および管理できるように、MPLS-TP ネットワーク内のデバイスを識別するために使用されます。

ユーザがルータ ID とグローバル ID を指定することを決定した場合、これらの値は、トンネル作成のために使用されます。これらの ID が指定されていない場合は、デバイス自体で設定されたルータ ID とグローバル ID が使用されます。

すべての MPLS-TP のトンネルと LSP には、トンネルの両端のグローバル ID、ルータ ID、トンネル ID、および LSP ID を連結して形成された一意の ID があります。この ID は、トンネルのすべてのエンドポイントおよびミッドポイントで設定されます。グローバル ID とルータ ID は、通常、ルータではグローバルに設定されているが、特定のトンネルにこれらの値を上書きすることができます。
Prime Provisioning は、グローバルに設定された ID を認識し、トンネルを設定する場合に使用します。ただし、必要に応じて、ユーザがこれらの値を上書きすることも許可します。

グローバル ID

すべての MPLS-TP 対応ノードには、グローバル コンフィギュレーション内で設定される MPLS-TP グローバル ID を割り当てることができます。グローバル ID が MPLS-TP のグローバル コンフィギュレーション レベルで設定されている場合、これは、すべてのエンドポイントおよびミッドポイントのコンフィギュレーションでデフォルト グローバル ID として使用されます。 設定しない場合は、トンネル コンフィギュレーション内で異なる値が明示的に指定されていない限り、設定されたトンネルに対して、0 のグローバル ID が使用されます。

MPLS-TP グローバル ID は、MPLS-TP ディスカバリによってデバイスから取得されます。

ルータ ID

MPLS-TP に対応するために、デバイスにはルータ ID が必要です。

MPLS-TP ルータ ID も MPLS-TP グローバル ID もデバイスから取得できない場合は、対応する MPLS-TP **ディスカバリ タスク**のログ ファイルに記録されます。残りのすべての MPLS-TP ディスカバリ ステップは、このデバイスに対して停止します。疑わしいデバイスには、MPLS-TP 非対応としてフラグが付けられます。

MPLS-TP サービス要求の作成

MPLS-TP サービス要求は、サービス要求を展開するために作成する必要があります。少なくとも 1 つの MPLS-TP のポリシーが使用可能であることを前提としています。使用可能ではない場合は、「MPLS-TP ポリシーの作成」（P.6-7）を参照してください。

MPLS-TP サービス要求を作成するには、次のステップを使用します。

ステップ 1　この操作には、次の 2 つの方法があります。

a. Policy Manager で、目的のポリシーを選択して、[Create Service Request] をクリックします。

b. [Operate] > [Create Service Request] を選択します。

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

[Policy] フィールドの横にある下矢印をクリックして、ポリシーの選択肢を開きます。

ステップ 2　必要な MPLS-TP ポリシーを選択します。

Service Request Editor が開きます。このエディタでは、次の操作を行います。

ステップ 3　[Service Request] アコーディオンで、[Service Description] フィールドに説明を追加します。

ステップ 4　[Tunnel Characteristics] アコーディオンでは、事前入力されたフィールド値を使用するか、必要な変更を行います。

[Diversity Options] の設定については、「MPLS-TP ポリシーの作成」（P.6-7）を参照してください。

ステップ 5　[Tunnel End-Points] アコーディオンでは、[Source Node] フィールドと [Destination Node] フィールド、および任意で他のフィールドにも入力します。

このアコーディオンでは、送信元デバイスと宛先デバイスの両方、および BFD 情報は必須です。

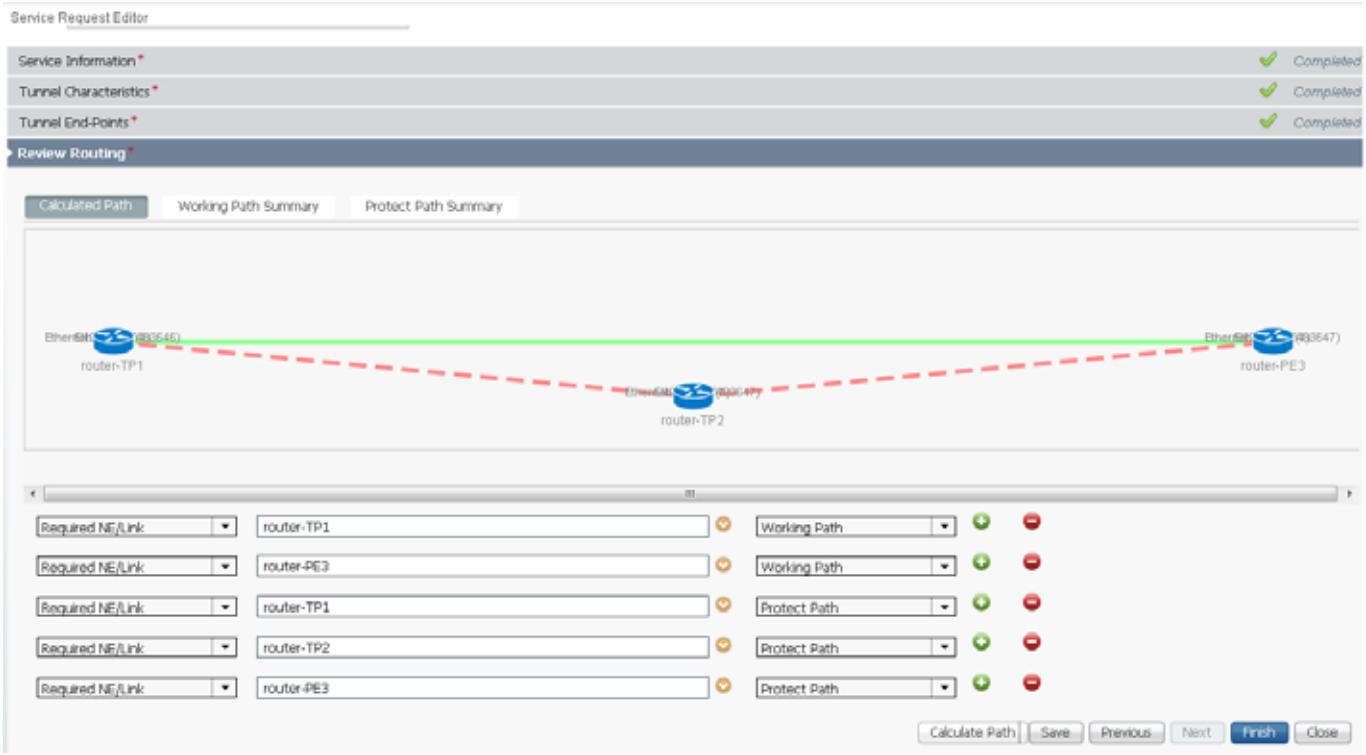
ステップ 6　[Review Routing] アコーディオンで、デフォルトのパスは、送信元と宛先の間で自動的に計算され、表示されます。

動作パス：緑の実線

保護リンク：赤の点線

MPLS-TP ルーティング図の例については、図 6-3 を参照してください。

図 6-3　MPLS-TP ルーティング図



- [Working Path Summary]：動作パスのホップおよびリンクの情報を表示するには、このボタンをクリックします。
- [Protect Path Summary]：保護パスのホップおよびリンクの情報を表示するには、このボタンをクリックします。
- 右のプラス（またはマイナス）アイコンをクリックして、パス制約を追加（または削除）します。
  - [Required NE/Link]：現用パスまたは保護パスのいずれかに対して、トラフィックが通過する必要があるネットワーク要素またはリンクを指定します。
  - [Excluded NE/Link]：現用パスまたは保護パスのいずれかに対して、トラフィックが通過**してはならない**ネットワーク要素またはリンクを指定します。

パス制約の詳細については、「パス制約の操作」（P.6-11）を参照してください。

ステップ 7　さまざまなアコーディオンに戻って、必要に応じて確認および編集します。

ステップ 8　サービス要求の作成操作を完了するには、最後のアコーディオンで [Finish] をクリックします。

[Service Request Manager] ウィンドウが開きます。

Service Request Manager の要素と操作については、第 8 章「サービス要求の管理」を参照してください。

パス制約を操作するためのガイドラインを「パス制約の操作」（P.6-11）に示します。

DRAFT 状態の MPLS-TP サービス要求を変更できます。**DRAFT MPLS-TP** サービス要求を変更した場合、新しい値で、以前に保存された値が置き換えられます。

DRAFT 状態のサービス要求は、Service Request Manager で白 / オレンジの三角コーンでマークされます。

パス制約の操作

パス制約は、作成の手順の ステップ 6 手順に示すように、サービス要求の作成または変更時に、トンネル パスを制御するために追加できます。

パス制約を追加する方法は 2 つあります。

- ルーティング図のノードまたはリンクをクリックし、プラス記号をクリックします。これにより、デフォルトで、新しいパス制約が現用パスに追加されます。必要に応じて、ドロップダウンを使用して [Protect Path] に変更します。同様に、マイナス記号をクリックすると、制約が削除されます。
- 除外 / 追加するノード / リンクが現在の図にない場合は、[Required NE/Link] の横のセレクタを使用できます。

（注）　最初のパス計算後に何かを変更した場合は（制約の追加 / 削除、保護のオン / オフの切り替えなど）、[Calculate Path] をクリックしてパス計算を再び実行する必要があります。

コンフィギュレーション監査の実行

コンフィギュレーション監査タスクは、MPLS-TP サービス要求に対して実行して、特定のサービス要求によってデバイスに展開されたコンフィギュレーションが、予想どおりにまだ存在することを確認できます。

MPLS-TP コンフィギュレーション監査タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Audit] > [Config Audit] をクリックして [Create Task] ウィンドウを開きます。

ステップ 3　必要に応じて [Name] または [Description] フィールドの内容を変更し、[Next] をクリックします。

サービス要求の選択ウィンドウが表示されます。

ステップ 4　サービス要求を追加し、スケジュールを選択するには、[Select SRs] をクリックします。

ステップ 5　[Submit] をクリックします。

成功した場合は、[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

作成されたタスクのタスク ログを表示するには、タスク マネージャで、作成されたタスクを選択し、[Logs] をクリックします。

MPLS-TP 機能監査の実行

MPLS-TP 機能監査では、トンネルの監査情報を提供するために、送信元および宛先エンドポイントから情報が取得されます。

このタスクでは、次のいずれかの状態でないサービス要求に対してのみ機能監査を実行します。

- **Draft**
- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

サービス要求での作業の詳細については、第 8 章「サービス要求の管理」を参照してください。

MPLS-TP 機能監査タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Audit] > [MPLS-TP Tunnel Functional Audit] をクリックして [Create Task] ウィンドウを開きます。

ステップ 3　必要に応じて [Name] または [Description] フィールドの内容を変更し、[Next] をクリックします。

サービス要求の選択ウィンドウが表示されます。

ステップ 4　サービス要求を追加し、スケジュールを選択するには、[Select SRs] をクリックします。

ステップ 5　[Submit] をクリックします。

成功した場合は、[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

作成されたタスクのタスク ログを表示するには、タスク マネージャで、作成されたタスクを選択し、[Logs] をクリックします。

MPLS-TP トポロジ変更の管理

ノードの挿入/削除によってトポロジが変更された場合、MPLS-TP ディスカバリでは次のことを実行できます。

- ノードの挿入/削除による MPLS-TP トポロジ変更を管理します。
- ノードの挿入/削除によって影響を受ける MPLS-TP トンネル SR を識別します。
- MPLS-TP トンネルを修復するには、影響を受ける SR を変更します。
- ノードの挿入/削除の影響を受ける MPLS-TP トンネル SR を検出します。
- 影響を受ける SR のパスを再計算します。再計算中：
  - 影響を受ける LSP は、中断のないトラフィックのために Prime Network によってロックされます。
  - Prime Provisioning 内の影響を受けるすべての SR は、Closed、Pending、In-Progress のいずれかの状態、または DELETE Op Type の場合を除き、再ルーティングされます。
- 影響を受ける SR を適切な状態に遷移させます。
  - 遷移は、展開された SR だけで発生します。

  - 展開された SR の障害トンネルに対して新しいルートが見つかった場合、SR は Requested 状態に移行します。
  - 新しいルートが見つからない場合、展開されたトンネル SR は無効な状態に移行します。
  - 他のすべての SR では、Closed、Pending、In-Progress のいずれかの状態、および Op Type DELETE の場合を除き、パスは状態の変更なしで再計算されます。
- 影響を受ける SR を報告し、SR ログを更新します。ディスカバリは、現用または保護 LSP がもはや存在していないか、変更された場合に影響を受ける SR とともに、ログを更新します。
  - 影響を受けるすべての SR では、ディスカバリは、ディスカバリのログおよび SR 履歴レポートを更新します。
  - ディスカバリは、SR 履歴を次の情報で更新します。
    - 影響を受けるパス、現用 / 保護 LSP。
    - 状態変更の詳細、以前 / 現在の状態。
    - パスの変更 / 失敗に関するメッセージ。
- 影響を受ける LSP だけを再プロビジョニングします。Requested Modify 状態の SR が展開のために選択された場合、変更された LSP だけが Prime Provisioning によって再プロビジョニングされます これにより、アクティブな LSP のトラフィックが中断しないようにします。

MPLS-TP トンネルの展開

MPLS-TP サービス要求をプロビジョニングするために必要な最後のステップは、サービス要求の展開です。これにり、サービス要求および関連するコンフィギュレーションの更新がネットワークに適用されます。

（注） DRAFT 状態のサービス要求は、展開できません。

展開機能は、他の Prime Provisioning サービスと同様です。MPLS-TP サービス要求を展開する方法については、「サービス要求の展開」（P.8-10）を参照してください。

デコミッション

MPLS-TP サービス要求のコンフィギュレーションは、Service Request Manager 内のデコミッション機能を使用して、ネットワークから削除できます。デコミッションによって、MPLS-TP トンネル パス内のすべてのトンネル エンドポイントおよびミッドポイント デバイスから、以前に展開されたコンフィギュレーションが削除されます。

1 つ以上のサービス要求をデコミッションするには、第 8 章「サービス要求の管理」を参照してください。

サンプル コンフィグレット

この項に含まれ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

この項のすべてのサンプルでは、MPLS-TP コアの存在を想定しています。

（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。

ここでは、Prime Provisioning での MPLS-TP サービス プロビジョニングのコンフィグレットの例について説明します。

次の項があります。

- 「MPLS-TP 現用トンネルのコンフィグレット（IOS-XR）」（P.6-16）
- 「MPLS-TP 現用トンネルのコンフィグレット（IOS-XR）」（P.6-16）

MPLS-TP 現用トンネルのコンフィグレット（IOS）

設定

- サービス：MPLS-TP 現用トンネル
- 機能：MPLS-TP 対応ノードを設定するための MPLS-TP コンフィグレット（IOS）。

コンフィグレット

IOS デバイスの設定	コメント

エンドポイントのコンフィギュレーション
`interface Tunnel-tp200`
`  description PrimeF:JobID:2(testTunnel)`
`  tp tunnel-name test`
`  tp bandwidth 100`
`  tp source 3.3.3.3 global-id 2`
`  tp destination 1.1.1.1 tunnel-tp 200 global-id 3`
`  bfd BFDTemplate-SingleHopMicrosec-1`
`  working-lsp`
`  lsp-number 0`
`  in-label 8018`
`  out-label 5003 out-link 8`
`  protect-lsp`
`  lsp-number 1`
`  in-label 8019`
`  out-label 50012 out-link 12`
 	
ミッドポイントのコンフィギュレーション
`mpls tp lsp source 3.3.3.3 global-id 2 tunnel-tp 200 lsp working destination 1.1.1.1 global-id 3 tunnel-tp 200`
`  forward-lsp`
`  tp bandwidth 100`
`  in-label 5003 out-label 50011 out-link 10`
`  reverse-lsp`
`  tp bandwidth 100`
`  in-label 5004 out-label 8018 out-link 8`
 	
エンドポイントのコンフィギュレーション
`interface Tunnel-tp200`
`  description PrimeF:JobID:2(testTunnel)`
`  tp tunnel-name test`
`  tp bandwidth 100`
`  tp source 1.1.1.1 global-id 3`
`  tp destination 3.3.3.3 tunnel-tp 200 global-id 2`
`  bfd BFDTemplate-SingleHopMicrosec-1`
`  working-lsp`
`  lsp-number 0`
`  in-label 50011`
`  out-label 5004 out-link 10`
`  protect-lsp`
`  lsp-number 1`
`  in-label 50012`
`  out-label 8019 out-link 12`
	`Create an MPLS-TP working tunnel with endpoint and midpoint nodes. This involves configuring the settings on each node in the tunnel.`
	
	`Create an MPLS-TP working tunnel with the following attributes:`
	
	`Endpoint 1:`
	`- tp tunnel name: test`
	`- Source: 3.3.3.3`
	`- Destination 1.1.1.1`
	`- Bandwidth 100 kbps`
	`- bfd BFDTemplate-SingleHopMicrosec-1`
	`- Working LSP configuration`
	`- Protect LSP configuration`
	
	`Midpoint:`
	`- Source: 3.3.3.3`
	`- Destination 1.1.1.1`
	`- Bandwidth 100 kbps`
	`- Forward LSP configuration`
	`- Reverse LSP configuration`
	
	`Endpoint 2:`
	`- tp tunnel name: test`
	`- Source: 1.1.1.1`
	`- Destination 3.3.3.3`
	`- Bandwidth 100 kbps`
	`- bfd BFDTemplate-SingleHopMicrosec-1`
	`- Working LSP configuration`
	`- Protect LSP configuration`

MPLS-TP 現用トンネルのコンフィグレット（IOS-XR）

設定

- サービス：MPLS-TP 現用トンネル
- 機能：MPLS-TP 対応ノードを設定するための MPLS-TP コンフィグレット（IOS-XR）。

コンフィグレット

IOS-XR デバイス設定	コメント

エンドポイントのコンフィギュレーション
`interface tunnel-tp0`
`  description PrimeF:JobID:2 (testTunnel)`
`  source 3.3.3.3`
`  destination 1.1.1.1 global-id 8 tunnel-id 1`
`  working-lsp`
`  in-label 36`
`  out-label 23 out-link 12`
`  lsp-number 0`
`  protect-lsp`
`  in-label 37`
`  out-label 33 out-link 100`
`  lsp-number 1`
`  bfd`
`  min-interval 50`
`  min-interval standby 50`
`  multiplier 3`
 	
ミッドポイントのコンフィギュレーション
`mpls traffic-eng tp`
`  mid 3.3.3.3_1_protect_3.3.3.4_0`
`  source 3.3.3.3 tunnel-id 1 global-id 8`
`  destination 1.1.1.1 tunnel-id 0 global-id 80`
`  forward-lsp`
`  in-label 32 out-label 37 out-link 100`
`  reverse-lsp`
`  in-label 33 out-label 24 out-link 10`
 	
エンドポイントのコンフィギュレーション
`interface tunnel-tp1`
`  description PrimeF:JobID:2(testTunnel)`
`  source 1.1.1.1`
`  destination 3.3.3.3 global-id 80 tunnel-id 0`
`  working-lsp`
`  in-label 23`
`  out-label 36 out-link 4`
`  lsp-number 0`
`  protect-lsp`
`  in-label 24`
`  out-label 32 out-link 10`
`  lsp-number 1`
`  bfd`
`  min-interval 50`
`  min-interval standby 50`
`  multiplier 3`
	Create an MPLS-TP working tunnel with endpoint and midpoint nodes. This involves configuring the settings on each node in the tunnel.
	
	Create an MPLS-TP working tunnel with the following attributes:
	
	Endpoint 1:
	- tp tunnel name: test
	- Source: 3.3.3.3
	- Destination 1.1.1.1
	- Bandwidth 100 kbps
	- Working LSP configuration
	- Protect LSP configuration
	
	Midpoint:
	- Source: 3.3.3.3
	- Destination 1.1.1.1
	- Bandwidth 100 kbps
	- Forward LSP configuration
	- Reverse LSP configuration
	
	Endpoint 2:
	- tp tunnel name: test
	- Source: 1.1.1.1
	- Destination 3.3.3.3
	- Bandwidth 100 kbps
	- Working LSP configuration
	- Protect LSP configuration

CHAPTER 7

MPLS トラフィック エンジニアリング サービスの管理

この章には、さまざまな機能、GUI、およびさまざまなトラフィック エンジニアリング管理タスクを実行するために必要な手順を含む『Cisco Prime Provisioning Traffic Engineering Management』（TEM）製品の詳細な説明が記載されています。

この章の内容は、次のとおりです。

スタートアップ

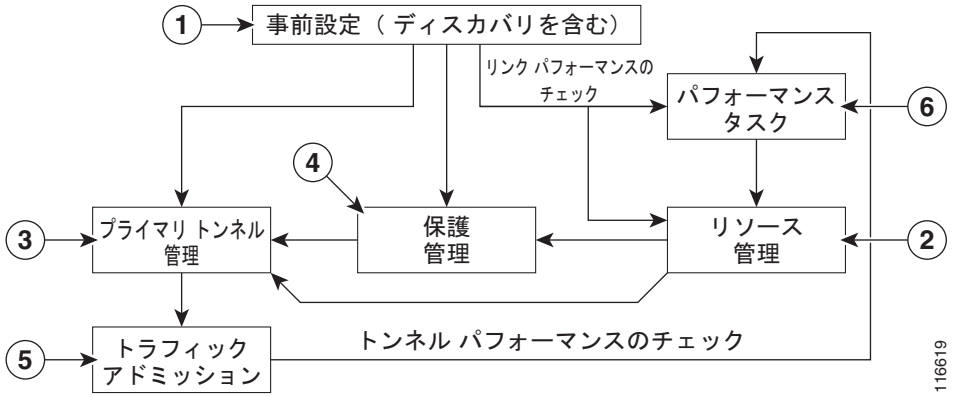
ここでは、Prime Provisioning のインストール手順について説明します。Cisco Prime Provisioning（Prime Provisioning）の一般的なインストール手順は、*『Cisco Prime Provisioning 6.3 Installation Guide』* で説明しています。

内容は次のとおりです。

プロセスの概要

TEM の主要なコンポーネントとフローは、図 7-1 に示されています。

図 7-1　TEM の主要なプロセス フロー

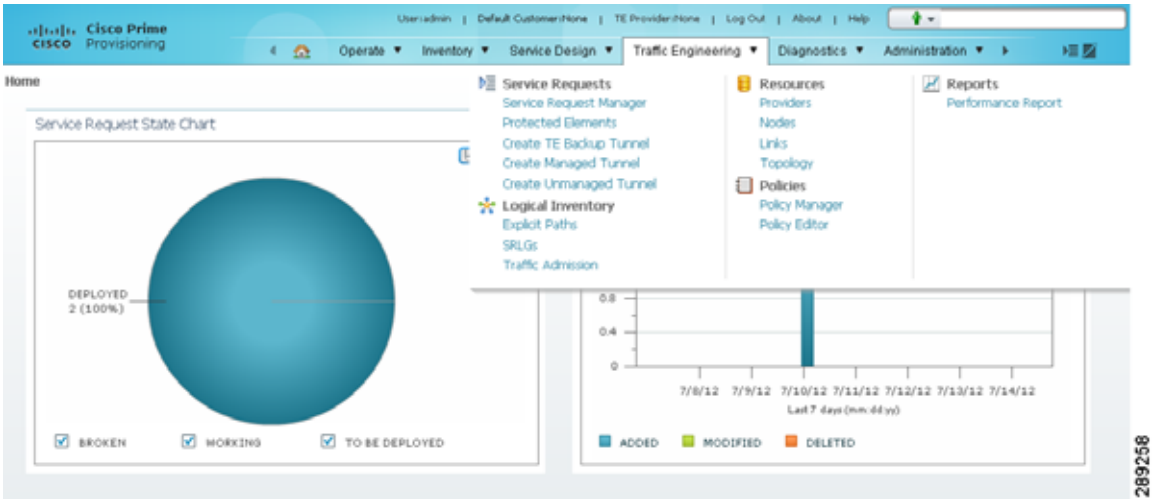


この図には、次のコンポーネントが含まれています。

1. 事前設定：システムで TE ネットワーク情報を収集してから（TE ディスカバリ）、選択したネットワークに TE 設定を導入できるようにする主要パラメータを設定します。（「スタートアップ」（P.7-1）を参照）
2. リソース管理：TE インターフェイスの特定のプロパティを調整してトンネル配置を最適化します。（「TE リソース管理」（P.7-21）を参照）
3. プライマリ トンネル管理：管理対象外（「基本的なトンネル管理」（P.7-28）を参照）または管理対象のプライマリ トンネルを作成および管理します。（「基本的なトンネル管理」（P.7-28）または「高度なプライマリ トンネル管理」（P.7-46）を参照）
4. 保護管理：ネットワークの選択された要素（リンク、ルータ、または SRLG）を障害から保護します。（「高度なプライマリ トンネル管理」（P.7-46）を参照）
5. トラフィック アドミッション：トラフィックをトラフィック エンジニアリングされたトンネルに割り当てます。（「TE トラフィック アドミッション」（P.7-68）を参照）
6. パフォーマンス タスク：簡易ネットワーク管理プロトコル（SNMP）を使用してインターフェイスおよびトンネルの帯域使用率を計算します。（「管理機能」（P.7-72）を参照）

Prime Provisioning ユーザ インターフェイスの [Traffic Engineering] メニューのオプションを図 7-2 に示します。

図 7-2　[Traffic Engineering] メニューのオプション



前提条件と制限事項

現在のリリースの Prime Provisioning には、ここで説明する一定の前提条件および制限事項があります。

一般的なシステムの推奨事項については、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください。

一般的な制限事項

Prime Provisioning の現在のリリースには、次の制限事項があります。

- Prime Provisioning の同時実行ユーザは現在の実装の計画部分でサポートされますが（「複数の同時実行ユーザ」（P.7-118）の項を参照）、ブラウザ セッション属性の制限のため、同じマシンで複数のブラウザを使用することは推奨されません。
- Java アプリケーションおよびアプレットを起動するには、クライアント コンピュータに JRE バージョン 1.6.0_07 以上をインストールする必要があります。これは、Java のコントロール パネルから行えます。Java をまだインストールしていない場合は、[Topology Tool] ページにあるリンクを使用して、Prime Provisioning にバンドルされているバージョンをインストールできます。
- ISC 4.1 リリースよりも前のリポジトリを使用していて、4.1 以降のリポジトリにアップグレードした場合は、サービス要求を展開する前に TE 検出タスクを実行してデバイスからソフトウェア バージョン情報を収集する必要があります。
- 競合を回避するために他のサービス要求を発行する前に、発行されたサービス要求の展開を完了します。この詳細は、トンネル プロビジョニングの項で説明されています。

機能固有の注意事項および制限事項

Prime Provisioning には、次のような機能固有の前提条件と制限事項があります。

- 一部の機能は、特定のライセンスがある場合に限り使用できます。また、ライセンスで提供されるノードの数により、ネットワークのサイズが制限されます。詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- TE ディスカバリ タスクに関連する固有の要件は多数あります。これらについては、「TE ディスカバリの前提条件と制約事項」（P.7-13）に記載されています。
- Prime Provisioning は、単一の OSPF エリアまたは IS-IS レベルを管理します。
  Prime Provisioning は複数の OSPF エリアもサポートしますが、エリア間のトンネルを検出しません。各 OSPF エリアは単一の TE プロバイダーマッピングされ、エリアごとに別々に検出されます。
- Prime Provisioning は、ポイントツーポイント リンクを使用した MPLS-TE トポロジのみをサポートします。

シスコ デバイス以外のデバイスおよび TEM

Prime Provisioning では、シスコ デバイス以外のデバイスを管理せず、Prime Provisioning は、そのようなデバイスのプロビジョニングに使用できません。

ただし、Prime Provisioning では、シスコ デバイス以外のデバイスを検出してリポジトリに格納します。これらのデバイスを通過するトンネルを設定でき、消費される帯域幅を算入できますが、デバイスのこれ以外の側面は Prime Provisioning によって管理されません。シスコ デバイス以外のデバイスを始点とする TE トンネルは検出されません。

Prime Provisioning GUI のさまざまな部分のさまざまな属性のソートを実行できます。ただし、シスコ デバイス以外のデバイスに対して追加されたサポートのため、[TE Nodes List] ウィンドウの [Device Name] と [MPLS TE ID] に対してソートを実行できません。

サポートされるプラットフォーム

サポートされるデバイスと IOS プラットフォームについては、*『Cisco Prime Provisioning 6.3 Installation Guide』*を参照してください。

エラー メッセージ

Prime Provisioning で TE 計画ツールを使用するときに呼び出される違反と警告は、「警告および違反」（P.7-102）に記載されています。

Prime Provisioning で展開を実行したときに、次のような Elixir 警告メッセージが表示されることがあります。

```
WARNING Elixir.ServiceBlade Unable to load support matrix for the platform or platform
family. The default support matrix is loaded instead for role: TunnelHead.
WARNING Elixir.ConfigManager Attribute - lockdown of Command - Tunnel_PathOption can NOT
be retrieved from the input SR - SKIPPING.
```

ただし、展開は正常に行われ、警告メッセージは無視しても安全です。

事前設定処理の概要

事前設定処理により、システムが TE ネットワーク情報を収集し、選択されたネットワークで TE 設定を展開することを可能にする主要なパラメータが設定されます。

図 7-3 で強調表示されたボックスは、事前設定処理が Prime Provisioning のどこで行われるかを示しています。

図 7-3　Prime Provisioning プロセス図：事前設定

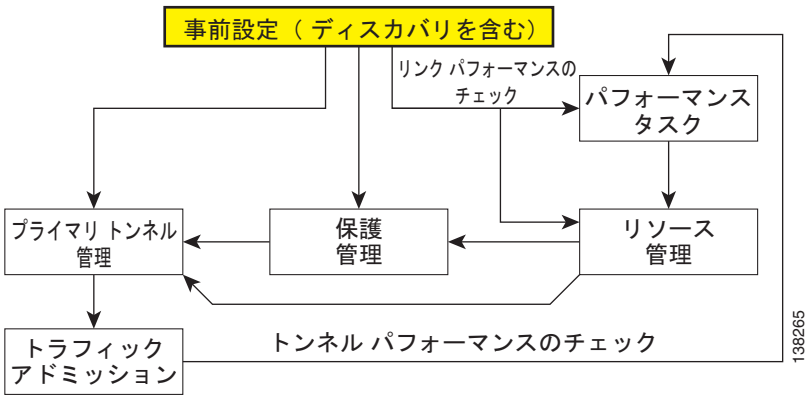
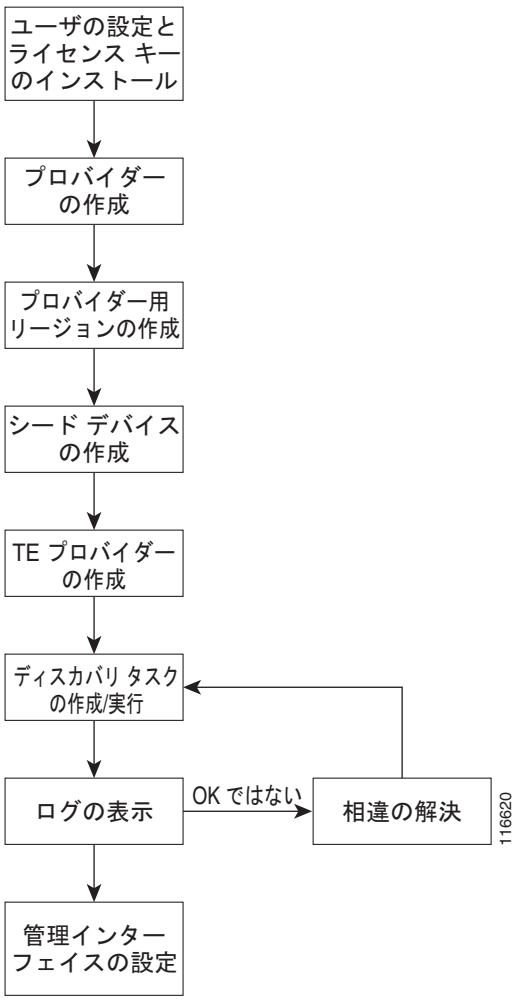


図 7-4 には、事前設定処理の異なる手順が示されています。

図 7-4　事前設定処理



事前設定処理を開始する前に、デバイスの TE ID として使用される IP アドレスに、管理ステーションから正常にアクセスできることを確認することにより、ネットワーク デバイスで MPLS-TE をイネーブルにする必要があります（このステップは TEM によってサポートされていません）。

事前設定処理は、次の手順から構成されます。

1. **新規ユーザの設定およびライセンス キーのインストール**：Prime Provisioning の TEM 機能を実行するには、新規ユーザの作成とライセンス キーのインストールが必要です。これらのキーにより、Prime Provisioning を使用して TE トンネルとリソースを表示および管理できるようになります。（「TEM のセットアップおよびインストール」（P.7-7）を参照）
2. **プロバイダーの作成**：プロバイダーは、複数のオペレータが Prime Provisioning で同時に作業を行えるように設計された概念です（各プロバイダーは異なるネットワークで作業します）。したがって、各プロバイダーを定義してさらにシステムで作業するために参照オペレータとして使用する必要があります （プロバイダーを作成するには、「プロバイダー」（P.2-15）を参照してください）。
3. **プロバイダーのリージョンの作成**：単一のプロバイダーは複数のネットワークを使用できるため、リージョンが重要になります。そのような環境に対応するために、リージョンはさらなる細分化のレベルとして使用されます。（リージョンを作成するには、「プロバイダー リージョン」（P.2-17）を参照してください）。

4. **シード デバイスの作成**：この IOS または IOS XR デバイスは、TE 検出のためのシード ルータになります。ネットワーク ディスカバリ プロセスでは、MPLS TE ネットワーク トポロジを検出するための初期通信ポイントとしてシード ルータを使用します （シード ルータを作成するには、「デバイス」（P.2-1）を参照してください）。
5. **TE プロバイダーの作成**：ネットワークで MPLS TE をサポートしているプロバイダーは、TE プロバイダーとして定義できます。TE ネットワークを管理できるようにするには、TE プロバイダーを作成する必要があります。特定のネットワークに関連付けられたすべての TE 関連データは、一意な TE プロバイダーの下に格納されます。プロバイダーとリージョンは、TE プロバイダーを一意に定義します（「TE プロバイダーの作成」（P.7-8）を参照）。
6. **TE ディスカバリ タスクの実行**：プライマリ トンネルとバックアップ トンネルを作成するために、リポジトリに入力する特定の TE プロバイダーの TE ネットワークを検出します。（「TE ネットワーク検出」（P.7-11）を参照）。
7. **管理インターフェイスの設定**：検出されたデバイスの管理インターフェイスを設定するか、検出されたすべてのデバイスに対する解決方法でサーバ ホスト ファイルを更新します。TE ネットワーク内のデバイスにホスト名でアクセスできない場合にだけ、このステップが必要です（「管理インターフェイスの設定」（P.7-20）を参照）。

（注） シード ルータと通信するために Telnet が選択された場合は、他のネットワーク デバイスにも Telnet を使用する必要があります。同様に、シード ルータに対して SSH が選択された場合、SSH は他のすべてのデバイスに使用する必要があります。

TEM のセットアップおよびインストール

Prime Provisioning を設定する前に、Prime Provisioning ソフトウェアをインストールする必要があります。これを行うには、*『Cisco Prime Provisioning 6.3 Installation Guide』*を参照してください。

新規 Prime Provisioning ユーザを設定する場合は、TE ロールを持つユーザを 1 つ以上作成する必要があります。ステップバイステップの説明については、*『Cisco Prime Provisioning 6.3 Administration Guide』*を参照してください。

ライセンスのインストールに必要な Prime Provisioning ライセンス オプションと手順を含むライセンス情報については、*『Cisco Prime Provisioning 6.3 Administration Guide』*を参照してください。

DCPL プロパティの編集（任意）

Prime Provisioning Dynamic Component Properties Library（DCPL）には、GUI からアクセスできるさまざまなプロパティが含まれます。これらのプロパティの一部は変更できます。

警告 **影響を十分に理解していない限り、DCPL プロパティの変更を試みないでください。**

Prime Provisioning の GUI で、DCPL プロパティは [Administration] > [Hosts] にあります。特定のホストのチェックボックスをオンにして、[Config] ボタンをクリックします。

TEM に関する DCPL プロパティは、次のフォルダにあります。

- [Provisioning] > [Service] > [TE]
- TE

- TE Topology

TE プロバイダーの作成

TE 検出または TE データの操作を行う前に、TE プロバイダーを少なくとも 1 つ作成する必要があります。たとえば、OSPF エリアは TE プロバイダーとして割り当てることができます。これよりも前に、プロバイダーおよびプロバイダー用のリージョンが設定されている必要があります（「事前設定処理の概要」（P.7-4）を参照）。

検出されたルータの場所であるデフォルト リージョンとして、1 つのリージョンを割り当てることができます。これらのルータは、後に任意のリージョンに配置できます。詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* の複数のホストの項を参照してください。

TE プロバイダーを作成するには、次のステップを実行します。

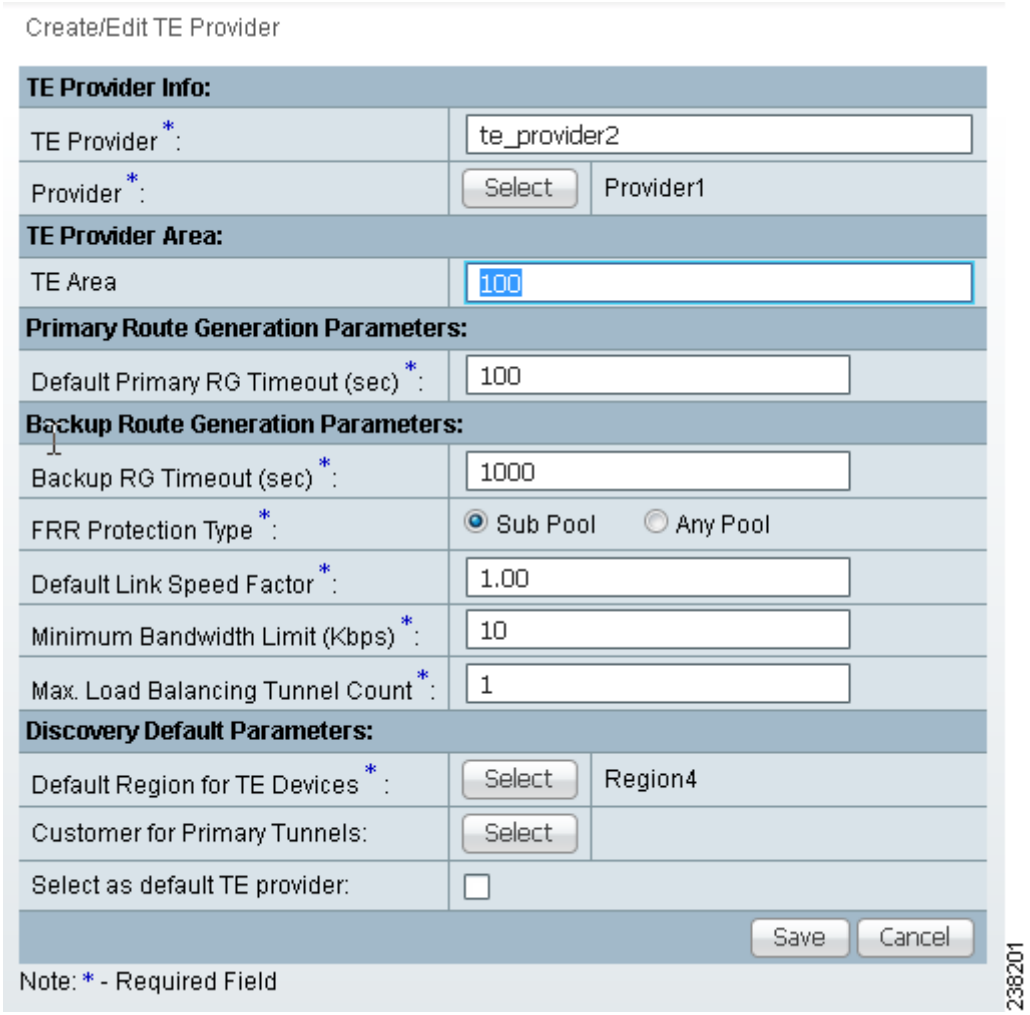
ステップ 1　[Traffic Engineering] > [Providers] を選択します。

[TE Providers] 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 TE をプロバイダーを作成します。

[Create/Edit TE Provider] 図 7-5 ウィンドウが表示されます。

図 7-5　Create/Edit TE Provider



[Create/Edit TE Provider] ウィンドウには、次のフィールドが含まれています。

- [TE Area]：TE プロバイダーに割り当てられた OSPF エリア。これは、0 ～ 4294967295 の正の整数または x.x.x.x 形式のドット表記アドレスにすることができます。ここで、x は 0 ～ 255 の間の数値です。
- [Default Primary RG Timeout]：プライマリ トンネルに対するデフォルトの計算タイムアウト。
- [Backup RG Timeout]：バックアップ トンネルの要素あたりの計算のタイムアウト（各保護対象要素に対して、タイマーは、Prime Provisioning が保護を試みる前にゼロにリセットされます）。
- [FRR Protection Type]：Fast Re-Route（FRR）保護タイプ。
  - [Sub Pool]：サブ プールのプライマリ トンネルだけを保護します。
  - [Any Pool]：サブ プールとグローバル プールの両方のプライマリ トンネルを保護します。

  プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。

- [Default Link Speed Factor]：影響を受けるトンネルを移動するためにリンク速度に適用するデフォルト増倍係数。これは保護する必要があります。リンクの帯域幅は、リンク速度係数によって乗算され、リンクのために予約された RSVP 帯域幅（FRR 保護タイプによって、サブ プールまたはグローバル プール）が差し引かれます。算出された帯域幅は、FRR バックアップ トンネルに使用できます。

  リンク速度係数の解釈：

  1.0 よりも大きい（オーバーブッキング）：リンクよりも多くのバックアップ帯域幅を使用できます。

  1.0 よりも小さい（アンダーブッキング）：リンクよりも少ないバックアップ帯域幅を使用できます。

- [Minimum Bandwidth Limit]：バックアップ トンネルで許可される最小帯域幅。
- [Max. Load Balancing Tunnel Count]：保護対象要素を通じてフローを保護するために必要なバックアップ トンネルの最大数です。ここでは、フローは次のように定義されます。

  保護対象リンクには、2 つのフローがあります（トラフィックのフローが可能な方向ごとに 1 つ）ノードの場合、フローの数は特定のノードのネイバー ノードの数によって決まります。フローは、ネイバー ペアごとに 1 つです。したがって、3 台のネイバー、A、B、および C があるノードには、そのノードを通過する 6 つのフローがあります（A->B、A->C、B->A、B->C、C->A、C->B）

- [Default Region for TE Devices]：デフォルト プロバイダー リージョンは、TE ディスカバリによって、新しく検出されたデバイスに割り当てられます。デバイスがリポジトリにすでに存在し、リージョンが定義されている場合、TE ディスカバリでは、その設定が維持されます。TE ディスカバリ後に、デバイスのリージョンを変更できます。
- [Customer for Primary Tunnels]：プライマリ TE トンネルのカスタマーの名前。

ステップ 3　[TE Provider] フィールドに新規 TE プロバイダーの名前を入力します。

ステップ 4　この TE プロバイダーとしてプロバイダーを選択するには、[Provider] フィールドの隣の [Select] ボタンをクリックします。

[Select Provider] ウィンドウが表示されます。

ステップ 5　オプション ボタンを使用して必要なプロバイダーを選択するか、プロバイダー名に一致する検索基準でプロバイダーを検索し、[Find] をクリックします。

ステップ 6　[Select] をクリックして必要なプロバイダーを選択します。

[Select Provider] ウィンドウが閉じます。選択されたプロバイダー名が、[Provider] フィールドに表示されます。

ステップ 7　[TE Area] フィールドに、TE エリアとして使用する OSPF エリアの番号を指定します。

エリア ID では、ドット表記と 10 進表記の両方がサポートされます。

（注）　TE ディスカバリに使用されるシード ルータがエリア境界ルータでなく、検出時に自動的に読み込まれる場合は、[TE Area] フィールドを空にできます。

TE 検出に使用されるシード ルータに応じて、エリア ID を次のように設定する必要があります。

- **シード ルータが ABR である場合：**TE プロバイダーのエリア ID フィールドが ABR の 2 つ以上のエリアのどれを検出するかを示すよう設定する必要があります。
- **シード ルータが ABR でない場合：**空にします。

（注）　[TE Provider] にエリア ID を設定しなかった場合は、TE ディスカバリによって設定されます。エリア ID は、設定後に変更できません。

ステップ 8　プライマリおよびバックアップのルート生成パラメータを追加します。

FRR（Fast Re-Route）保護タイプがサブ プールと同じである場合、ツールにより生成されたバックアップ トンネルはサブ プール プライマリ トンネルのみを保護します。[Any Pool] の場合、ツールによって生成されるバックアップ トンネルでは、サブプールおよびグローバル プールの両方のプライマリ トンネルを保護します。

Fast Re-Route（FRR）保護プールの詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）で、帯域幅プールの項を参照してください。

ステップ 9　残りの必須フィールド（「*」とマークされたフィールド）と、必要に応じてオプション フィールドに値を入力します。

ステップ 10　必須の [Default Region for TE Devices] フィールドで、対応する [Select] ボタンをクリックします。

[Region for Create TE Provider] ウィンドウが表示されます。

ステップ 11　オプション ボタンを使用して必要なリージョンを選択します。

ステップ 12　[Select] をクリックして必要なデフォルト リージョンを選択します。

[Region for Create TE Provider] ウィンドウが閉じます。選択されたリージョン名が [Default Region for TE Devices] フィールドに表示されます。

ステップ 13　オプションの [Customer for Primary Tunnels] フィールドで、対応する [Select] ボタンをクリックします。

[Customer for Create TE Provider] ウィンドウが表示されます。

ステップ 14　必要な場合は、オプション ボタンを使用してカスタマーを選択するか、[Show Customers with Customer Name matching] フィールドにカスタマー検索基準を入力してカスタマーを検索し、[Find] をクリックします。

ステップ 15　[Select] をクリックして必要なカスタマーを選択します。

[Select Customer for Create TE Provider] ウィンドウが閉じます。選択されたカスタマー名が、[Create/Edit TE Provider] ウィンドウの [Customer for Primary Tunnels] フィールドに表示されます。

ステップ 16　[Save] をクリックします。

作成された TE プロバイダーは、[TE Provider] ウィンドウに表示され、TE 検出と他の TE 機能を実行するために使用できるようになります。

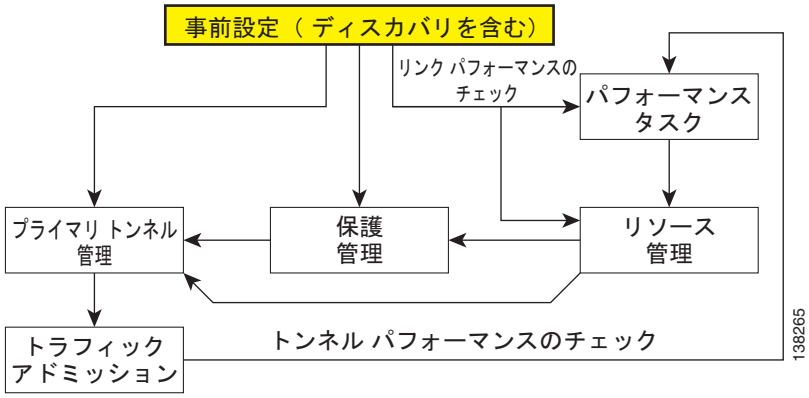
TE プロバイダーを切り替えるには、メニュー ツールバーの上の Prime Provisioning ウィンドウの上部に移動し（図 7-2）、[TE Provider] リンクをクリックします。

TE ネットワーク検出

事前設定処理を完了し、シード ルータの作成を終えれば、特定の TE プロバイダーの TE ネットワークを検出できます。これによって、ネットワーク トポロジがリポジトリに入力されます。また、管理インターフェイスの設定が必要になる場合があります。必要なステップについては、この項で説明します。

図 7-3 で強調表示されているボックスは、Prime Provisioning で行う事前設定のステップを示しています。

図 7-6　Prime Provisioning プロセス図：事前設定



TE 検出プロセスの目的は、TE トポロジ、TE トンネル、明示的パス、およびライブ ネットワークに存在するトンネルへのスタティック ルートをリポジトリに入力することです。

TE 検出プロセスでは、Telnet または SSH のいずれかを使用している MPLS TE ネットワーク トポロジを検出するためにシード デバイスを使用します。ネットワーク内のすべてのトラフィック エンジニアリング ルータは、TE ID を介してアクセス可能にする必要があります。

TE ディスカバリは、1 回または定期的に実行できるスケジュール設定可能なタスクです。リポジトリとネットワークの間の不一致は、ディスカバリ ログに報告されます。サービス状態の情報は、ラベル スイッチド パス（LSP）のログを記録し、サービス要求（SR）状態を更新することにより、段階的に更新されます。

ここでは、次の内容について説明します。

TE ディスカバリの前提条件と制約事項

次の前提条件は、主に TE 検出に適用されます。

一般的な Prime Provisioning の前提条件と制約事項については、「前提条件と制限事項」（P.7-3）を参照してください。

TE 検出の TE ルータへアクセス

TE ディスカバリ タスクを正常に実行するには、シード ルータに管理ステーションから直接アクセスできる必要があります。

すべての TE ルータは、Prime Fulfillment マシンから TE ルータ ID を介してアクセスできる必要があります。多くの場合、これはループバック IP アドレスですが、常にそうであるわけではありません。

Telnet/SSH では、『Cisco Prime Provisioning Traffic Engineering Management』（TEM）管理ステーションから各デバイスへの直接 Telnet/SSH アクセスが必要です。

シード ルータの設定時に Telnet または SSH を選択する方法の手順については、「事前設定処理の概要」（P.7-4）を参照してください。

（注） TE 検出の実行後、デバイスでの RSVP グレースフル リスタートを手動で再設定しないことを推奨します。これは、データベースとの同期に影響を与え、展開が失敗する可能性があります。この場合、新たに TE 検出を実行する必要があります。

大規模ネットワークでのメモリの不足

大規模ネットワーク（250 以上のデバイスまたは 5000 以上のトンネルなど）で TE ディスカバリを実行している場合、または OutOfMemoryException が発生した場合は、メモリ設定を変更することを推奨します。

これを行うには、次のステップを実行します。

ステップ 1　[Administration] > [Hosts] を選択します。

ステップ 2　ホストを選択し、[Config] ボタンをクリックします。

ステップ 3　[watchdog] > [server] > [worker] > [java] > [flags] を選択します。

ステップ 4　プロパティ文字列の最初の部分を変更します。たとえば、デフォルト値 **-Xmx512m** の代わりに **-Xmx1024m** に変更します。

これにより、**TE 検出**タスクのヒープ サイズが増加し、これにより、OutOfMemoryException の問題が解決します。

ステップ 5　**watchdog.server.worker.java.flags** プロパティを元の値に戻し、不要になったときにリソース使用率を減らします。

（注） または、**vpnsc.properties** ファイルの **watchdog.server.worker.java.flags** プロパティを編集することにより、同様にメモリの増加を実現することができます。

IOS XR およびイネーブル パスワード

IOS XR デバイスをシード デバイスとして使用している場合、IOS XR 自体はイネーブル パスワードを必要としませんが、イネーブル パスワードをデバイス レコードに設定する必要があります。このように、ネットワーク内の IOS デバイスは、イネーブル パスワードを必要としませんが、完全に検出することができます。

初期ディスカバリのシード デバイスとして機能する IOS XR デバイスを [Devices] タブ（[Inventory] > [Devices]）から作成する場合は、イネーブル パスワードを指定する必要はありません。TEM では、ログイン可能であり、必要なすべてのデータを取得できます。

ただし、同じネットワークに他の IOS デバイスがある場合、TEM はこれらのデバイスのイネーブル モードを開始できません。その結果、イネーブル モードを開始できないために TEM で収集できない関連データがあるという意味で、これらのデバイスのディスカバリは完全ではありません。これらの他の IOS ルータは、[Devices] ウィンドウでは [unknown] デバイスとして表示されます。

制限事項

同じ TE プロバイダーの同時 TE ディスカバリはサポートされていません。TE プロバイダーごとに、一度に 1 人のユーザのみが TE ディスカバリ タスクを実行できます。

TE 検出タスクの作成

タスク マネージャでは、次の 2 つのタイプの TE ディスカバリ タスクを実行できます。

- 「TE 増分ディスカバリ」（P.7-14）
- 「TE フル ディスカバリ」（P.7-15）

TE 増分ディスカバリ

比較的大きい OSPF エリアで、この再ディスカバリ プロセスは、完了までに長い時間がかかる場合があります。

TE 増分ディスカバリでは、ディスカバリ タスクは、新しいデバイスまたはリンクの追加など、ネットワークで変更が発生するたびに漸次的に実行されます。このため、TE フル ディスカバリよりも、メモリ オーバーヘッドがはるかに小さくなります。

TE ネットワーク上で TE 検出タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

[Task Manager] ウィンドウが表示されます。

ステップ 2　[Create] > [TE Incremental Discovery] を選択します。

[Task Creation] ウィザードが開きます。

ステップ 3　（任意）[Name] および/または [Description] フィールドを変更し、[Next] をクリックします。

[TE Provider] ウィンドウが表示されます。

ステップ 4　TE プロバイダーを選択し、[Next] をクリックします。

[Device/Link Discovery Information] ウィンドウが表示されます。

次のいずれかの操作を実行できます。

- デバイス ディスカバリ：ネットワークに追加された新しいデバイスは、デバイス ディスカバリを使用して検出できます。デバイス ディスカバリでは、シスコ以外のデバイス（ある場合）は、リストから除外されます。

  デバイスは、[Select] ボタンをクリックして選択できます（インベントリに追加されたデバイスのリストが表示されます）。

  ここで、検出する必要があるデバイスは、その管理 IP アドレスとともに追加する必要があるという前提条件があります。デバイスのクレデンシャルは、リポジトリにすでに入力されている他のデバイスのクレデンシャルと同じである必要はありません。デバイスは、TE プロバイダーと同じ OSPF エリアに含まれる場合に限り、検出に成功します。

- リンク ディスカバリ：ネットワークに追加された新しいリンクは、リンク ディスカバリを使用して検出できます。明示的パス、リンクを通過するプライマリおよびバックアップ トンネルも検出されます。

  すでに TE ノードである [End Device A] および [End Device B] をデバイスのリストから選択できます。[Interface A] および [Interface B] を指定する必要があります。

ステップ 5　ネットワークを検出するためのシード デバイスを選択し、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 6　次の 2 つの方法のいずれかでタスク スケジュールを作成します。

- すぐに実行するタスクをスケジュールする場合は、[Now] をクリックします。この場合、スケジュール情報が [Task Schedules] のリストに自動的に入力されます。
- このタスクのスケジューラを作成するには、[Create] をクリックします。この場合、[Task Schedule] ウィンドウが表示されます。

ステップ 7　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

（注）　デフォルト設定では、単一の **TE ディスカバリ タスク**をすぐに実行します（[Now]）。

ステップ 8　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 9　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 10　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

TE フル ディスカバリ

TE フル ディスカバリでは、ディスカバリ タスクは、すべてのデバイスが検出されるまで停止せずに動作します。

TE ネットワーク上で TE 検出タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

[Task Manager] ウィンドウが表示されます。

ステップ 2　[Create] > [TE Full Discovery] を選択し、新しいタスクを作成します。

[Create Task] ウィンドウが表示されます。

ステップ 3　（任意）[Name] および/または [Description] フィールドを変更し、[Next] をクリックします。

[Select TE Provider] ウィンドウが表示されます。

ステップ 4　TE プロバイダーを選択し、[Next] をクリックします。

[Select Seed Device] ウィンドウが表示されます。シスコ以外のデバイス（ある場合）は、リストから除外されます。

ステップ 5　ネットワークを検出するためのシード デバイスを選択し、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 6　次の 2 つの方法のいずれかでタスク スケジュールを作成します。

- すぐに実行するタスクをスケジュールする場合は、[Now] をクリックします。この場合、スケジュール情報が [Task Schedules] のリストに自動的に入力されます。
- このタスクのスケジューラを作成するには、[Create] をクリックします。この場合、[Task Schedule] ウィンドウが表示されます。

ステップ 7　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

（注）　デフォルト設定では、単一の **TE ディスカバリ タスク**をすぐに実行します（[Now]）。

ステップ 8　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 9　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 10　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

エリア別ディスカバリの管理

エリア別 TE ディスカバリを実行する前に、Prime Provisioning による複数 OSPF エリアの管理方法を理解することは有益です。

このトピックの背景情報については、「トラフィック エンジニアリング管理の概念」（P.7-115）で複数の OSPF エリアの項を参照してください。

このセクションでは、次の操作について説明します。

- 「エリア別 TE 検出の実行」（P.7-16）
- 「ABR を使用したエリア別 TE 検出の実行」（P.7-17）。

エリア別 TE 検出の実行

選択した TE プロバイダーがある領域に対して TE ディスカバリを実行すると、その領域に関連付けられたすべてのトンネルおよび明示的パスが Prime Provisioning データベースにインポートされます。

エリア別 TE ディスカバリを開始するには、次のステップを実行します。

ステップ 1　プロバイダーを作成します。

ステップ 2　リージョンを作成します。

ステップ 3　TE プロバイダーを作成します。

ステップ 4　[Devices] ウィンドウからシード デバイスを作成します。

ステップ 5　[Operate] > [Task Manager] > [Create] > [TE Full Discovery] を選択します。

TE ディスカバリ タスクの名前を指定するか、またはデフォルトを受け入れて、[Next] をクリックします。

ステップ 6　TE プロバイダーを選択し、[Next] をクリックします。

ステップ 7　シード デバイスを選択し、[Next] をクリックします。

ステップ 8　TE ディスカバリからスケジュールを選択し、[Next] をクリックします。

ステップ 9　ディスカバリ タスクの要約を確認します。

受け入れ可能な場合は、[Finish] をクリックして、TE ディスカバリプロセスを開始します。

ABR を使用したエリア別 TE 検出の実行

TE プロバイダー設定でエリア識別子が指定されておらず、シード デバイスが ABR の場合、図 7-7 の警告メッセージが表示されて TE 検出が中断し、TE プロバイダーのエリア識別を指定する、または ABR 以外のデバイスをシードとして使用するように通知します。

図 7-7　TE エリア識別子が指定されていない ABR を使用した TE 検出

TE 検出タスクの検証

TE 検出タスクは、次の 4 つの方法で評価できます。

- Task Logs：ネットワークで発生した変更のサマリー ログを表示します。
- TE トポロジ：リポジトリから最新の TE トポロジを表示します。
- ネットワーク要素の表示：トラフィック エンジニアリング管理 GUI で、[TE Nodes]、[TE Links]、[TE Primary Tunnels] などに移動し、特定のネットワーク要素タイプの状態を確認します。
- 検出されたデバイスの状態の表示：[Service Requests] ウィンドウに移動し、検出されたデバイスの状態が想定どおりかどうかを調べます。

Task Logs

TE 検出ログは、ネットワークの状態をキャプチャし、リポジトリの最新のスナップショットと比較します。

TE 検出タスクのタスク ログを表示するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Logs] を選択します。

[Task Logs] ウィンドウが表示されます。

タスクのステータスが [Status] 列に表示されます。これは自動的に更新され、TE 検出プロセスが完了した時間を通知します。

タスクが完了しておらず、[Auto Refresh] が選択されている場合は、完了するまで表は更新を定期的に続行します。

ステップ 2　特定のタスクのログを表示するには、[Operate] > [Task Manager] に移動し、必要なタスクを選択してから、[View Log] ボタンをクリックします。

TE 検出ログのコピーを、図 7-8 から始まる次のスクリーンショットで示します。この最初の例では、TE ディスカバリによってトポロジ内で発見された TE 対応のデバイスとリンクを示します。各デバイスが識別された後に、エラーの特定を容易にするために、各デバイスに対して、一連のデバッグ、情報、警告、およびエラーのログが作成されます。

（注）　次のスクリーンショットに示すネットワークにおける変更の要約を探すには、ログの下部までスクロールしてください。

図 7-8　TE ディスカバリ タスク ログ - 例 1

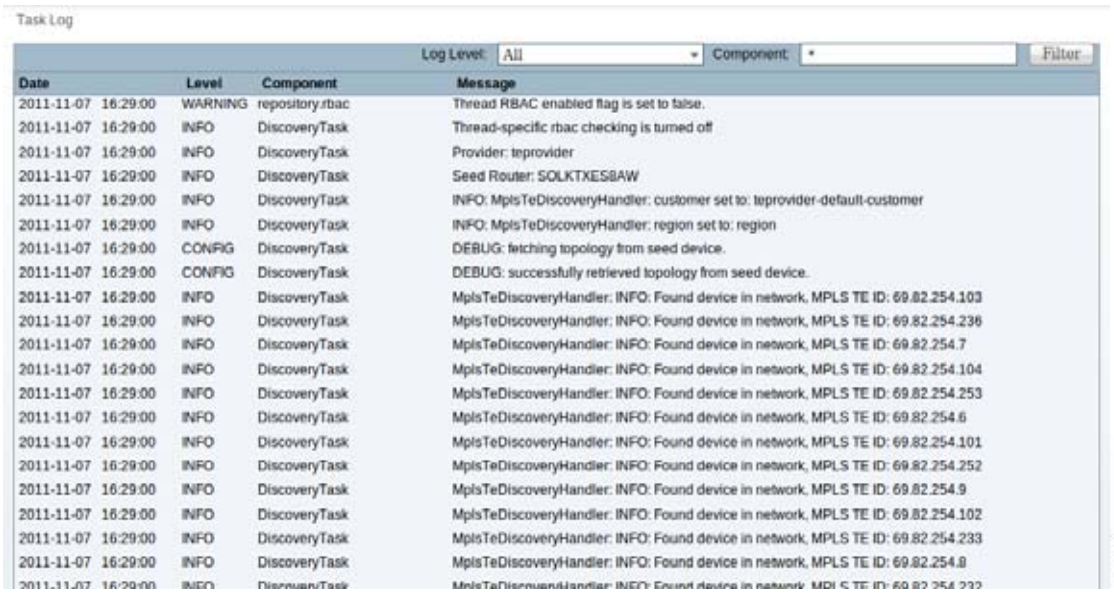


図 7-9 と 図 7-10 には、デバイスのデバッグおよび情報セクションの例を示します。

図 7-9　TE ディスカバリ タスク ログ - 例 2

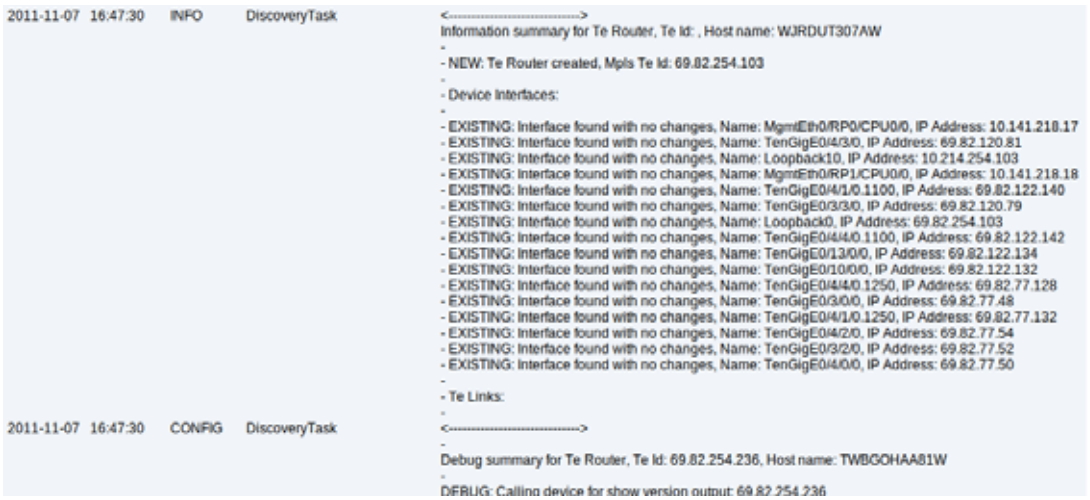
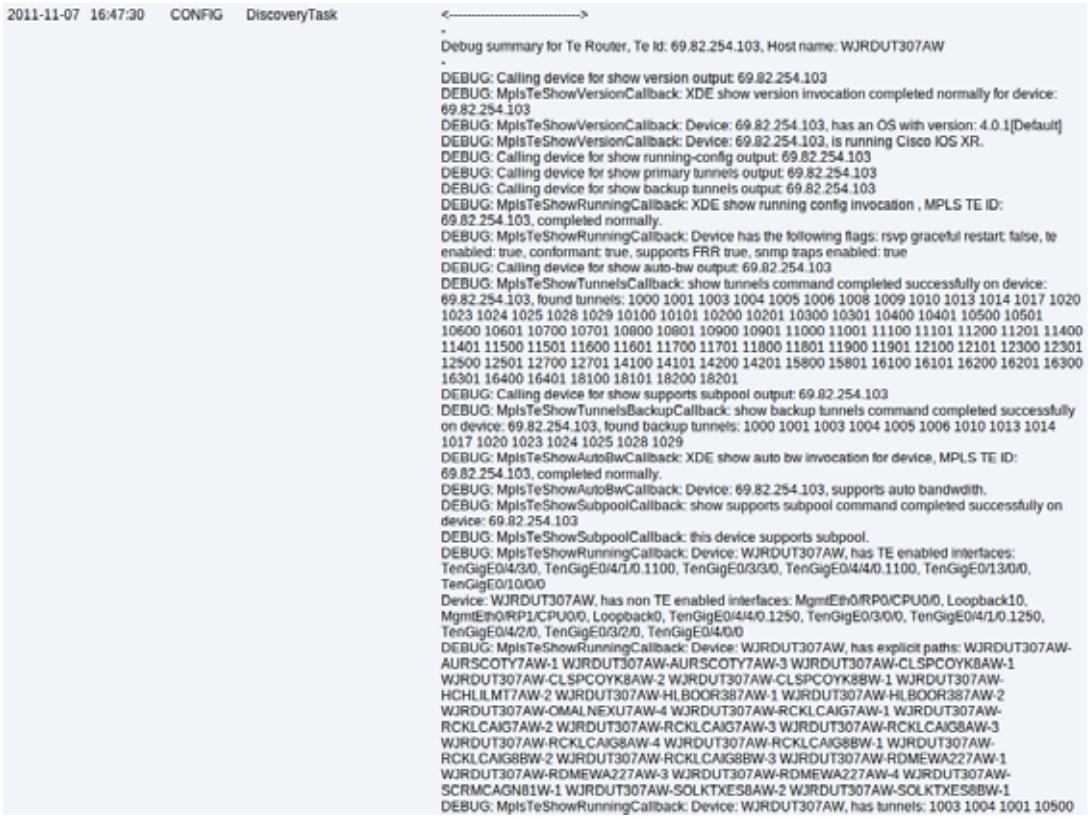


図 7-10　TE ディスカバリ タスク ログ - 例 3



ステップ 3　[Return to Logs] をクリックして、現在のログとオプションを終了し、別のログを開きます。

TE トポロジ

TE トポロジ ツールは、ネットワークの現在の状態の視覚的なスナップショットを提供します。すでにネットワークで行われた変更を判断するために使用することはできません。

ネットワークのトポロジ グラフの生成に必要なステップについては、「TE トポロジ」（P.7-84）を参照してください。

ネットワーク要素の表示

TE ディスカバリを実行した後でネットワークの状態を確認する別の方法は、[Traffic Engineering] メニュー オプションに移動し、確認する要素のタイプを選択することです。

たとえば、TE ディスカバリを実行した後でノードのステータスを確認するには、[Traffic Engineering] > [Nodes] を選択します。TE ノードの更新されたリストを確認し、ネットワーク内のノードを評価します。

[TE Links]、[TE Primary Tunnels]、[TE Backup Tunnels] などについて繰り返します。

管理インターフェイスの設定

トンネル管理操作を開始する前に、管理インターフェイスを設定する必要があります。ただし、このステップは、ネットワーク デバイスが、管理ステーションからホスト名によってアクセスできない場合のみ必要です。

特定のデバイスで管理インターフェイスを設定する方法の詳細については、「デバイス」（P.2-1）を参照してください。

MPLS-TE 管理プロセス

MPLS-TE 管理プロセスには、次のステップが関係します。

1. ネットワーク上で MPLS-TE をイネーブルにし、デバイス TE ID として使用されている IP アドレスが管理ステーションからアクセスできることを確認します（このステップは TEM によってサポートされていません）。
2. MPLS-TE ネットワークの検出するためにリポジトリを準備します。
3. 検出されたデバイスの管理インターフェイスを設定するか、検出されたすべてのデバイスの解決策でサーバ ホスト ファイルを更新します。繰り返しになりますが、ホスト名がすでに管理ステーションからアクセス可能な場合、これは必要ありません。
4. MPLS-TE ネットワークを検出します。

次に、TEM で使用可能な他の MPLR-TE 機能を実行することができます。

（注）　リポジトリが空の場合、または管理 IP アドレスが TE ネットワーク内の現在のデバイスに設定されていない場合、管理ステーションからルータ MPLS TE ID に到達できることを確認してください。つまり、TE 検出プロセスはシード パススルーをサポートしていません。

イーサネット リンクの設定

TEM では、ポイントツーポイント リンクのみサポートされます。POS リンクはデフォルトでポイントツーポイントですが、そうでない場合は、イーサネット リンクをポイントツーポイントとして設定する必要があります。

IOS の場合は、次のコマンドを入力します。

```
(config-if)# ip ospf network point-to-point
```

IOS XR の場合は、次のコマンドを入力します。

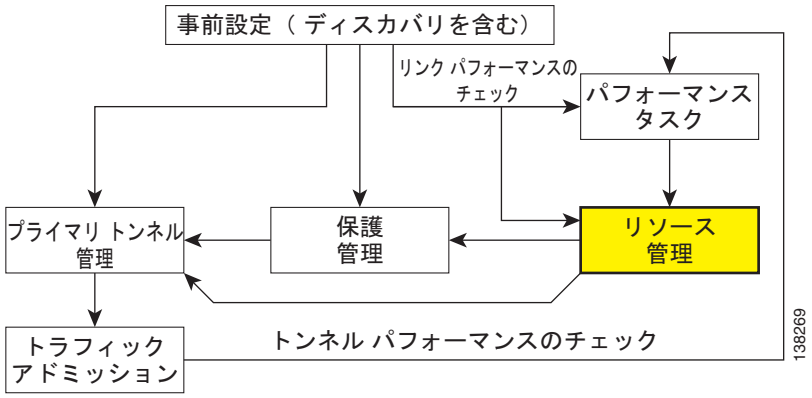
```
# router ospf <id> area <area identifier> interface <name> network point-to-point
```

TE リソース管理

TE リソース管理は、トンネル配置を最適化する TE インターフェイスの特定のプロパティの調整として定義されます。

図 7-3 で強調表示されたボックスは、リソース管理が Prime Provisioning のどこで行われるかを示しています。

図 7-11　Prime Provisioning プロセス図：リソース管理



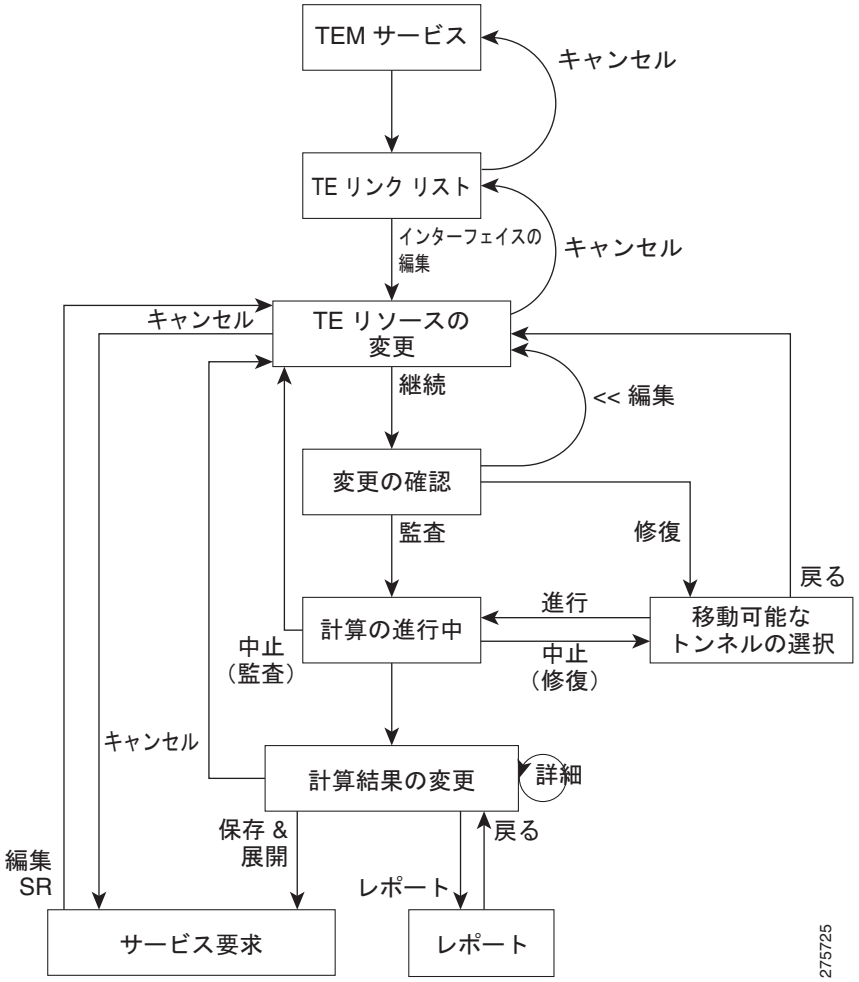
トンネル配置が試行され、十分な帯域幅がない場合は、TE リンクのリソースが変更され、トンネル配置が再試行されることがあります。

ここで述べられているネットワーク リソースは、TE ネットワークのルータ、これらのルータを接続するインターフェイス、RSVP 帯域幅、およびリンクで設定された他のプロパティを意味します。Prime Provisioning は、検出プロセスに依存してリポジトリにネットワーク要素を追加するため、リソース管理を実行する前にリソースを検出する必要があります。

TE リソース管理は、必要に応じて実行する手動プロセスです。元の設定がすでに最適である場合は、リソース管理タスクを行う必要がありません。以降のディスカバリで不一致が見つかったり、保護計画またはプライマリ トンネル配置で期待する結果をなかなか得られなかったりする場合は、リソースを調整する必要があることがあります。

リソース管理プロセスの概要については、図 7-12 を参照してください。

図 7-12　リソース管理プロセス



ここでは、次の内容について説明します。

- 「ネットワーク リソースの変更」（P.7-22）
- 「リンク ステータスの変更」（P.7-24）
- 「TE リンクの削除」（P.7-25）
- 「TE トンネルの削除」（P.7-26）
- 「TE ノードの削除」（P.7-27）。

ネットワーク リソースの変更

リソース管理タスクは、[TE Links List] ウィンドウから主に実行されます。

（注）　説明など特定の属性はこれらのツールで実行する計算に影響を与えず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

TE リンクを変更するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

[TE Links List] ウィンドウが表示されます。

リンク リストには、TE ネットワークで現在アクティブなリンクが表示されます。必要に応じ、矢印を使用してページを移動してください。

ステップ 2　リンク リストで必要なリンクを選択します。

（注）　[Admin Status]：リンクが**アップ**なのか**ダウン**なのかを示します。これは Prime Provisioning に対してローカルです ネットワーク インターフェイスのステータスではありません。

ステップ 3　[Edit] > [Interface A] または [Edit] > [Interface B] をクリックして、リンクのいずれかのインターフェイスを編集します。

（注）　編集対象としてシスコ デバイス以外のインターフェイスを選択した場合、[Edit] ウィンドウで加えた変更は ISC リポジトリに保存されますが、導入はされません。

[TE Resource Modification] ウィンドウが表示されます。次のフィールドが含まれます。

- [Max Global (BC0) Reservable]：TE トンネルで予約できる帯域幅の最大量（kbps）。
- [Max Sub Pool (BC1) Bandwidth]：サブプール TE トンネルで予約できる帯域幅の最大量（kbps）。範囲は、1 ～ [Max Global Reservable] の値までです。
- [Attribute Bits]：パスを選択するときに、比較対象の属性をトンネルのアフィニティ ビットにリンクします。有効な値は 0x0 ～ 0xFFFFFFFF で、32 属性（ビット）を表します。属性の値は 0 または 1 です。
- [TE Metric]：リンクの Interior Gateway Protocol（IGP）管理上の重み（コスト）を上書きするために使用されるメトリック。
- [Propagation Delay]：トラフィックがリンクに沿ってヘッド インターフェイスからテール インターフェイスまで移動する時間。
- [Max Delay Increase]：リンクのバックアップ トンネルの伝搬遅延を制約する FRR バックアップ トンネルの計算で使用されます。バックアップ トンネルを生成する場合、リンクの最大遅延の増加によって、遅延の制約を緩めに設定する必要が生じることがあります。これは、保護されているフローと比較して遅延が増加されない場合、バックアップ トンネルのパスを見つけることは困難であるためです。
- [Link Speed Factor]：プライマリ トラフィックおよびバックアップ トラフィックで使用可能なリンク速度の量（パーセンテージ）に対応する増倍係数。通常は 1 に設定されます。

ステップ 4　必要な変更を行い、[Continue] をクリックして確認ページに進み、変更を確認するか、[Cancel] をクリックして変更を保存せずに終了します。

ステップ 5　[Edit] をクリックして編集可能なウィンドウに戻るか、次のいずれかの方法で続行します。

- [Proceed with Changes]：トンネル監査またはトンネル修復を実行します。

  トンネル監査およびトンネル修復の詳細については、「高度なプライマリ トンネル管理」（P.7-46）を参照してください。

  シスコ デバイス以外のデバイスが編集された場合は、[Proceed with Changes] が無効になります。代わりに、[Save & Deploy] が有効になり、変更を保存できます（展開はできません）。

- [Save & Deploy]：行われた変更がトンネル配置に影響を与えない場合は、[Save & Deploy] をクリックして作業を続行します。この場合は、トンネル監査またはトンネル修復を実行する必要がありません。

（注）　[Save & Deploy] をクリックすると、バックグラウンド プロセスが開始されます。別の配置との競合を避けるために、[Save & Deploy] で別の SR を展開する前にサービス要求（SR）の [Requested] および [Pending] 状態が完了するまで待機してください。展開の状態を確認するには、[Operate] > [Service Request Manager] に移動するか、[Operate] > [Task Manager] を開きます。

（注）　Prime Provisioning で、サービス要求（SR）は、TE トラフィック アドミッション SR を除き、[Operate] > [Service Request Manager] ページではなく、一般に各 TE サービスから展開されます。

展開後、SR のステータスは、[Operate] > [Service Request Manager] の SR ウィンドウで表示できます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] に移動し、展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。タスク ログの詳細については、「Task Logs」（P.7-18）を参照してください。

リンク ステータスの変更

[TE Links List] ウィンドウで、リンクがオフラインになった場合の影響を確認することもできます。この方法は、インターフェイスを実際にシャットダウンする前にリンクからトンネルを移動するために使用できます。

（注）　Prime Provisioning のリンク ステータスはローカルでのみ有効です。ここで説明するリンク ステータスの変更は、ネットワークにプロビジョニングされません。

リンク ステータスを変更するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

[TE Links List] ウィンドウが表示されます。

ステップ 2　1 つまたは複数のリンクを選択し、[Change Status] ボタンをクリックします。

ステップ 3　[Enable] または [Disable] を選択して、選択されたリンクを有効または無効にします。

たとえば、[Disable] を選択すると、リンク ステータスが DOWN に変更されます。

同様に、[Enable] を使用してステータスを [UP] に変更します。

ステップ 4　トンネル監査またはトンネル修復を使用して、トンネルの配置に対する影響を評価し、変更を展開するには、[Proceed with Changes] をクリックします。

トンネル監査およびトンネル修復の詳細については、「高度なプライマリ トンネル管理」（P.7-46）を参照してください。

TE リンクの削除

[TE Link List] ウィンドウには削除機能（[Delete] ボタン）があります。この機能では、TE リンクおよびリンクの両端にある TE インターフェイスをリポジトリから削除できます。この場合、ネットワークの物理リンクには変更が加えられません。

リンク削除は、具体的な TE プロバイダーに基づいて選択できます。異なるプロバイダーに属する異なるリンクを削除する場合は、最初に適切なプロバイダーを選択し、次に削除するリンクをマークします。

また、同じプロバイダーの複数のリンクの同時削除もサポートされます。

制約事項

Prime Provisioning の GUI では、TE オブジェクトが使用しているリンクを削除できません。

次のオブジェクトがチェックされます。

- ストリクト明示的パス
- バックアップ トンネルの保護されたインターフェイス
- SRLG
- 保護された要素
- TE リソース SR

パス オプションを通過するプライマリまたはバックアップ トンネルが存在する場合は、エラー レポートが表示されます。それ以外の場合は、関連する上記のオブジェクト セットを削除する確認を求めるメッセージが表示されます。

使用例

この例では、プライマリまたはバックアップ トンネルが通過できるリンクを削除するときに必要な手順を示します。

次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

ステップ 2　対応するチェックボックスをオンにしてリンクを選択します。

ステップ 3　[Delete] ボタンをクリックします。

ステップ 4　次の 2 通りの結果が考えられます。

- パス オプションがあるトンネルがリンクを通過します。リンクの削除に失敗し、リンクの削除を再試行する前にこれらのトンネルを再ルーティングまたは削除するよう求められます。この場合は、[TE Links List] ページに移動されます。
- パス オプションがあるトンネルがリンクを通過しません。そのリンクに対して TE に関連するオブジェクトのリストが表示され、TE リンクに関連するオブジェクトの自動削除に同意するか、リンクの削除トランザクションをキャンセルするかを確認するよう求められます。

ステップ 5　必要なすべてのトンネルを再ルーティングするか削除してからリンク削除を試行した場合は、まだ関連しているオブジェクトのリストが表示されます。

ステップ 6　プライマリ トンネルの再ルーティング後または削除後にリストされた関連する TE オブジェクトを削除する場合は、バックアップ リンク保護を提供するトンネルまたは複数のインターフェイスを保護するトンネルが存在する場合のみ、トランザクションの進行状況を示す新しいウィンドウが表示されま

す。バックアップ リンク保護を提供するトンネルまたは複数のインターフェイスを保護するトンネルが存在しない場合は、関連する TE オブジェクト リスト ページから、成功または失敗トランザクションに関する [TE Links] ウィンドウに移動します。

関連する TE オブジェクトに関する次の注意事項を確認してください。

ステップ 7　関連するすべてのオブジェクトが削除されたら、[TE Links List] ウィンドウが表示されます。

関連 TE オブジェクトに関する注意事項

関連する TE オブジェクトは次のいずれかになります。

- リンクを通過しているストリクト明示的パスおよびルーズ明示的パス（ストリクト ホップ タイプのもの）
- リンク保護を提供するバックアップ トンネル

（注）　リンクが SRLG から削除され（SRLG に複数のリンクがある場合）、またはリンクと SRLG の両方が削除されます（削除のためにマークされたリンクが、SRLG 内で唯一のリンクである場合）。

- リソース：SRs
- 保護された要素

上記リストの関連する TE オブジェクトは、リンクが TEM で設定されている方法によって異なります。

たとえば、関連する TE オブジェクトにリンク保護を提供するバックアップ トンネルがある場合は、保護されたインターフェイスが、利用可能な TE リンクに対して適切に更新され、バックアップ トンネル SR が再展開される [Link Deletion Progress] ウィンドウが表示されます。リンク保護を提供するバックアップ トンネルが関連する TE オブジェクトの資格を満たさない場合は、残りの TE オブジェクトが、関連する TE オブジェクトが表示されたウィンドウから自動的に削除されます。

TE トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ、または個々のプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます（「プライマリ トンネルの削除」（P.7-40）または「バックアップ トンネルの削除」（P.7-45）を参照）。

[TE Links] ウィンドウで、1 つ以上のトンネルが通過するリンクを削除する必要性が、トンネルを削除する理由である場合があります。

トンネルを [TE Links List] ウィンドウで削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

ステップ 2　削除するトンネルのリンクを選択し、[Show Tunnels] ボタンをクリックします。

表示するトンネルのカテゴリを選択できるトンネル フィルタが表示されます（[All]、[Managed]、[Unmanaged]、[Backup]）。

ステップ 3　いずれかのトンネルのカテゴリを選択します。

リンクを通過し、選択したフィルタのカテゴリに属するすべてのトンネルのリストが表示されます。

ステップ 4　削除する 1 つ以上のトンネルを選択し、[Delete] ボタンをクリックします。

新しいプロビジョニング操作の開始によって、選択したトンネルが削除されます。

TE ノードの削除

また、TE ノードを削除することもできます。この処理は、リンクの削除と非常に似ていますが、PE デバイス画面から実行します。対応する PE デバイスを削除することにより、TE ノードを事実上削除します。

TE リンクの場合と同様の制限が適用されます。削除操作は、いかなる TE オブジェクトもノードを使用していない場合にだけ成功します。

制約事項

Prime Provisioning の GUI では、TE オブジェクトが使用しているノードを削除できません。

TE リンクと同様に、次のオブジェクトを確認します。

- ストリクト明示的パス
- バックアップ トンネルの保護されたインターフェイス
- SRLG
- 保護された要素
- TE リソース SR

また、ノードの削除では、いかなる管理対象トンネル、管理対象外トンネル、またはバックアップ トンネルも、そのノードで開始または終了していないことが確認されます。

これらのオブジェクトのいずれかがノードを使用している場合は、ノードを削除しようとすると、エラー メッセージが発生し、ノードとそのインターフェイスが未変更のままになります。

使用例

この機能の例は、TE ルータをネットワークからデコミッションし、大規模なトポロジ変更の一環として 1 つまたは複数の新しい TE ルータに置き換える場合です。

このノードを削除できるようにするためには、次のようなステップが必要です。

1. トンネル修復を使用してこのノードからすべての管理対象トンネルを再ルーティングする。
2. トンネルから離れるパスの一部としてノードを使用して、すべての管理対象外トンネルとバックアップ トンネルを再ルーティングする。
3. ノードを構成するいずれかのインターフェイスを保護するすべてのバックアップ トンネルを削除する。
4. ノードを使用する明示的なパスをすべて削除する。
5. [TE Links List] ウィンドウでリポジトリからノードを削除する。
6. Prime Provisioning の外部で、適切な停止期間内に、ノードのデコミッションを行い、新しいノードをセットアップする。
7. 新しい [TE discovery] タスクを実行する。この結果、新しく追加されたノードがリポジトリに追加される。

8. ネットワークの FRR 要件に応じて、バックアップ計算を使用して新しいノードを保護する。（「バックアップ計算」（P.7-65）を参照）。
9. ネットワーク グルーミング（「グルーミング」（P.7-59）を参照）を実行して、管理対象トンネルを最適化することにより、管理対象トンネルで新規ノードが使用されるようにする。

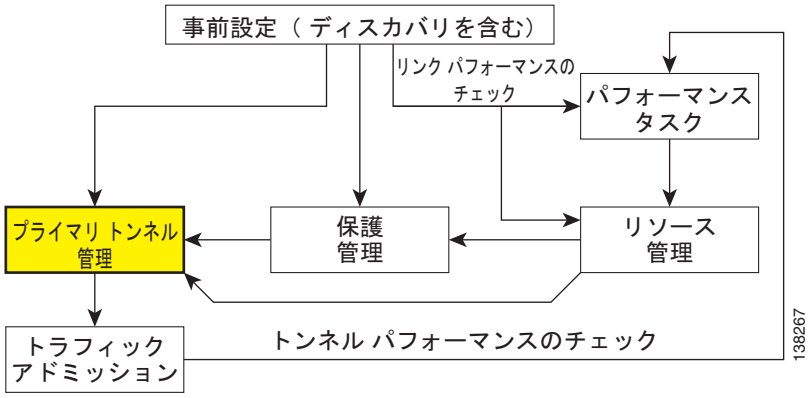
これらの手順が正常に行われると、TE ノードと、そのノードで開始されるすべての TE リンクおよび TE インターフェイスがリポジトリから削除されます。

基本的なトンネル管理

ここでは、Prime Provisioning でプライマリおよびバックアップ トンネルの作成に必要なプロセスについて説明します。トンネルを作成するには、以前の項の説明に従って、特定のステップをまず実行する必要があります。

図 7-3 で強調表示されているボックスは、Prime Provisioning のプライマリ トンネル管理が発生した場所を示します。

図 7-13　Prime Provisioning プロセス図：プライマリ トンネル管理



プライマリ トンネルは、通常操作においてトラフィックを伝送することによって特徴付けられます。可能なパスの優先順位リストがあり、これにより、トラフィックをルーティングすることができます。いずれの時点でも、優先順位の最も高い、使用可能なパスがトラフィックのルーティングに使用されます。これに失敗した場合、トラフィックは通常、より高い優先順位のパスが再び使用可能になるまで、次に使用可能なパスを介してリルートされます。

トンネルを設定する前に、トラフィックを制御する TE ポリシーを定義する必要があります。ルートを確立するために明示的パスが作成され、プライマリ トンネルの場合は、管理対象または管理対象外トンネルのいずれかとして作成されます。

バックアップ トンネルの目的は、ネットワーク内のルーティングが再コンバージェンスされるまで、失敗した要素の周辺の Fast Re-Route（FRR）で保護されたトラフィックを伝送することです。これは、プライマリ トンネルに沿って移動するトラフィックを保護することを意図しています。ロード バランシングの使用を通じて、同じトラフィックを複数のバックアップ トンネルが保護することが考えられます。

ネットワークが再コンバージされない場合は、バックアップ トンネルによる伝送が続行されます。

管理対象トンネルと管理対象外トンネルの違いは、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象 / 管理対象外プライマリ トンネルの項で説明します。

帯域幅プールという重要な概念があり、ここからトンネルで帯域幅を予約します。これは、「トラフィック エンジニアリング管理の概念」（P.7-115）の帯域幅プールの項で説明します。

ここでは、次の内容について説明します。

TE ポリシーの作成

プライマリ トンネルを作成するには、各プライマリ トンネルをポリシーに関連付ける必要があります。ポリシーは、複数のトンネルで使用できます。

バックアップ トンネルの場合、このステップは必要ありません。この場合は、「明示的パスの作成」（P.7-30）に進みます。

他の TE ポリシー管理の操作については、「TE ポリシー」（P.7-73）を参照してください。

TE ポリシーは、TE ネットワークを制御する一連のルールで、プライマリ トンネル トラフィックのサービス クラス（たとえば、ゴールド、シルバー、ブロンズ）を定義します。

Prime Provisioning には、管理対象および管理対象外のポリシーの概念があります。管理対象ポリシーの設定/保持優先順位は 0/0 であり、保護レベルや最大遅延などの追加のルーティング制約があります。管理対象外ポリシーのトンネルは、システムによってプロビジョニングされますが、システムは展開のみを追跡し、トンネルの操作は追跡しません。管理対象外ポリシーの設定/保持優先順位は 0 にできません。

管理対象および管理対象外のプライマリ トンネルの詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）で、管理対象/管理対象外プライマリ トンネルの項を参照してください。

ポリシーは [Service Design] の [Policies] で管理します。**ポリシー** GUI の詳細については、「TE ポリシー」（P.7-73）を参照してください。

TE ポリシーを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [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　[Create] をクリックし、[TE Policy] を選択して新規 TE ポリシーを設定します。

既存のポリシーを編集するには、変更するポリシーを選択し、[Edit] をクリックします。[TE Policy Editor] ウィンドウが表示されます。

（注）　トンネルで使用されているポリシーは変更できません。ただし、使用中のポリシーの名前と所有権は変更できます。

さまざまなウィンドウ要素の説明については、「TE ポリシー」（P.7-73）を参照してください。

ステップ 3　アスタリスク（*）が付いた必須フィールド、および任意フィールドに入力します。

管理対象トンネルの TE ポリシーを使用する場合は、[Managed] チェックボックスがオンであることを確認します。

管理対象トンネルのポリシーを設定する場合は、**設定**および**保持**優先順位が 0（最も高い優先順位）に自動的に設定されます。管理対象外トンネルのポリシーを設定する場合は、希望する**設定**および**保持**優先順位の設定を指定することができます。

ステップ 4　[Save] をクリックします。

明示的パスの作成

パスは、ソース ルータと宛先ルータの間で定義され、これらの間には 1 つ以上のホップがある可能性があります。パスは、明示的パスのオプションで、プライマリ トンネルおよびバックアップ トンネルに対して使用されます。

管理対象トンネルの明示的パスを作成する場合、パスに TE 以外に対応したインターフェイスを含めないでください。TE 以外に対応したインターフェイスを持つパスは、管理対象トンネルおよびバックアップ トンネルのトンネル エディタのトンネル パス選択によるフィルタリングによって除外されます。

明示的パスを作成または編集するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Explicit Paths] を選択します。

[TE Explicit Path List] ウィンドウが表示されます。

ステップ 2　[TE Explicit Path List] で明示的パスを作成するには、[Create] をクリックします。

[New TE Explicit Path] ウィンドウが表示されます。

明示的パス リストで明示的パスを編集するには、変更する明示的パスを選択し、[Edit] をクリックします。これにより、[TE Explicit Path Editor] ウィンドウが開きます。

（注）　トンネルで使用されている明示的パスは変更できません。ただし、パスを表示するには [Edit] を使用します。

[New TE Explicit Path] ウィンドウには、次の GUI 要素があります。

- [Path Name]：明示的パスの名前。
- [Head Router]：ヘッド ルータの名前。
- [Path Type]：次の 3 タイプの明示的パスがサポートされています。
  - [STRICT]：すべてのストリクト ホップはパスで定義されます。
  - [Loose]：すべてのルーズ ホップ（純粋なルーズ パスまたはルーズ ホップとストリクト ホップの組み合わせ）は、パスで定義されます。

  - [EXCLUDE]：すべての除外ホップはパスで定義されます。
- [Links (table)]：現在のパスに追加されたリンクを示し、次の情報が含まれます。
  - [Device]：パスのリンク元である TE デバイスのホスト名。
  - [Outgoing Interface]：発信元デバイスの発信インターフェイスのインターフェイス名。
  - [Outgoing IP]：発信インターフェイスの IP アドレス。
  - [Next Hop]：ネクスト ホップ デバイスのホスト名。
  - [Incoming Interface]：ネクスト ホップ デバイスの着信インターフェイスの名前。
  - [Incoming IP]：ネクスト ホップ デバイスの着信インターフェイスの IP アドレス。
- [Provision Preference]：**ip explicit-path** コマンドの **next-address** サブコマンドをプロビジョニングするための設定。[Outgoing Interface] または [Incoming Interface] を選択します。
  - [Outgoing Interface]：ルータ上の発信インターフェイス。
  - [Incoming Interface]：ルータ上の着信インターフェイス。

（注） トンネルでパスが使用されている場合、変更することはできません。[Outgoing Interface] および [Incoming Interface] リンクは選択できず、[Provision Preference] 行および [Add Link]、[Delete Link]、および [Save] ボタンは表示されません。

ステップ 3　パス名を指定してヘッド ルータを選択します。

ステップ 4　パス タイプを選択します。

- [Strict]：[Strict] が選択されている場合は、現在のパネルを使用して、宛先に到達するまで 1 つずつ接続されたリンクを一覧表示します。
- [Loose]：[Loose] が選択されている場合、IP アドレスを入力することにより新しいホップが追加されます。[Strict] が選択されている場合は、[TE Links List] からのみ選択することができます。

（注） IOS XR で、ヘッド デバイスが IOS XR 3.4 以降を実行している場合は、[Loose] タイプのみ使用できます。

（注） [Loose] が選択されている場合、ルーズ ホップ定義を 1 つずつ追加する新しいパネルが一覧表示されます。ルーズ明示的パス定義にはストリクト ホップとルーズ ホップの組み合わせを使用できるため、ストリクト ホップを含む柔軟性が、パスに少なくとも 1 つのルーズ ホップが存在するという制約とともに提供されます。

- [Exclude]：[Exclude] を使用することによって、除外する IP アドレスを指定できます。ステップ 6 を参照してください。

ステップ 5　[Strict] が選択された場合、[Add Link] ボタンをクリックして空白行をホップ リスト テーブルに追加します。

[Loose] または [Exclude] を選択した場合は、[Add Hop] ボタンが表示され、このボタンをクリックすると IP アドレスを指定するポップアップ ウィンドウが開きます。

ステップ 6　次に、ヘッド ルータのインターフェイスを選択する必要があります。

パス タイプの選択に応じて、次のいずれかのウィンドウが表示されます。

A. ストリクト パス タイプ：

[Add Link] ボタンをクリックし、次に [Add Interface] をクリックします。[Select Next Hop] ウィンドウが表示されます。

ネクスト ホップ リストには、明示的パスにすでに含まれているものを除き（パス ループを避けるため）、ルータのすべての可能なネクスト ホップが含まれています。

次のホップ リストには、TE インターフェイスおよび最大 1 つの各ルータの TE 以外のインターフェイスが含まれます（ループバック インターフェイスがデバイスの MPLS TE ID として使用されている場合）。TE インターフェイスの場合、[Outgoing Interface] および [Outgoing IP] 列がアプリケーションによって生成されます。

（注）　TE 以外のインターフェイスが選択されている場合、[Provision Preference] は [Incoming Interface] に設定されます。プロビジョニング設定は手動で設定できません。

インターフェイスを選択し、[Select] をクリックします。対応するリンク情報が、[Links] テーブルの新しい明示的パスに追加されます。

[New TE Explicit Path] ウィンドウで、受信および発信インターフェイスの両方のフィールドが生成されます。

B. ルーズ パス タイプ：

[Add Hop] ボタンをクリックします。[Loose Hop Definition] ウィンドウが表示されます。

このウィンドウで、必要なルーズ ホップの IP アドレスを指定し、[OK] をクリックします。[Loose Hop Definition] ウィンドウが閉じます。

[New TE Explicit Path] ウィンドウに、追加したルーズ ホップが表示されます。

C. 除外 パス タイプ：

[Add Hop] ボタンをクリックします。[Exclude Hop Definition] ウィンドウが表示されます。

このウィンドウで、必要な除外ホップの IP アドレスを指定し、[OK] をクリックします。[Exclude Hop Definition] ウィンドウが閉じます。

[New TE Explicit Path] ウィンドウに追加された除外ホップが表示されるようになります。

ステップ 7　別のリンクを追加するには、[Add Link] または [Add Hop] をクリックします。

ステップ 8　ストリクト ホップの場合、[Outgoing Interface] または [Incoming Interface] オプション ボタンのいずれかをクリックすることにより、オプションで [Provision Preference] を選択できます。

（注）　TE 以外のインターフェイスが存在しない場合にリンクを追加する前に [Provision Preference] を選択しようとすると、[Add Link] プロセスにより [Provision Preference] が無効になり、受信に設定されます。

ステップ 9　作成した TE 明示的パスを保持するには [Save] をクリックし、保存せずに終了するには [Cancel] をクリックします。

明示的パスの削除

Prime Provisioning では、プライマリ / バックアップ トンネルの削除 / デコミッション時の明示的パスのデコミッションをサポートしています。これは、IOS XR の場合にのみサポートされます。

このような状況で明示的パスを削除できるかどうかは、他のグローバル アプリケーションによって使用されるかどうかによって異なります。

明示的パスの削除は、プライマリ管理対象/管理対象外トンネル、バックアップ トンネル、および任意の非適合トンネルの両方の SR トンネル削除と関連して行われ、すべてのパス オプション タイプ（STRICT、LOOSE、EXCLUDE）に適用可能です。

トンネル設定の変更により、システム内のトンネルが明示的パスを使用しなくなった場合、明示的パス設定は Prime Provisioning によって自動的に削除されます。この状況は、トンネルを削除した場合、または Prime Provisioning でトンネルをリルートした場合に発生します。

デバイスから明示的パス設定を削除した場合でも、明示的パスはまだ Prime Provisioning データベースには存在しています。データベースに残っているこのような明示的パスは、再使用できます。

Prime Provisioning の外部で（たとえば、デバイス自体の CLI を介して）トンネルをリルートまたは削除した場合、明示的パスは削除されません。ただし、トンネルが明示的パスを使用しなくなるように、トランザクションが Prime Provisioning を使用してトンネルをリルート、削除、変更した場合、その明示的パス設定は自動的にデバイスから削除されます。

プライマリ トンネルの操作

Prime Provisioning を使用することにより、多くのプライマリ トンネルの操作を実行できます。これらについては、次の項で説明します。

プライマリ トンネルの作成

TE ポリシーおよび明示的パスの設定を終えれば、プライマリ トンネルを作成できます。プライマリ トンネルには、次の 2 つのタイプがあります。

- 管理対象プライマリ トンネル
- 管理対象外プライマリ トンネル

以降では、管理対象外プライマリ トンネルを作成する場合の GUI の流れを説明します。これは、管理対象プライマリ トンネルと非常に似ており、わずかな違いについては、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象/管理対象外プライマリ トンネルの項で説明されています。

管理対象プライマリ トンネルまたは管理対象外プライマリ トンネルを作成するには、次のステップを実行します。

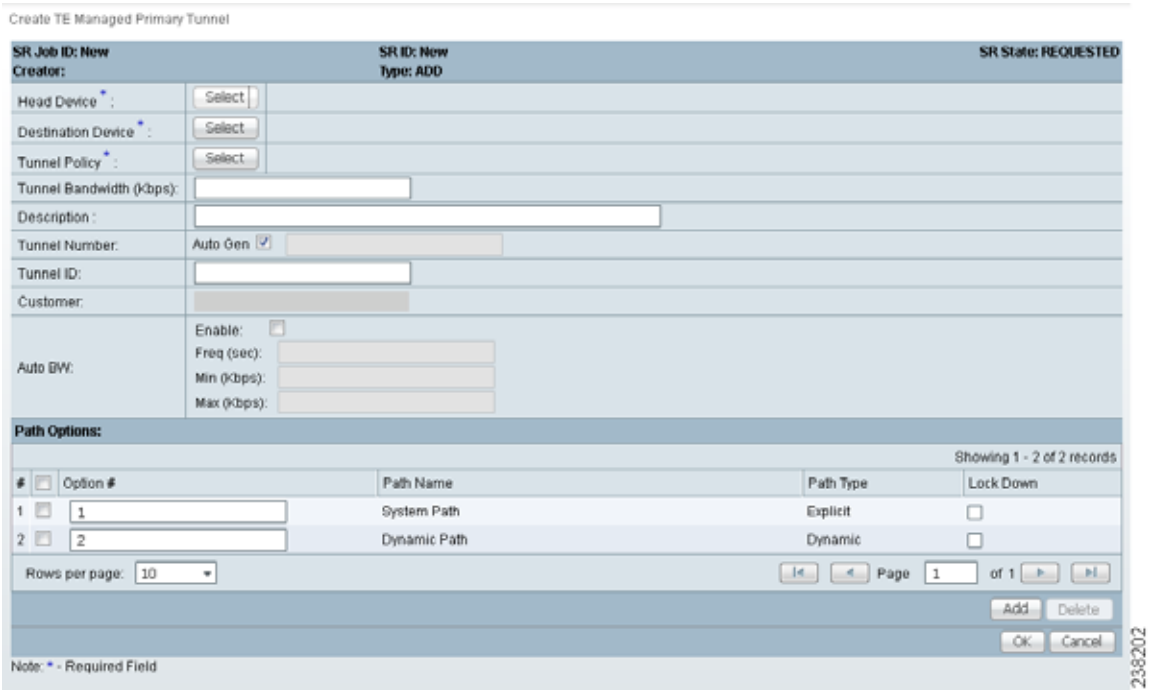
ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed Tunnel] をクリックします。図 7-14 に示すように、[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

図 7-14　Create TE Managed Primary Tunnel



次の要素を含む [TE Managed Primary Tunnels SR] ウィンドウが表示されます。

- [Op]：トンネルの SR 操作。次のいずれかになります。
  - [ADD]：新しく追加されたトンネルを示します。
  - [MODIFY]：変更された既存のトンネルを示します。
  - [DELETE]：削除される既存のトンネルを示します。
  - [ADMIT]：トンネル計算によってアドミッションされる既存のトンネルを示します。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [T#]：ヘッド ルータのトンネル番号。
- [Head]：ヘッド ルータのホスト名。
- [Dest]：宛先ルータのホスト名。
- [Policy]：トンネルの TE ポリシー。
- [BW]：トンネル帯域幅。トンネルが auto-bw 対応の場合、[BW] には、トンネル帯域幅と最大自動帯域幅のうち大きい方が示されます。
- [AutoBW]：**true** であれば自動帯域幅がイネーブルにされており、そうでない場合は **false** です。
- [Deploy Status]：トンネル展開ステータス。
- [Verified]：トンネルの検証が成功したかどうかを示します（succeed、failed、または unknown）。
- [Allow Reroute]：再ルーティングが許可されるかどうかを指定します（true または false）。再ルーティングが許可されない場合、トンネルは移動可能に設定できないため、操作によって再ルーティングできません。
- [Head Region]：ヘッド ルータが含まれているリージョン。
- [Tail Region]：テール ルータが含まれているリージョン。

次のアクションを実行できます（ボタン）。

- [Display]：ネットワークのトポロジの表示を開き、選択されたプライマリ トンネルを強調表示します。選択したトンネルは、方向を示す矢印を使用してカラーでマークされます。
- [Details]：トンネルのタイプ、ステータス、LSP、およびその他の情報を提供する [TE Tunnel Details] ウィンドウを開きます。
- [Admit]:選択した事前に検証されていないトンネルを管理対象トポロジにアドミッションします。この機能は、検証が失敗したディスカバリ済みのトンネル、または管理対象外トンネルの移行にのみ使用します。
- [Create]：管理対象プライマリ トンネルを作成します。
- [Edit]：選択したプライマリ トンネルを編集します。
- [Delete]：選択したプライマリ トンネルを削除します。
- [Import]：インポート XML ファイルからトンネル データをインポートします。
- [Placement Tools]：これらのツールは、トンネルに変更を加えていない場合にだけ使用できます。現在のトポロジおよびトンネルに対して次の機能を適用します。
  - [Groom]：最大リンクの使用率を下げるために、ネットワークの管理対象トンネルを分析し、再ルーティングします。
  - [Tunnel Audit]：SRLG またはバックアップ トンネルに対して以前に加えた変更が、管理対象トンネルで制約違反の原因となったかどうかを調べます（これは、管理対象トンネルに FRR 保護の制約がある場合に発生することがあります）。
  - [Tunnel Repair]：[Placement Tools] > [Tunnel Audit] で明らかになった管理対象トンネルの制約違反を修復します。
- [Update Tunnel ID]：対応するトンネルを展開せずに、リポジトリでトンネル ID を直接更新します。
- [Proceed with Changes]：トンネルの変更を確認します。トンネルが作成、削除、またはアドミッションされるか、またはトンネルの属性が変更された場合に、次のいずれかの配置ツールに進むことができます。
  - [Tunnel Audit]：トンネルの変更が原因となった可能性がある制約違反をチェックします。
  - [Tunnel Placement]：新しいトンネルのアドミッションを行い、ネットワークですでにアドミッションされたトンネルを変更します。
  - [Tunnel Repair]：変更を受け入れるためにできるだけ少ない既存のトンネルを移動することにより、既存のトンネルの帯域幅要件または遅延パラメータの変更による不一致を解決します。

管理対象外トンネルのリストでは、管理対象リストの最後の 2 列（[Verified] および [Allow Reroute]）が [Conformance] 列に置き換えられることに注意してください。

次の例では、管理対象外トンネルが作成されます。

ステップ 3　[Create] をクリックします。

[Create TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

[Create TE Managed Primary Tunnel] ウィンドウと [Create TE Unmanaged Primary Tunnel] ウィンドウには、わずかな違いがありますが、次の要素が含まれています。

- [Head Device]：トンネルのヘッド デバイス。
- [Destination Device]：トンネルの宛先デバイス。
- [Tunnel Policy]：トンネルに対して確立されたルールのセット。
- [Tunnel Bandwidth]：トンネルに割り当てられている合計帯域幅。

- [Description]：トンネルの識別に役立つ説明のテキスト。
- [Tunnel Number]：トンネル インターフェイスの名前に対応するトンネル番号。
  - [Auto Gen]：トンネル番号を自動的に生成する場合は、このボックスをオンにします。オンにしない場合は、希望する番号を入力します。

（注）　手動で入力したトンネル番号が小さすぎると、展開の妨げになるおそれがあります。

（注）　MPLS-TE トンネルには、マルチキャスト GRE トンネルと干渉する潜在性があります。Prime Provisioning では、auto-gen を使用して新規トンネルを作成しますが、このトンネル番号は、MDT GRE トンネルによってすでに使用されているおそれがあります。このため、Prime Provisioning は、複雑さを回避するために大きいトンネル番号を使用します。

- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [Customer]：トンネルに対して選択したカスタマー。
- [Auto BW]：自動帯域幅調整のためにトンネルを設定し、トンネルの帯域幅の調整方法を制御します。
  - [Enable]：自動帯域幅をイネーブルにするには、このボックスをオンにします。
  - [Freq]：帯域幅調整の間隔。
  - [Min]：このトンネルの最小自動帯域幅（kbps 単位）。
  - [Max]：このトンネルの最大自動帯域幅（kbps 単位）。

パス オプション：

- [Option #]：使用可能な明示的パスの連続番号。
- [Path Name]：明示的パスの名前。既存のパスの場合、名前は明示的パス ビューアにリンクする URL です。
  - [System Path]：システム生成の明示的パス。管理対象トンネルでは、最初のパスは明示的パスでなければなりません。トンネルにシステム パスが含まれている場合、計画の機能は、トンネルの最適パスを生成します。
  - [Dynamic Path]：動的パスは、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。
- [Path Type]：パス オプション タイプ（[Explicit] または [Dynamic]）。
- [Lock Down]：トンネルの再最適化チェックをディセーブルにします。オンにした場合、パスは変更できません。

ステップ 4　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Head Device] を選択するには、対応する [Select] ボタンをクリックし、[Select Device for TE Head Router] ウィンドウを開きます。

ステップ 5　デバイス名を選択し、[Select] をクリックします。

[Select Device for TE Head Router] ウィンドウが閉じられ、[Create TE Unmanaged Primary Tunnel] ウィンドウにプロンプトが戻ります。

ステップ 6　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Destination Device] を選択するには、対応する [Select] ボタンをクリックし、[Select Device for TE Tail Router] ウィンドウを開きます。

ステップ 7　デバイス名を選択し、[Select] をクリックします。

[Select Device for TE Tail Router] ウィンドウが閉じられ、[Create TE Unmanaged Primary Tunnel] ウィンドウにプロンプトが戻ります。

ステップ 8　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Tunnel Policy] を選択するには、対応する [Select] ボタンをクリックして [Select Unmanaged TE Tunnel Policy] ウィンドウを開きます。

（注）　管理対象トンネルを作成するときは、1 つ以上の管理対象トンネル ポリシーが使用可能なことを確認してください。このようになっていない場合は、[Policies]（「TE ポリシーの作成」（P.7-29）を参照）に移動し、[Managed] チェックボックスがオンであることを確認します。

ステップ 9　ポリシーを選択し、[Select] ボタンをクリックします。

これにより、トンネル エディタに戻ります。

ステップ 10　[Add] をクリックし、トンネルのパス オプションを設定します。[Select TE Explicit Path] ウィンドウが表示されます。

[Path Options] には、パス タイプが 2 つ示されます。

[Explicit Path]：次の 3 種類のパスを含む、特定のヘッドから特定の宛先デバイスへの固定パス：[Strict]、[Loose]、および [Exclude]。

[Dynamic Path]：動的パスは、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。

ステップ 11　ダイナミック パスだけを希望する場合を除き、必要な TE の明示的パスを選択します。

使用可能なものがない場合は、まず設定することができます。これを行うには、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 12　[Select] をクリックします。

選択したパスが、作成ウィンドウの [Path Options] セクションに表示されます。

明示的パス（*<head_device>-<destination_device>*）の場合は、パス名をクリックして編集不可の明示的パス ビューアを開くことができます。

さまざまなウィンドウ要素の説明については、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 13　[Create TE Unmanaged Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして終了し、[TE Unmanaged Primary Tunnels SR] ウィンドウに戻ります。

[Op] フィールドに [ADD] を設定した、新規作成した SR を含む [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、[ADD] 状態から元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 14　[TE Unmanaged Primary Tunnel] ウィンドウで [Save & Deploy]（（注）（P.38）を参照）をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。

展開の状態を確認するには、[Operate] > [Service Request Manager] で [Service Requests] ウィンドウに移動するか、[Operate] > [Task Manager] を開きます。

- [Save & Deploy]：トンネル配置に影響を与えないトンネルの変更をコミットします。ネットワークに対して SR トンネルを保存し、展開するための 2 つのオプションがあります。

- [SR Tunnels Only]：トンネル配置に影響しないトンネルのすべての変更を展開するか、SR に変更が加えられていない場合に、このオプションを使用して、[Requested] 状態または [Invalid] 状態だった SR を再展開します。
- [Force Deploy All Tunnels]：この SR に含まれるすべてのトンネルを強制的に展開します。SR の前回プロビジョニングが失敗し、SR に含まれるすべてのトンネルを強制的に展開する必要がある場合に有用です。

（注）　TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

（注）　管理対象トンネルの場合、[Proceed with Changes] ボタンを使用してトンネル配置、トンネル監査、またはトンネル修復（「高度なプライマリ トンネル管理」（P.7-46））を実行するまで、サービス要求を展開できません。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Operate] > [Service Request Manager] からではなく、常に特定の [TE SR] ウィンドウからすぐに展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます（最初は REQUESTED、次に PENDING、成功した場合は DEPLOYED）。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

[Service Request Manager] ウィンドウからサービス要求を編集する場合は、「プライマリ トンネルの編集」（P.7-38）の説明に従って、[TE Managed Primary Tunnels SR] ウィンドウまたは [TE Unmanaged Primary Tunnels SR] ウィンドウに戻ります。

プライマリ トンネルの編集

プライマリ トンネル属性はプライマリ トンネル エディタで変更できます。

プライマリ トンネル エディタにアクセスする方法は 2 通りあります。

- 管理対象または管理対象プライマリ トンネルの SR ウィンドウから、または
- [Service Requests] ウィンドウから

プライマリ トンネルの SR ウィンドウからのアクセス

プライマリ トンネルの SR ウィンドウ（[TE Managed Primary Tunnels SR] または [TE Unmanaged Primary Tunnels SR] ウィンドウ）からプライマリ トンネル エディタにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。図 7-14 の [TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged TE Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Edit TE Managed Primary Tunnel] ウィンドウまたは [Edit TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

プライマリ トンネル エディタは、プライマリ トンネル作成 GUI のエディタと同じです。さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 4　必要な変更を加え [OK] をクリックして受け入れるか、[Cancel] をクリックして変更を廃棄します。

[TE Unmanaged Primary Tunnel SR] ウィンドウで、[Op] フィールドが [MODIFY] に変わります。

（注）　変更したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [MODIFY] フラグが消えます。

ステップ 5　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウからアクセス

SR がすでに作成されている場合に [Service Requests] ウィンドウからプライマリ トンネル エディタにアクセスするには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　必要なトンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

管理対象トンネルを選択したのか管理対象外トンネルを選択したのかに応じて、[Service Requests] ウィンドウで選択した SR を表示した、[TE Managed Primary Tunnel SR] ウィンドウまたは [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を選択し、[Edit] をクリックします。

[Edit TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

「プライマリ トンネルの SR ウィンドウからのアクセス」（P.7-38）に移動し、ステップ 4 から処理を続行します。

プライマリ トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ（「TE トンネルの削除」（P.7-26）を参照）、またはプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます。

管理対象または管理対象外のプライマリ トンネルを [TE Managed Primary Tunnels SR] ウィンドウまたは [TE Unmanaged Primary Tunnels SR] ウィンドウから削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged TE Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　トンネルを削除するには、削除するトンネルを選択し、[Delete] をクリックします。

[Op] フィールドのステータスが [DELETE] に変わります。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

（注）　削除したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [DELETE] フラグが消えます。

ステップ 4　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

バックアップ トンネル操作

Prime Provisioning では、いくつかのバックアップ トンネルの操作を実行できます。これについては、この項で説明します。

「トラフィック エンジニアリング管理の概念」（P.7-115）の「Connectivity Protection (CSPF) Backup Tunnels」は、バックアップ保護を実現する手法の 1 つです。

バックアップ トンネルの作成

バックアップ トンネルの作成方法は、プライマリ トンネルとほぼ同じです。いずれの場合も、対象のルータを通過する既存のパスがすでに存在する場合は、明示的パスの作成は不要です。パスは、パスの帯域幅キャパシティの許す限り、任意の数のトンネルで使用できます。

バックアップ トンネルの作成の前提条件は、明示的パスが存在することです。明示的パスを作成するには、「明示的パスの作成」（P.7-30）を参照してください。

バックアップ トンネルを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

[TE Protection SR] ウィンドウには、次の要素が含まれます。

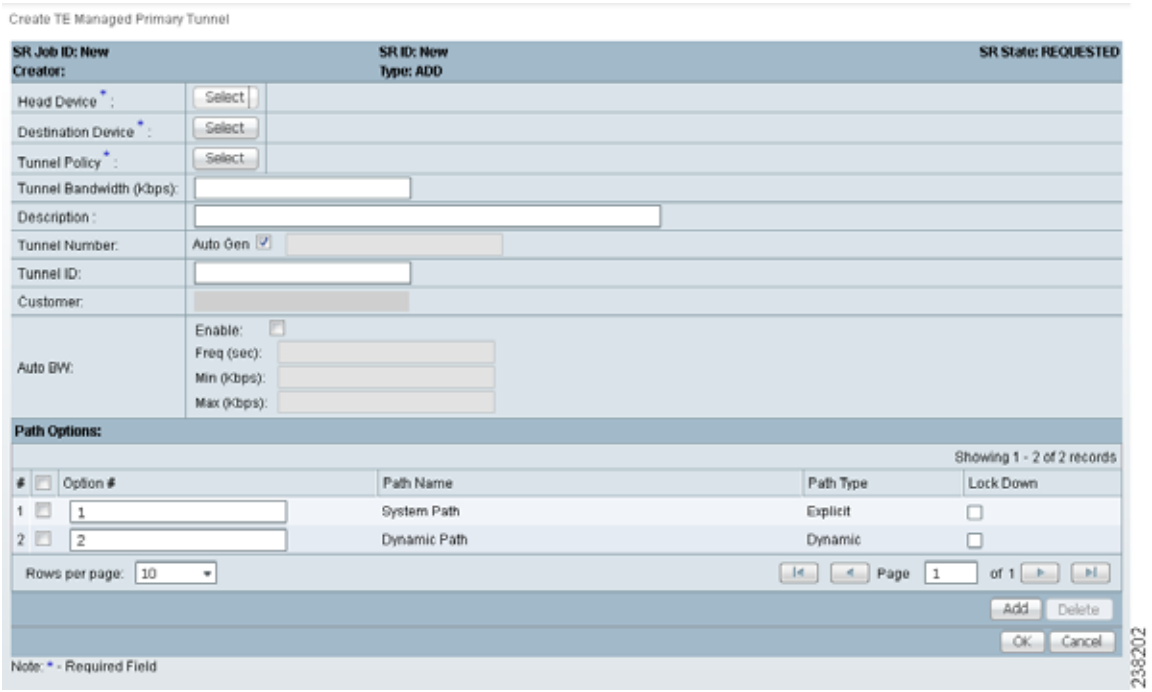
トンネル リストの列には、次の情報が示されます。

- [Op]：トンネルの現在の SR 操作。次のいずれかになります。
  - [ADD]：システムによって計算され、またはユーザによって入力された新規追加トンネルを示します。
  - [MODIFY]：変更された既存のトンネルを示します。
  - [DELETE]：システムの計算によるか、ユーザが開始することによって削除される既存のトンネルを示します。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [T#]：ヘッド ルータのトンネル番号。
- [Head]：ヘッド ルータのホスト名。
- [Dest]：宛先ルータのホスト名。
- [BW Quota]：このバックアップ トンネル保護できる帯域幅の量。ルータでは、LSP の帯域幅の合計が指定された帯域幅の総計を超えないように、このバックアップ トンネルを使用できる LSP を制限できます。複数のバックアップ トンネルがある場合、ルータは最適なアルゴリズムを使用します。
- [Deploy Status]：トンネル展開ステータス。
- [Conformance]：ディスカバリを実行して判明したトンネルの適合性を示します。予約された帯域幅が非ゼロで、保持プライオリティまたはセットアップ プライオリティがゼロの場合、トンネルは不適合です。TEM から入力したトンネルの場合は、常に適合しています。接続保護トンネルは、トンネル帯域幅が 0 で、バックアップ帯域幅が無制限であり、最初のパス オプションが「exclude address」である場合は、Conformant = true とマークされます。それ以外の場合は、Conformant = false とマークされます。
- [Backup Type]：帯域幅によって保護されているバックアップ トンネル（**BW** 保護）または CSPF-routed バックアップ トンネル（**CSPF**）のいずれかにすることができます。これらのバックアップ トンネルのタイプについて詳しくは、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- [Head Region]：ヘッド ルータが含まれているリージョン。
- [Tail Region]：テール ルータが含まれているリージョン。

ステップ 2　[Create] をクリックします。

図 7-15 の [Create TE Backup Tunnel] ウィンドウが表示されます。

図 7-15　Create TE Backup Tunnel



[Create TE Backup Tunnel] ウィンドウには次の要素が含まれています。

- [Head Device]：トンネルのヘッド デバイス。
- [Destination Device]：トンネルの宛先デバイス。選択ウィンドウは、ヘッド デバイス選択のウィンドウに非常に似ています。
- [Protected Interface(s)]：このバックアップ トンネルで保護するヘッド ルータ上のインターフェイス。
- [Description]：トンネルの識別に役立つ説明のテキスト。
- [Backup Bandwidth Limit]：バックアップ トンネルによって保護される帯域幅。
  - [Any Pool BW]：サブプールまたはグローバル プールのいずれかを保護するために保留する帯域幅。
  - [Sub Pool (BC1) BW]：サブ プール用に保留する帯域幅。
  - [Global Pool (BC0) BW]：グローバル プール用に保留する帯域幅。

  プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- [Tunnel Number]：トンネル インターフェイスの名前に対応するトンネル番号。
  - [Auto Gen]：プロビジョニング時にトンネル番号を生成する場合は、このボックスをオンにします。オンにしない場合は、希望する番号を入力します。

  （注）　手動で入力したトンネル番号が小さすぎると、展開の妨げになるおそれがあります。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [Tunnel Bandwidth]：このバックアップ トンネルで許可される合計帯域幅（表示のみ）。

- [Tunnel Pool Type]：このポリシーのトンネル帯域幅プール タイプ（表示のみ）。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
  - [Global Pool (BC0)]：帯域幅はグローバル プールから予約されます。
  - [Sub Pool (BC1)]：帯域幅はサブプールから予約されます。
- [Setup Priority (0-7)]、[Hold Priority (0-7)]、[Affinity]、[Affinity Mask]：手動で作成するすべてのバックアップ トンネルでは、セットアップ プライオリティおよび保持プライオリティがいずれも 0 で、アフィニティ値およびマスクが 0x0 の場合に限り、要素を保護できます。

パス オプション：

- [Option #]：使用可能な明示的パスの連続番号。
- [Path Name]：明示的パスの名前。
- [Path Type]：明示的パス タイプ（[Explicit] または [Dynamic]）。
- [Lock Down]：オンにした場合は、トンネルに対する再最適化検査がディセーブルになります。

ステップ 3　最低限、[Head Device]、[Destination Device]、および [Protected Interface] を選択します。

ゼロより大きい [Backup Bandwidth Limit] も指定してください。必要に応じて他のトンネル情報を追加します。

ステップ 4　[Add] をクリックして、1 つのパスだけを追加します。

[Select TE Explicit Path] ウィンドウが表示されます。

ステップ 5　明示的パスを選択します。

これは既存のパスのヘッドおよび宛先と一致している必要があります。使用可能なものがない場合は、まず設定する必要があります。これを行うには、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 6　[Select] をクリックします。

選択したパスが、[Select TE Explicit Path] ウィンドウに示すように、ページの [Path Options] セクションに表示されます。

明示的パスの場合は、パス名をクリックして明示的パス ビューアを開くことができます。

ステップ 7　[Create TE Backup Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして保存せずにウィンドウを終了します。

[TE Protection SR] ウィンドウで、[Op] フィールドに [ADD] を設定した新規バックアップ トンネルがトンネル リストに追加されています。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 8　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、バックアップ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Save & Deploy] ボタンには 2 つのオプションがあります。

- [SR Tunnels Only]：トンネル配置に影響しないトンネルのすべての変更を展開するか、SR に変更が加えられていない場合に、このオプションを使用して、[Requested] 状態または [Invalid] 状態だった SR を再展開します。
- [Force Deploy All Tunnels]：この SR に含まれるすべてのトンネルを強制的に展開します。SR の前回プロビジョニングが失敗し、SR に含まれるすべてのトンネルを強制的に展開する必要がある場合に有用です。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注）　TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Operate] > [Service Request Manager] ページからではなく、常に特定の [TE SR] ウィンドウからすぐに展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

バックアップ トンネルの編集

バックアップ トンネル属性はバックアップ トンネル エディタで変更できます。

バックアップ トンネル エディタにアクセスする方法は 2 通りあります。

- [Protection SR] ウィンドウからアクセス
- [Service Requests] ウィンドウから

[Protection SR] ウィンドウから

[Protection SR] ウィンドウにアクセスしてバックアップ トンネルを編集するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

ステップ 2　トンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Edit TE Backup Tunnel] ウィンドウが表示されます。バックアップ トンネル エディタは、バックアップ トンネル作成 GUI のエディタと同じです。さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

ステップ 3　必要な変更を加えて [OK] をクリックします。

[TE Protection] ウィンドウで [Op] フィールドが [MODIFY] に変わります。

（注）　変更したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [MODIFY] フラグが消えます。

ステップ 4　[TE Protection SR] ウィンドウで、[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、バックアップ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウから

SR がすでに作成されている場合に [Service Requests] ウィンドウからバックアップ トンネルを編集するには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　必要なトンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Service Request Manager] ウィンドウで選択した SR を表示している [TE Protection SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を選択し、[Edit] をクリックします。

[Edit TE Backup Tunnel] ウィンドウが表示されます。

「バックアップ トンネルの編集」（P.7-44）に移動し、ステップ 3 から処理を続行します。

バックアップ トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ（「TE トンネルの削除」（P.7-26）を参照）、またはプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます。

[TE Protection SR] ウィンドウからバックアップ トンネルを削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

ステップ 2　トンネル SR を削除するために、削除する SR を選択し、[Delete] をクリックします。

管理対象外トンネルの [Op] フィールドのステータスが [DELETE] に変わります。

さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

（注）　削除したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [DELETE] フラグが消えます。

[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

サービス要求の削除

[Service Request Manager] ウィンドウにある [Purge] 操作は、ネットワークに影響を与えることなくリポジトリからサービス要求を削除することを目的としています。

[Purge] ボタンには 2 つのオプションがあります。

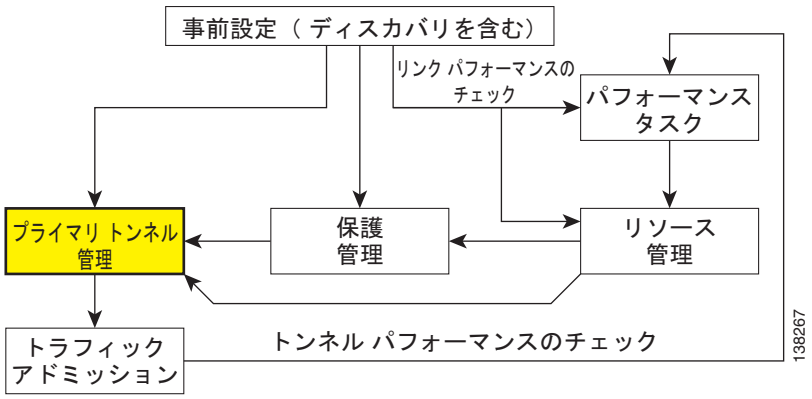
- [Purge]：通常の削除は、[CLOSED] 状態にあるサービス要求のみに使用できます。したがって、TE リソース、TE トンネル、および TE 保護サービス要求に対しては使用できません。これらは撤去できないためです。これらの 3 つのサービス要求タイプは、強制削除のみ可能です。
- [Force Purge]：強制削除では、リポジトリでサービス要求に対する必要な依存関係を検査してから削除が可能になります。したがってサービス要求を削除できない場合は、エラー メッセージが出されます。

高度なプライマリ トンネル管理

「基本的なトンネル管理」（P.7-28）で説明している基本的なトンネル管理ツールに加え、Prime Provisioning では、最適なトンネル配置を実現し、ネットワーク リソースの効率的な使用を保証する、一連の高度なトンネル計画ツールにアクセスできます。

図 7-3 で強調表示されているボックスは、Prime Provisioning のプライマリ トンネル管理が発生した場所を示します。

図 7-16　Prime Provisioning プロセス図：プライマリ トンネル管理



高度なツールは、管理対象のトンネルにのみ使用できます。管理対象トンネルと管理対象外トンネルの違いは、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象/管理対象外プライマリ トンネルの項で説明します。

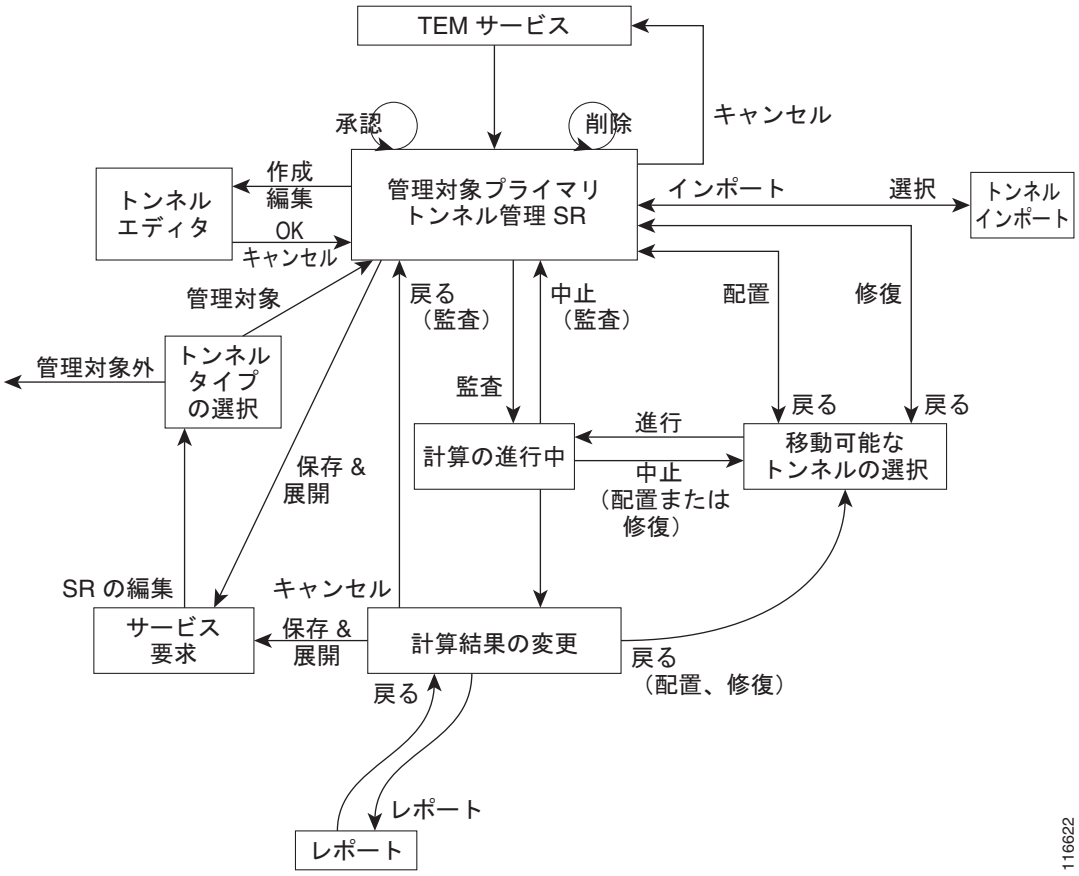
ここでは、次の内容について説明します。

トンネル操作

ここでは、計画ツールを組み込む Prime Provisioning の高度なトンネル操作について説明します。

プライマリ トンネル管理プロセスの概要については、図 7-17 を参照してください。

図 7-17　プライマリ トンネル管理プロセス



[Tunnel Type Selection] で、[Unmanaged] を選択していると [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます（「基本的なトンネル管理」（P.7-28）を参照）。

図 7-17 のその他のすべての要素は、この項で説明します。

プライマリ トンネルの作成

RG ライセンスがインストールされた状態で TE 管理対象プライマリ トンネルを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 3　[Create] をクリックします。

[Create TE Managed Primary Tunnel] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

[Path Options] セクションには、3 つのパス タイプ [System Path]、[Explicit Path]、および [Dynamic Path] が示されます。

[System Path] は、Prime Provisioning システムによって生成される明示的パスです（固定）。最初のパスは明示的パスでなければなりません。

[Explicit Path] は、特定のヘッドから特定の宛先デバイスへの固定パスです。

[Dynamic Path] は、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。

ステップ 4　[Head Device] を選択するために、対応する [Select] ボタンをクリックしてデバイス選択ウィンドウを開きます。

ヘッド デバイスを選択し、[Select] をクリックします。

ステップ 5　[Destination Device] を選択するために、対応する [Select] ボタンをクリックしてデバイス選択ウィンドウを開きます。

テール デバイスを選択し、[Select] を選択します。

ステップ 6　[Tunnel Policy] を選択するために、対応する [Select] ボタンをクリックしてポリシー選択ウィンドウを開きます。

（注）　使用可能なトンネル ポリシーがない場合、その理由は、すべてが管理対象外である可能性があります。管理対象トンネルを作成するには、[Managed] チェックボックスを必ずオンにして、まず、[Service Design] > [Policy Manager]（「ポリシーの作成」（P.7-73）を参照）で管理対象ポリシーを作成します。

[Select Managed TE Tunnel Policy] ウィンドウには、次の要素が含まれています。

- [Policy Name]：TE ポリシー名。
- [Pool Type]：このポリシーのトンネル帯域幅プール タイプ。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。
  - [SUB_POOL]：帯域幅は、サブ プールから予約されます。
  - [GLOBAL]：帯域幅は、グローバル プールから予約されます。
- [Setup Priority]：優先する既存のトンネルを判別するために、トンネルの LSP をシグナリングするときに使用される優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。したがって、セットアップ プライオリティが 0 の LSP は、0 以外の保持プライオリティのすべての LSP より優先されます。
- [Hold Priority]：シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定するため、トンネルの LSP に関連付けられた優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。
- [Affinity]：トンネルを伝送するリンクで必要な属性値（ビット値は 0 または 1 のいずれか）。
- [Affinity Mask]：チェックする属性値。マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。マスクのビットが 1 の場合、そのビットに対するリンクの属性値とトンネルに必要なアフィニティは一致する必要があります。
- [Delayed Constraint]：True または False の値。true の場合、トンネルには、パスが超えてはならない最大遅延があります。
- [FRR Protection]：バックアップ トンネルが存在しており、リンク障害が発生した場合に、MPLS トラフィック エンジニアリング トンネルで、バックアップ トンネルの使用をイネーブルにするために使用します。
  - [None]：バックアップ トンネルは必要ありません。
  - [Best Effort]：可能な場合に、バックアップ トンネルを使用します。

- [Link and SRLG (only managed tunnels)] : FRR バックアップ トンネルで保護されるリンクと SRLG だけを通じて、プライマリ トンネルをルーティングする必要があることを指定します。
- [Link, SRLG and Node (only managed tunnels)] : FRR バックアップ トンネルで保護されるリンク、SRLG、およびノードだけを通じて、プライマリ トンネルをルーティングする必要があることを指定します。

• [MPLS IP Enabled] : MPLS IP が対応するトンネルで設定されているかどうかを示します。

ステップ 7　ゼロより大きいトンネル帯域幅を指定します。

ステップ 8　必要に応じて他のトンネル情報を追加します。

ステップ 9　オプションで、Prime Provisioning によって提供されるシステム パスを使用せずに、明示的パスを指定したい場合は、システム パスを削除し、次に明示的パスを追加します。

このステップの詳細については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 10　[Create TE Managed Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして終了し、[TE Managed Primary Tunnels SR] ウィンドウに戻ります。

SR が追加されたことを示す [ADD] を [Op] フィールドに設定した新規トンネルを表示している [TE Managed Primary Tunnel SR] ウィンドウが表示されます。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 11　[TE Managed Primary Tunnel SR] ウィンドウで、より多くのトンネルを作成または編集できます。また、すべての変更が完了した場合は、次のどちらのボタンがアクティブであるかに応じて、次の 2 つの方法のいずれかに進みます（[Save & Deploy] は、[Create] 操作の後は使用できません）。

- [Proceed with Changes] : 入力した変更は、トンネル配置に影響を与えます。SR を保存および展開できるまで、配置ツールに記載されている計画フローのいずれか（「配置ツール」（P.7-54）を参照）を使用して続行するには、これをクリックします。
- [Save & Deploy] : 入力した変更は、トンネル配置に影響を与えません。SR を保存および展開するには、これをクリックします。この機能は、「プライマリ トンネルの作成」（P.7-33）で詳細に説明されています。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Inventory and Connection Manager] の [Service Requests] ページではなく、常に特定の [TE SR] ウィンドウから直接展開されます。

ステップ 11 で [Save & Deploy] を選択した場合、[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が開き、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

（注）　TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「タスク ログ」（P.10-29）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

プライマリ トンネルの編集

トンネルの作成と編集の唯一の違いは、トンネル エディタでは、ヘッド デバイス、宛先デバイス、およびトンネル番号のフィールドを編集できないことです。それ以外の場合は、同じ属性を作成および編集できます。

入力した変更がトンネル配置に影響するかどうかに応じて、両方ではなく、[Proceed with Changes] または [Save & Deploy] だけが使用可能です。

プライマリ トンネルを編集する場合は、「プライマリ トンネルの編集」（P.7-38）を参照してください。

プライマリ トンネルの削除

1 つ以上のトンネルを削除するには、「プライマリ トンネルの削除」（P.7-40）を参照してください。

プライマリ トンネルのアドミッション

アドミッション機能は、選択した以前検証されていないトンネルを管理対象トポロジにアドミッションします。この機能は、検証が失敗した検出済みのトンネルにのみ使用します。ディスカバリ プロセスでは、トンネルを初めてアドミッションすると想定し、トンネル配置アルゴリズムによって検証が実行されます。

ここでいう検証は、検出された管理対象トンネルをネットワーク トポロジと照合して検証することおよび十分な帯域幅のあるトンネル パスであるかどうかを TEM によって検査すること（いずれもトンネルに指定）を意味します。

一般的に、他のトンネルまたはリンク キャパシティ / 帯域幅の制限の存在が原因で、帯域幅が十分ではない場合、検証が失敗します。

具体的には、これは、優先順位 0 のトンネルが TEM とは独立して作成され、TE 検出タスクが実行された場合に発生する可能性があります。管理対象トンネルの制約の一部を満たさない（つまり、通過するリンクで使用可能な帯域幅より多い帯域幅を予約する）トンネルの場合、TE ディスカバリでは、そのトンネルの「verified」に「false」とマークします。これは、[Admit] ボタンを使用して検証が行われるまで、TEM による管理対象になりません。通常、制約が現在満たされていることを保証するために、これには他のトンネルまたはリソース変更が伴う必要があります。

プライマリ トンネルのアドミッションを行うには、次のステップを実行します。

ステップ 1　[TE Managed Primary Tunnel SR] で、移行する 1 つ以上の未検証のトンネルを選択します。

ステップ 2　[Admit] をクリックします。

未検証のトンネルが検証され、成功した場合は、[Op] 列に [ADMIT] フラグが表示されます。

ステップ 3　[Proceed with Changes] > [Tunnel Placement] を選択して、トンネルを配置できるかどうかを判別します。そうでない場合は、トンネルを編集し、再度試行します。

プライマリ トンネルのインポート

この機能を使用すると、ファイルベースのインポート メカニズムを介してトンネルを一括して更新することができます。データは、管理対象プライマリ トンネル サービス要求に移行されます。

XML インポート ファイルの作成

ファイルからトンネルをインポートするには、まず、システムが提供する文書型定義（DTD）ファイル（「ドキュメント タイプ定義（DTD）ファイル」（P.7-112）を参照）で定義された構造に準拠している XML インポート ファイルを作成します。次に、Prime Provisioning サーバで、同じディレクトリに DTD ファイルとともに XML ファイルを保存します。有効なインポート ファイルを作成するには、提供されたコマンドライン検証ツール（「コマンドライン検証ツール」（P.7-52）を参照）を使用します。

次のファイルは、Prime Provisioning アプリケーションへのデータのインポートに必要であり、インストールに含まれています。

- 次にあるインポート ファイルの DTD ファイル
  < *installedDir*>/ *resources/java/xml/com/cisco/vpnsc/ui/te*
  - **TeImport.dtd**

    （サンプル ファイル **sample.xml** も含まれます）
- <*installedDir*>*/bin* ディレクトリでコマンドライン バリデータを実行するためのシェル スクリプト
  - **ImportTeTunnels**

    使用方法：**importTeTunnels <***importfile***>**

importfile は XML ファイルであり、**TeImport.dtd** をその DTD として指定する必要があります。**TeImport.dtd** は、*importfile* と同じディレクトリにある必要があります。

コマンドライン検証ツール

コマンドライン バリデータの目的は、**TeImport.dtd** に対応する有効なインポート ファイルのオフラインでの作成を支援することです。このツールは、整形式でないファイルおよび DTD によって設定されるルールに準拠していないファイルに関連するエラーを排除するために有用です。

DTD ファイルの使用法については、DTD ファイルのマニュアルを参照してください。

ツールはインポート ファイルを行単位で読み取り、解析時に出力上で各行をエコーし、発生した解析エラーをレポートします。解析および検証は、解析エラーが発生した場合であっても、ファイル構造が意味を持つ限り続行されます。

（注） このツールでは、クロス フィールド検証を行わず、Prime Provisioning アプリケーションの観点からのデータ完全性エラーを検査しません。

インポート手順

ファイルベースのインポート機能は、サービス要求にコミットされていない新規のトンネル、変更されたトンネル、削除されたトンネルが存在しない場合のみイネーブルになります。

多数のトンネルを一度に追加、編集、削除、または移行できます。

インポート手順を開始するには、次のステップを実行します。

ステップ 1　DTD ファイルに準拠した XML インポート ファイルを準備します。

ステップ 2　[Traffic Engineering] に移動します。

ステップ 3　このセッションでまだプロバイダーを選択していない場合は、プロバイダーを選択します。

ステップ 4　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 5　[Import] をクリックし、インポート プロセスを開始します。

[Select Import File] ウィンドウが表示されます。

（注）　[Import] ボタンは、サービス要求にコミットされていない新規のトンネル、変更済みのトンネル、または削除されたトンネルが存在する場合のみイネーブルになります。

[Select Import File] ウィンドウには、[Look in] フィールドに表示されるディレクトリ名の下に、すべての XML ファイルとディレクトリが示されます。

[Look in] フィールドに表示されているデフォルト ディレクトリは、DTD およびサンプル XML ファイルが存在するインストール ディレクトリに対応します。

ステップ 6　インポート操作で使用する、必要な XML ファイルを選択します。

ファイルが解析されます。何らかのエラーが検出された場合は、[Tunnel Import Error Status] ウィンドウに報告されます。

[Tunnel Import Error Status] ウィンドウに、ファイルの URL、最後に変更されたタイムスタンプ、インポート ステータス、およびエラー / 警告メッセージが表示されます。

ステップ 7　インポート操作が失敗した場合は、[Cancel] をクリックして前のウィンドウに戻ります。

部分的に成功した場合は、[Continue] ボタンがイネーブルになるため、エラーおよび警告に対するシステム処置を受け入れる追加のオプションを指定して、インポート操作を続行します。

ステップ 8　ファイルが正常に解析された、または [Continue] をクリックした場合、ファイルのすべての有効なトンネルがサービス要求に追加され、SR ビューで [TE Managed Primary Tunnels SR] ウィンドウが再表示されます。インポートされたトンネルが、適切なトンネル **Op** タイプと表示されます。

計画ストラテジ

計画ツールを使用する主な目的は、ネットワーク上の既存のトラフィックへの影響の発生を最小限にする一方で、ネットワーク全体の最適な利用を実現することです。

ほとんどの場合、次のストラテジを適用できます。

- 既存トラフィックを移動させないで、使用率を最適化しながら新規トラフィックのアドミッションを試行する（配置機能）。これにより、既存のトラフィックを変更せずに、新しいトラフィックに適応することが可能になります。一方で、予約済み帯域使用率は、既存のトンネルを移動しない制約のもとで引き続き最適化されます。
- これが失敗した場合、変更を最小化する同じ新しいトラフィックの既存のトラフィックへのアドミッションを試行し（修復機能）、必要以上に既存のトンネルに影響を与えずに新しいトラフィックを適応できるかどうかを確認します。
- 新しいネットワーク トラフィックの配置が成功したが、希望よりも全体の予約済み帯域使用率が高い場合は、ネットワークのグルーミングを検討してください。
- 修復に失敗する場合は、検討可能な変更の数を制御するパラメータを確認します。また、希望のトラフィックへの指定は変更でき、リソースの変更を実行できます。

このストラテジは、ソリューションを探求するさまざまなアルゴリズムで採用されているさまざまなアプローチを反映します。ただし、他の組み合わせが可能です。

配置ツール

プライマリ トンネルの計画ツールは、変更が管理対象プライマリ トンネルに行われたかどうかによって、[TE Primary Tunnel SR] ウィンドウの [Proceed with Changes] および [Placement Tools] ボタンから使用できます。

- [Proceed with Changes]：トンネルに変更（追加/変更/削除/アドミッション）を加えている場合に使用します。トンネル操作については、「トンネル操作」（P.7-47）を参照してください。次に、いずれかの配置ツールを選択して、システムと照合しながら初期配置を検証して展開を続行します。このボタンは、[Resource Management] でも使用可能です。
- [Placement Tools]：既存のネットワークの計画機能を実行するために使用されます。
  - [Tunnel Audit] オプションは、既存の管理対象プライマリ トンネルの制約ベースの配置と既存のネットワーク トポロジを検証するために使用する必要があります。このオプションを使用して、プライマリ配置の最適性を確認することができます。プライマリ トンネルで「ベスト エフォート」より上の保護レベルが必要な場合は、保護ネットワークで変更が行われた後に、監査を実行することも重要です。監査の結果が警告/違反の場合は、[Tunnel Repair] オプションを使用して、ソリューションを見つけることができます。
  - [Groom] オプションは、プライマリ配置の最適化に使用します。すべてのプライマリの計算において、帯域幅プールの最適性および使用率を表示する品質レポートが生成されます。まず、トンネル監査を実行して、ネットワークでグルーミングが必要かどうかを判断することができます。

計画ツールの詳細については、次の項で説明します。

（注） 配置ツール（auto-bw frequency など）でサポートされていないトンネル属性がサポートされている属性とあわせて変更された場合は、[TE Computation Results] ウィンドウに属性が正しく表示されます。ただし、サポートされていない属性のみが変更された場合、[TE Computation Results] ウィンドウには行われていない変更のみが表示され、変更を展開できないように [Save & Deploy] ボタンはグレー表示されます。

トンネル監査

トンネルの変更または TE リソースの変更の任意のタイプの変更が必要な場合は、変更によって生じる不一致（ある場合）を判断するためにトンネル監査が実行されます。また、トンネル監査は、ネットワーク利用の最適化を確認するためにいつでも使用できます。

監査は、プライマリ トンネル ウィンドウからか [TE Links List] ウィンドウから実行できます。（「TE リソース管理」（P.7-21）を参照）。

作成したトンネルで監査を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

トンネル監査は、次の 2 つの方法で使用できます。

- 1 つ以上のトンネルを作成したか、その属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] を選択することによってトンネル監査をアクティブにできます。
- 変更が行われていない場合、[Placement Tools] を選択することによってトンネル監査にアクセスできます。

この例では、新規プライマリ トンネル SR が作成されています。

[TE Managed Primary Tunnel SR] ウィンドウが表示されます。

ステップ 3　[Proceed with Changes] > [Tunnel Audit] を選択します。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

このウィンドウには、次の要素が含まれます。

[Status] セクション（上部）

- [Computation Status]：計算が、成功したか、または失敗したかを示します。
- [Tunnels]：
  - [unplaced]：合計内で、配置されていないトンネルの数。
  - [moved]：移動されたトンネルの数。
- [Bandwidth - unplaced]：すべての既存および新規トンネルの合計帯域幅の内、配置されていないトンネル帯域幅の量。
- [Global Util.]：グローバル プール帯域利用率。

  使用率の値は、次のいずれかです。
  - [Global Pool]：さまざまなグローバル プール属性の比較データ。
  - [Sub Pool]：さまざまなサブ プール属性の比較データ。
  - [Median]：すべてのリンクを使用率で順序付けした場合に、中間であるリンクの使用率。
  - [Max. Modifiable]：通過する移動可能なトンネルがあり、最も使用されているリンクの使用率の値。
  - [Mean]：ネットワーク全体の平均リンク使用率。
  - [Max.]：トポロジ内で最も使用されているリンクの使用率の値。
- [Sub Pool Util.]：サブプール帯域利用率。
- [Solution]：生成されたソリューションの使用率。
- [Original]：元の配置の使用率。

[Changes] セクション（左方）

- [Changes]：変更の合計数の内、実現した変更の数。
  - [Achieved]：特定の変更が成功したかどうかを示します（[Yes] または [No]）。
  - [Origin]：変更の実行元。[user]（ユーザによる変更）または [compute]（トンネルの再ルーティングなどの計算による変更）にすることができます。
  - [Type]：要求された変更のタイプ（[Tunnel Add Change]、[Tunnel Modify Change]、[Tunnel Remove Change]、または [Element Modify Change]）。
  - [Object ID]：トンネルまたはリンクの ID。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 4　トンネルの詳細情報を取得し、変更要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Details] をクリックします。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 5　監査レポートを表示するには、[View Report] をクリックします。

場合によっては、qualityReport と違反レポートの両方が生成されます。

ステップ 6　**qualityReport** の内容を表示するには、**qualityReport** を選択し、[Details] ボタンをクリックします。

右ウィンドウ ペインの qualityReport フィールドには、次の要素が含まれます。

[Status] セクション（上）：上に説明があります。

[Report] セクション（左）：

- [Report Type]：**qualityReport**（毎回生成されます）、警告レポート、および違反レポートの 3 種類の基本的なレポート タイプがあります。
- [Summary Info]：レポートの結果に関するサマリー情報。

[Information] セクション（右）

- [Report Type]：上記の説明を参照してください。
- [Description]：レポートに関する特定の情報。
- [Achievement]：計算の試行やソリューションの成功または失敗（**SUCCESS** または **CONSTRAINT_VIOLATIONS_REPORTED**）。
- [Solution]：ソリューションが見つかったかどうかを示します（**SOLUTION_FOUND**、**PARTIAL_SOLUTION_FOUND** または **NO_SOLUTION_FOUND**）。
- [Termination]：計算が完了したかどうかを示します。
  - [COMPLETED]：計算の処理は、制限時間の前に完了しました。
  - [TIMED_OUT]：計算の処理は、時間制限内に完了できませんでした。表示されるソリューションは、使用可能な時間内に検出できた最善のソリューションです。
- [Optimality]：計算が最適であったかどうかを示します。
  - **OPTIMAL_FOR_ALL_CRITERIA**：生成されるソリューションは、すべての最適化基準で最適であることが実証されています。
  - **NO_OPTIMALITY_PROOF**：ソリューションの最適性が不明です。
  - **OPTIMAL_FOR_DEMAND_SELECTION**：生成されたソリューションは、配置された合計帯域幅に関して最適であることが証明されましたが、使用率の最適性は不明です。

OPTIMAL_FOR_SUB_POOL_PATH_SELECTION：生成されたソリューションは、配置された合計帯域幅と最大サブ プール使用率に関して最適であることが証明されましたが、グローバル プールの使用率に関して最適であることは証明されませんでした。

ステップ 7　違反レポートの内容を表示するには、違反レポートを選択し、[Details] ボタンをクリックします。

[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻ります。

提示された変更が行われた場合は、[Save & Deploy] をクリックして実現可能な変更をリポジトリに保存し、ネットワークにトンネルの変更を実装します。

（注）　[Save & Deploy] では、実現不可能な変更は破棄されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

トンネル配置

配置機能は、ネットワークへの新規のトンネルのアドミッション、およびネットワークへのアドミッションがすでに行われている変更をサポートしています。 Prime Provisioning は、ネットワーク利用が最適化される方法で、変更の実装を試行します。

作成したトンネルを配置するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　1 つ以上のトンネルを作成したか、その属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] > [Tunnel Placement] を選択します。

[Movable Tunnel Selection (Placement)] ウィンドウが表示されます。

ステップ 4　移動可能または移動不能な管理対象トンネルを設定します。

新規のトンネルのアドミッションを行う場合は、既存のトンネルを移動（リルート）できるかどうかを指定できます。ユーザが設定できます。デフォルトでは、管理対象トンネルは移動不能です。

ステップ 5　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 6　トンネルの詳細情報を取得し、配置要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

配置リクエストが正常に完了した場合（[Achieved] : yes）、[Detail] ペインには選択可能な計算済みの**パス**が含まれます。

パス情報を表示するには、計算された [Path] フィールドの青色のリンクをクリックします。[TE Explicit Path] ウィンドウが表示されます。

ステップ 7　配置レポートを表示するには、[Changes] ウィンドウの [View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 8　配置レポートの内容を表示するには、レポートのいずれかを選択し、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが右側のレポート ペインに表示されます。

ステップ 9　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

トンネル修復

既存のトンネルの帯域幅要件または遅延パラメータに変更が行われると、トンネル配置に不一致が生じます。トンネル修復を実行して、このような不一致に対処できます。トンネル修復は、できるだけ少ない既存のトンネルを移動して、変更に対応できるようにすることを目的としています。

修復操作は、プライマリ トンネル ウィンドウからか [TE Links List] ウィンドウから実行できます（「TE リソース管理」（P.7-21）を参照）。

次では、編集済みトンネルの修復を行います。

ステップ 1　[Traffic Engineering] > [Create Managed Tunnel] を選択します。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

トンネル修復は、次の 2 つの方法で使用できます。

- 1 つ以上のトンネルを作成したか、トンネルの属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] > [Tunnel Repair] を選択することによってトンネル修復をアクティブにできます。
- 変更が行われていない場合、トンネル修復には、[Placement Tools] > [Tunnel Repair] を選択してアクセスできます。

ステップ 2　この例では、新規プライマリ トンネル SR が作成されています。

[TE Managed Primary Tunnels SR] ウィンドウから変更したトンネル上でトンネル修復を実行します。これには、次のように移動します。

[Proceed with Changes] > [Tunnel Repair]

[Movable Tunnel Selection] ウィンドウが表示されます。

ステップ 3　移動可能にする必要のあるトンネルを設定します。

トンネル修復は、必要な場合に限り、既存のトンネルを移動します。トンネル修復で移動しない特定のトンネルがある場合は、そのトンネルを移動可能なトンネルの選択リストから明示的に除外する必要があります。

[Maximum number of tunnel moves] フィールドを使用して、受け入れ可能なトンネル移動の最大数の制限を指定することもできます。

（注）　デフォルトでは、変更済のトンネルを移動可能に設定する必要はありません。

ステップ 4　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　トンネルの詳細情報を取得し、変更要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

ステップ 6　修復レポートを表示するには、[View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 7　修復レポートの内容を表示するには、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

グルーミング

グルーミングは、ネットワーク要素に関してトンネルのパスを分析することと、リソース割り当てを最適化することを目的としています。

グルーミングは、変更要求が作成されている場合は使用できません。その場合は、[Proceed with Changes] の下の配置ツールだけが使用可能です。

ネットワークでグルーミングを実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create Managed TE Tunnel] を選択します。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 2　次に移動して、グルーミングを実行します。

[Placement Tools] > [Groom]

[Movable Tunnel Selection] ウィンドウが表示されます。

ステップ 3　移動可能にする必要のあるトンネルを設定します。

トンネル修復では、グルーミングは必要な場合にのみ既存のトンネルを移動します。グルーミング処理で移動しない特定のトンネルがある場合は、そのトンネルを移動可能なトンネルの選択リストから明示的に除外する必要があります。

ステップ 4　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　グルーミングの詳細情報を取得し、グルーミングが成功したかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

ステップ 6　グルーミング レポートを表示するには、[View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 7　グルーミング レポートの内容を表示するには、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

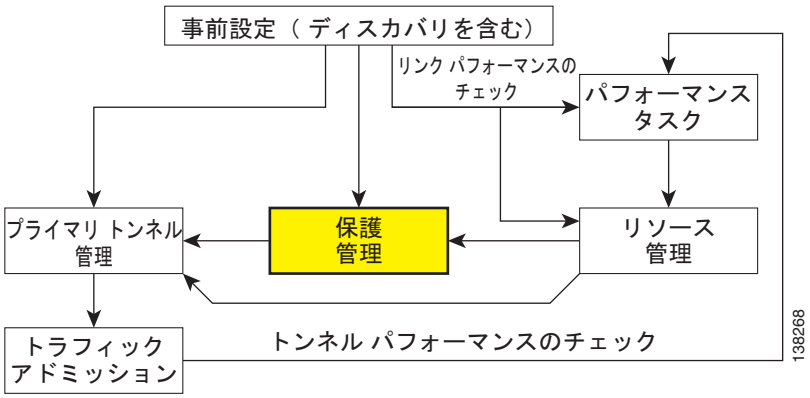
サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

保護計画

ここでは、自動保護ツールを使用してネットワーク要素の保護を作成および管理するプロセスについて説明します。基本的なツールを使用するこのプロセスについては、「基本的なトンネル管理」（P.7-28）を参照してください。

図 7-18 で強調表示されたボックスは、保護管理が Prime Provisioning のどこで行われるかを示しています。

図 7-18　Prime Provisioning プロセス図：保護管理



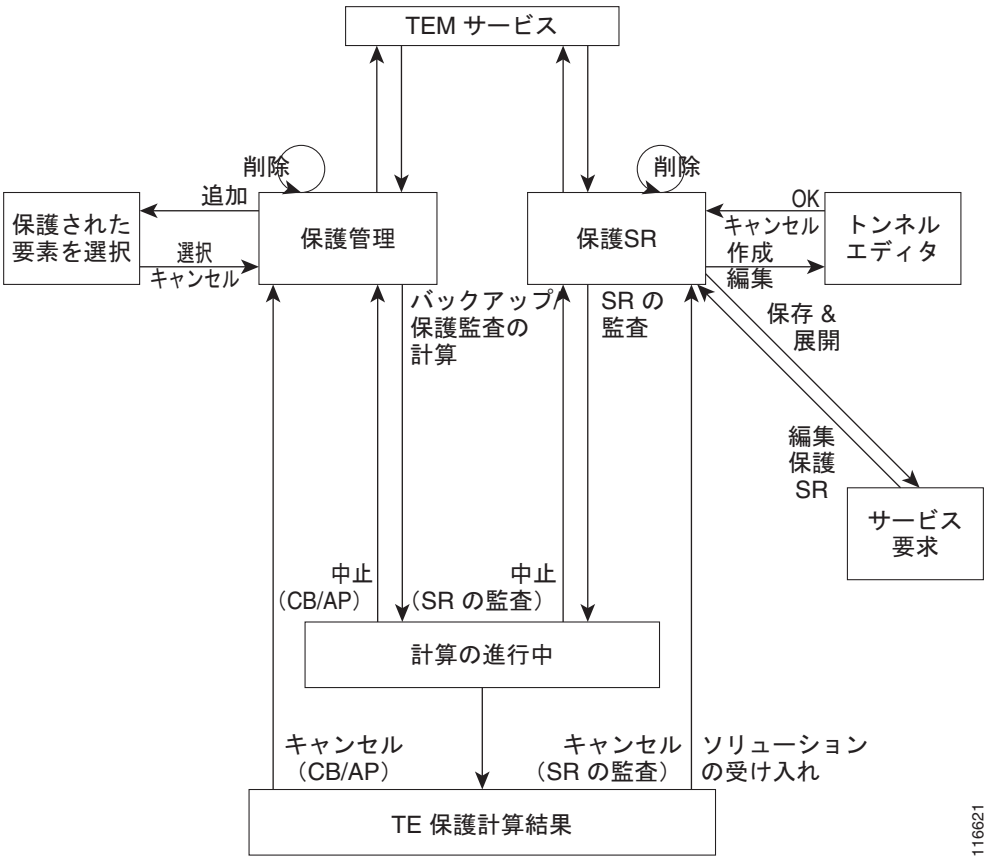
保護計画では、ネットワーク内の選択した要素（リンク、ルータ、または SRLG）を障害から保護することを目的としています。

最初の手順では、保護する必要がある要素を特定し、保護ツールを呼び出して、保護されたトンネルを計算します。計算によって、システムは、要素を保護する一連のトンネル、または保護できなかった理由を判断するために役立つ一連の違反と警告のいずれかとともに、各要素に対して応答します。

正常に保護された要素の場合は、トンネルをネットワークに展開できます。保護できない要素の場合は、保護が無視されるか、保護の場合に制約が変更されます。より具体的には、要素に関連付けられたリンクの TE 帯域幅設定が変更され、変更されたネットワークで保護の計算が再実行されます。

保護管理プロセスの概要は、図 7-19 で提供されます。

図 7-19　保護管理プロセス



ここでは、次の内容について説明します。

- 「SRLG 操作」（P.7-62）
  - 「SRLG の作成」（P.7-63）
  - 「SRLG の編集」（P.7-63）
  - 「SRLG の削除」（P.7-63）
- 「要素保護の設定」（P.7-64）
- 「保護ツール」（P.7-64）
  - 「バックアップ計算」（P.7-65）
  - 「保護監査」（P.7-66）
  - 「監査 SR」（P.7-67）。

SRLG 操作

リンクの物理的特性が同一になることがあります（同じコンジットに物理的に存在する場合や同じハードウェアに接続される場合など）。この結果、単一の障害発生時に、これらのリンクがグループとして失敗することがあります。共有リスク リンク グループ（SRLG）は、一緒に失敗することがあるリンクを特定してこの問題を解決します。

SRLG の変更（作成、編集、削除）後に、[TE Protection Management] ウィンドウで保護計画機能を使用して、適切な保護がネットワークで利用可能になるようにします。

SRLG の作成

SRLG の作成は、共有リスク リンク グループが特定され、共有リスク リンク グループを保護する必要がある場合にのみ必要です。

SRLG を作成するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　[TE SRLG List] で SRLG を作成するには、[Create] をクリックします。

[TE SRLG Editor] ウィンドウが表示されます。

ステップ 3　[SRLG Name] を指定します。

ステップ 4　[Add Link] をクリックします。

SRLG ウィンドウに関連付けられたリンクが表示されます。

ステップ 5　1 つまたは複数のリンクを選択し、[Select] をクリックします。

対応するリンク情報がリンク リストに追加され、[Select] ウィンドウが閉じられて、SRLG エディタに戻ります。

ステップ 6　[Save] をクリックして SRLG を保存します。

これにより、SRLG エディタが閉じられ、新しく作成された SRLG がリストされた [TE SRLG List] がアクティブ ウィンドウとして表示されます。

SRLG の編集

SRLG を編集するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　TE SRLG リストの SRLG を編集するために、[TE SRLG List] ウィンドウから変更する SRLG を選択し、[Edit] をクリックします。

[TE SRLG Editor] ウィンドウが表示されます。

ステップ 3　[Add Link] と [Remove Link] を使用して、選択された SRLG の必要なリンク セットに調整します。

ステップ 4　変更を保存するには、[Save] をクリックします。

SRLG の削除

SRLG を削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　[TE SRLG List] で SRLG を削除するために、[TE SRLG List] ウィンドウから削除する SRLG を選択し、[Delete] をクリックします。[Delete Confirm] ウィンドウが表示されます。

ステップ 3　[Delete] をクリックして確認します。

[Delete Confirm] ウィンドウが閉じられます。[TE SRLG List] ウィンドウが更新されると、削除された SRLG は SRLG リストに表示されなくなります。

要素保護の設定

保護計算を行う前に、ネットワーク要素の保護を設定する必要があります。

ネットワーク要素保護を設定するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Protected Elements] を選択します。

[TE Protection Management] ウィンドウが表示されます。

[Protection Status] フィールドの説明

[Protection Status] : 表示される保護ステータスは、監査が最後に実行された時間から決定されます。監査は、ユーザによって明示的に、または保護 SR が展開されたときに、実行されます。保護ステータスは、ネットワーク要素ごとに示され、[Protected]、[Not Fully Protected]、または [Unknown] のいずれかです。保護ステータスに基づいて要素をソートするには、列ヘッダー [Protected] をクリックします。

ステップ 2　最初に、保護する必要があるネットワーク要素を決定します。

[TE Protection Management] ウィンドウで、[Add] をクリックして保護要素（リンク、ノード、または SRLG）を追加します。[The Select Protection Elements] ウィンドウが表示されます。

シスコ デバイス以外のデバイスに接続されたリンクは保護できず、[Select] 保護要素ウィンドウに表示されません。同様に、シスコ デバイス以外のデバイスと、シスコ デバイス以外のデバイスへのリンクを含む SRLG は保護できず、選択から除外されます。

ステップ 3　保護する 1 つ以上の要素を選択し、[Select] をクリックします。

[Select Protection Element] ウィンドウが閉じられ、[TE Protection Management] ウィンドウが再び表示されます。

次に、適用すべき保護ツールを決定します。これらについては、「保護ツール」（P.7-64）に記載されています。

保護ツール

「基本的なトンネル管理」（P.7-28）で説明するように、バックアップ トンネルの手動の作成に依存しているため、比較的大きく、複雑なネットワークに限らず、独自の制約が生じます。

Prime Provisioning で利用可能な保護ツールは、指定されたネットワーク要素の保護を自動的に計算して確認する複数のツールを提供します。

（注）　説明など特定の属性はこれらのツールで実行する計算に影響を与えず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

バックアップ計算

バックアップ計算は、指定されたネットワーク要素を保護するために必要なバックアップ トンネルを Prime Provisioning に自動計算させるために使用します。手動処理については、「基本的なトンネル管理」（P.7-28）で説明されています。

バックアップ計算を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Protected Elements] を選択します。

ステップ 2　「要素保護の設定」（P.7-64）の説明に従って、必要な保護要素を設定します。

ステップ 3　選択された要素に対してのみバックアップ計算を実行する場合は、バックアップ パスを計算する 1 つまたは複数の要素を選択します。

ステップ 4　[Compute Backup] をクリックし、次のいずれかを選択します。

- All Elements
- Selected Elements

最初に [Computation In Progress] ウィンドウが表示され、次に、[TE Protection Computation Results] ウィンドウが表示されます。

[Element:] テーブルには、保護計算に含まれている各要素の計算結果が表示されます。各要素のステータスは、テーブルの要素ごとに最低 1 行に示されています。ステータスが無効の場合、テーブルには、警告または違反ごとに 1 行が含まれます。

[Element]：テーブルには、次の列があります。

- [Element Name]：保護するネットワーク要素の名前。
- [Type]：ネットワーク要素のタイプ（ノード、リンク、または SRLG）。
- [Report]：計算エンジンから報告されたときに、要素に関連付けられた警告または違反（存在する場合）。
- [Status]：ネットワーク要素の計算のステータス。
  - [Valid Tunnels]：要素はバックアップ トンネルによって十分に保護されています。
  - [InvalidTunnels]：保護監査は、要素が既存のバックアップ トンネルによって十分に保護されていないことを検出しました。
  - [No Solution Exists]：バックアップ計算は、完全に要素を保護することができないことを証明しました。

（注）　説明など特定の属性は保護ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　特定の警告または違反に対応する行を選択して [Detail] をクリックします。詳細説明が右ペインに表示され、選択した項目に関連付けられているバックアップ トンネルが下部ペインに表示されます。

警告と違反の説明については、「警告および違反」（P.7-102）を参照してください。

[Protection Type] 列の説明

- [Protection Type]：トンネルのアクティブ化による保護の副次的効果。次の 3 つの保護タイプがあります。
  - [Protection tunnels]：指定された要素を保護するためにアクティブにできるトンネル。
  - [Side-effect tunnels]：隣接する要素を保護するためにアクティブになるが、指定された要素に障害が発生した場合にもアクティブになるトンネル。
  - [Activated tunnels]：指定した要素に障害が発生した場合にアクティブになり、指定した要素またはネイバーを保護する場合と保護しない場合があるトンネル。

[Backup Tunnel] テーブルには、必要な新規保護トンネルおよび各要素について保持または削除する必要のあるすべての既存トンネルが表示されます。

ステップ 6　提示された保護ソリューションが受入可能であれば、[Accept Solution] をクリックします。

[TE Protection SR] ウィンドウが表示され、システムにより計算されたすべてのトンネルの追加および削除が示されます。

さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

オプションで、トンネルの変更をここで行い、[Audit SR] を実行して、展開する前に保護の必要なレベルを設定することができます（「監査 SR」（P.7-67）を参照）。

ステップ 7　[Save & Deploy] をクリックして、新しいトンネル SR をネットワークに展開します。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Inventory and Connection Manager] の [Service Requests] ページではなく、常に特定の [TE SR] ウィンドウから直接展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が開き、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Monitoring] > [Task Manager] > [Logs]）を参照してください。

保護監査

P.65 で説明されたバックアップ計算ツールとは異なり、保護監査ではバックアップ ソリューションの作成が試行されません。保護監査では、現在の一連のバックアップ トンネルによる指定されたネットワーク要素の保護について検証を試み、検出されたすべての警告および違反を報告します。TE リンクまたは SRLG メンバーシップのリソースなどの TE トポロジで変更がコミットされた場合は、必ず保護監査を実行して、すべての要素の保護ステータスを確認することを推奨します。

計算は、バックアップ計算と同じ計算結果ページに表示されます。計算結果ページから戻ると、[TE Protection Management] ウィンドウの [Protection Status] 列が更新され、各要素の保護のレベルが示されます。

この項では、1 つまたは複数のネットワーク要素に対して保護監査を実行するために必要な手順について説明します。

保護監査を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [TE Protected Elements] を選択します。

[TE Protection Management] ウィンドウが表示されます。

[Protection Status] フィールドの説明

[Protection Status]：表示される保護ステータスは、監査が最後に実行された時間から決定されます。監査は、ユーザによって明示的に、または保護 SR が展開されたときに、実行されます。保護ステータスは、ネットワーク要素ごとに示され、[Protected]、[Not Fully Protected]、または [Unknown] のいずれかです。保護ステータスに基づいて要素をソートするには、列ヘッダー [Protected] をクリックします。

ステップ 2　選択された要素に対してのみ保護監査を実行する場合は、バックアップ パスを計算する 1 つまたは複数のトンネルを選択します。

[Audit Protection] をクリックし、次のいずれかを選択します。

- All Elements
- Selected Elements

[Computation In Progress] ウィンドウが表示されます。

次に、[TE Protection Computation Results] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「バックアップ計算」（P.7-65）を参照してください。

（注）　説明など特定の属性は保護ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 3　特定の要素のバックアップ トンネルを表示するには、要素を選択し、[Details] をクリックします。

[TE Protection Computation Results] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「バックアップ計算」（P.7-65）を参照してください。

ステップ 4　特定の警告または違反に対応する行を選択して [Details] をクリックします。詳細説明が右ペインに表示され、選択した項目に関連付けられているバックアップ トンネルが下部ペインに表示されます。

警告または違反に関連付けられたトンネルには、下部ペインにある [Backup Tunnels] テーブルの [Report] 列でフラグが付けられます。

監査はソリューションではなく評価を提供するため、[Accept Solution] ボタンはグレー表示されます。

警告と違反の説明については、「警告および違反」（P.7-102）を参照してください。

ステップ 5　[Cancel] をクリックして、[TE Protection Management] ウィンドウに戻ります。

保護ステータスが [Protection Status] 列で更新されます。

監査 SR

監査 SR では、[TE Protection Management] ウィンドウのすべての要素の保護を [TE Protection SR] ウィンドウのバックアップ トンネルに対して監査します。

この機能は、展開前に、[TE Protection SR] ウィンドウで、手動で追加、変更、および削除したトンネルに対する保護を監査するために使用できます。

TE バックアップ トンネル SR を監査するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create TE Backup Tunnel] をクリックします。

[TE Protection SR] ウィンドウが表示されます。さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

ステップ 3　保護 SR を監査するために [Audit SR] をクリックします。

（注）　監査 SR は、[TE Protection Management] ウィンドウに要素がある場合のみ有効になります。[TE Protection Management] ウィンドウに要素がない場合は、[Audit SR] ボタンが無効になります（グレー表示されます）。

FRR 監査プロセスが開始され、[TE Protection Computation Results] ウィンドウが表示されます。

このプロセスの残りの説明については、「保護監査」（P.7-66）を参照してください。これらの 2 つのプロセスでは、詳細ウィンドウとレポート ウィンドウはまったく同じです。

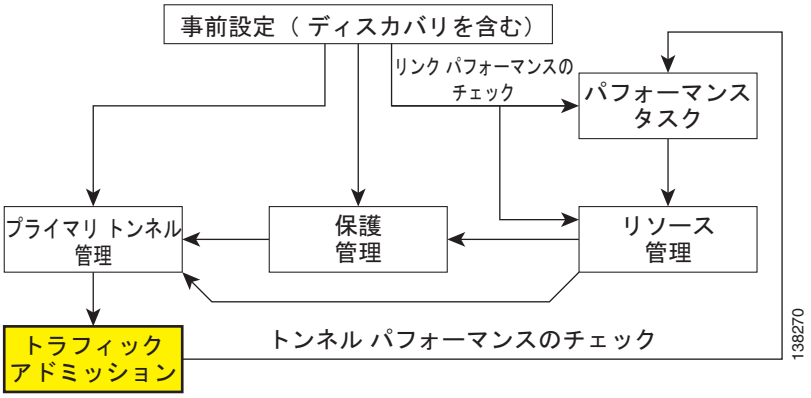
TE トラフィック アドミッション

TE トラフィック アドミッションは、TE トンネルでサービスを有効にするための最初のステップです。トラフィックをトンネルに転送して基本 IP 接続を提供するために使用できるメカニズムは多数存在します。現在の実装では、『Cisco Prime Provisioning Traffic Engineering Management』（Prime Provisioning）トンネルの存在をルーティング プロトコルに通知するために、スタティック ルーティングと自動ルート通知の両方が使用されます。自動ルート通知は、ルーティング プロトコル計算の一部としても使用できます。

TE トラフィック アドミッション ツールは、トラフィック エンジニアリングされたトンネルにトラフィックを割り当てるために使用されます。

図 7-3 で強調表示されているボックスは、Prime Provisioning TE トラフィック アドミッションが発生する場所を示しています。

図 7-20　Prime Provisioning プロセス図 : TE トラフィック アドミッション



スタティック ルーティングは、おそらく、トラフィックをトンネルに転送する最も簡単な方法です。ターゲット宛先プレフィックスと一致するトラフィックは、特定のトンネルにルーティングされます。

これにより、トラフィックを特定のトンネルに転送するという基本的な目的は達成されますが、このアプローチには制約があります。第 1 に、ディファレンシエーテッド サービス クラス（CoS）の処置の提供は、宛先ベースの CoS に制限されます。各ソース PE は複数のトラフィック フローの集約ポイントとして機能し、トンネルへは一般的なルーティングを通してアクセスするため、どのトラフィックが宛先への優先処置を受信するかを制限する方法はありません。第 2 に、スタティック ルーティング メカニズムでは各 PE ルータによって処理できる大量のサブネットのキャプチャに加えて、これらの各サブネットに対する CoS の処置もキャプチャできる必要があるため、通常は、スケーラブルなソリューションにはなりません。

スタティック ルーティングは、宛先によって CoS 処理を区別する必要がない場合に、最適に動作します。つまり、1 つ以上の特定のプレフィックス宛てのすべてのパケットは、すべて同じ CoS を受信します。

ここでは、次の内容について説明します。

- 「TE トラフィック アドミッション SR の作成」（P.7-69）
- 「TE トラフィック アドミッション SR の展開」（P.7-71）
- 「その他のトラフィック アドミッション SR の操作」（P.7-72）
- 「SR 状態の表示」（P.7-72）。

TE トラフィック アドミッション SR の作成

Cisco ISC TEM の TE トラフィック アドミッション ツールでは、トンネルが TE プロバイダーと関連付けられており、TE アドミッション SR とまだ関連付けられていない場合に、プライマリ トンネル（管理対象または管理対象外）だけが表示されます。つまり、このツールでは、現時点でいずれのトラフィックも伝送していない、トンネル宛ての新規トラフィックだけをアドミッションすることを想定しています。

TE トラフィック アドミッション SR を作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[TE Traffic Admission] をクリックします。

[TE Traffic Admission Tunnel Selection] ウィンドウが表示されます。

（注）　このウィンドウが開かない場合は、TE プロバイダーに関連付けられているトンネルがないか、TE プロバイダーに関連付けられているすべてのトンネルが TE アドミッション SR とすでに結びつけられているかのいずれかです。

[TE Traffic Admission Tunnel Selection] ウィンドウには、アドミッション SR と関連付けられていない、管理対象および管理対象外の両方を含むすべてのプライマリ トンネルがリストされます。

[Deploy Status] には、[Pending]、[Deployed]、または [Functional] を指定できます。

（注）　バックアップ トンネルは、[TE Traffic Admission Tunnel Selection] ウィンドウに表示されません。

ステップ 3　対応するオプション ボタンをクリックして TE トンネルを選択し、[Select] をクリックします。

[TE Traffic Admission SR] ウィンドウが表示されます。

[TE Traffic Admission SR] メイン ウィンドウには、次のフィールドが含まれています。

- [Tunnel]：トンネル名。
- [Description]：サービス要求の説明。
- [EXP]（IOS デバイスだけ）：CBTS のクラス マーキング ビット。
- [Policy]（IOS XR デバイスだけ）：PBTS のポリシー マーキング ビット。
- [Autoroute announce]：Interior Gateway Protocol（IGP）で、拡張最短パス優先（SPF）の計算に（トンネルがアップの場合）トンネルを使用することを指定します。
  - [On]：自動ルート通知はイネーブルになります。
  - [Off]：自動ルート通知はディセーブルになります。
- [Autoroute Metric]：マルチ プロトコル ラベル スイッチング（MPLS）のトラフィック エンジニアリング トンネル メトリックを指定するために使用します。これは、Interior Gateway Protocol（IGP）の拡張 Shortest Path First（SPF）の計算で使用されます。
  - [Absolute]：絶対メトリック モード。正のメトリック値を入力できます。
  - [Relative]：相対メトリック モード。正、負、またはゼロの値を入力できます。
- [Static Routes]：トンネルが使用するスタティック ルートが表示されます。
- [Destination]：トンネルの宛先に対するスタティック ルートの名前。
- [Distance]：アドミニストレーティブ ディスタンス（コスト）。

（注）　PBTS 属性などの TE トラフィック アドミッション SR 属性が Prime Provisioning の外部で変更されて TE ディスカバリ タスクが実行される場合、ディスカバリ タスク ログでは不一致警告が報告されず、リポジトリはデバイスからの新規設定で更新されます。

ステップ 4　フォームの入力時に、[Autoroute Announce] を [On] に設定した場合は、[Autoroute Metric] を [Absolute] または [Relative] のどちらにするかを指定します。

ステップ 5　オプションの自動ルート メトリックも設定できます。

相対メトリックの場合、範囲は -10 ～ 10、絶対メトリックの場合、範囲は 1 ～ 2147483647 です。

（注）　CBTS は IOS、PBTS は IOS XR でサポートされます。トンネル ヘッド ルータが IOS XR を実行している場合、[EXP] フィールドは表示される、[PBTS] フィールドに置き換えられます。

[Add] ボタンをクリックすると、[Add TE Static Route] ウィンドウが表示されます。

ステップ 6　[Add TE Static Route] ウィンドウで、**宛先** IP アドレス（w.x.y.z/n）の最小値を指定します。

オプションで、アドミニストレーティブ **ディスタンス**を指定します。1 つ以上のスタティック ルートを定義するか、代わりに自動ルートを定義するかのいずれかを行うことを推奨します。

ステップ 7　エントリを受け入れるには [OK] をクリックし、ウィンドウを閉じるには [Cancel] をクリックします。

メイン [TE Traffic Admission SR] ウィンドウで、別の TE スタティック ルートを追加するか、既存のルートを編集することができます。

ステップ 8　[Save] をクリックして、サービス要求を保存します。

[Service Requests] ウィンドウが表示され、TE トラフィック アドミッション SR が [REQUESTED] 状態になり、操作タイプが [ADD] に設定されていることがわかります。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウからサービス要求を展開する場合は、「TE トラフィック アドミッション SR の展開」（P.7-71）を参照してください。

TE トラフィック アドミッション SR の展開

TE アドミッション SR は、[TE Primary Tunnel SR]、[Backup Tunnel SR]、[TE Resource Modification] ウィンドウではなく、一般的な [Service Requests Manager] ウィンドウから展開する必要があります。

TE アドミッション SR を展開するには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

[Service Requests] ウィンドウが表示されます。

[Service Requests] ウィンドウには、次の要素が含まれています。

- [Job ID] : SR のジョブ ID。
- [Data Files] : このフィールドは、テンプレートを使用した変数の置換に使用され、現在、TEM SR には適用されません。
- [State] : トンネル状態が [DEPLOYED] または [NOT DEPLOYED] であるか、および [Conformed] または [Not Conformed] であるかを示します。
- [Type] : 要求を発行したサービスを示すサービス要求のタイプ。使用可能なサービス タイプの詳細については、このマニュアルのサービス要求の管理の部分を参照してください。
- [Operation Type] : トンネル上の SR 操作。[ADD]、[MODIFY]、[DELETE]、または [ADMIT] のいずれかになります。現在の SR のトンネルにのみ適用できます。
- [Creator] : SR を作成したユーザの ID。
- [Customer Name] : SR が適用されるカスタマーの名前。
- [Policy Name] : SR に関連付けられたポリシーの名前。
- [Last Modified] : SR の最終変更日時。
- [Description] : ユーザが指定した SR の説明。

ステップ 2　目的のサービス要求を選択し、[Deploy] をクリックします。

[Deploy] ボタンの下にドロップダウン メニューが表示されます。ドロップダウン メニューで、[Deploy] または [Force Deploy] を選択します。正常に展開されると、SR の [State] が [Deployed] に変わります。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

その他のトラフィック アドミッション SR の操作

他のサービス要求と異なり、TE トラフィック アドミッション SR は、[Service Requests] ウィンドウでデコミッションできます。

TE トラフィック アドミッション サービス要求の編集およびデコミッション操作は、[Service Requests Manager] ウィンドウで処理されます。これらの操作については、このガイドでサービス要求の管理に関する部分で説明します。

SR 状態の表示

サービス リクエストの状態を表示するには、[Operate] > [Service Request Manager] に移動します。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。「SR 展開ログ」（P.10-48）

管理機能

『Cisco Prime Provisioning Traffic Engineering Management』（TEM）のいくつかの管理機能は、Prime Provisioning と共通です。これらの機能を使用する手順については、*『Cisco Prime Provisioning 6.3 Administration Guide』* から詳細に説明されています。

ここでは、TE 固有の管理機能だけを示します。

ここでは、次の内容について説明します。

TE のユーザ ロール

TE のユーザ ロールは、事前に定義されたロールまたは一連の権限を定義するユーザ指定ロールです。Prime Provisioning のユーザ ロールとその使用方法の詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* を参照してください。

[User Roles] ウィンドウにアクセスし、TE のユーザ ロールを指定するには、[Administration] > [Roles] を選択します。[User Roles] ウィンドウが表示されます。

事前定義された TEM ユーザ ロールには次の 2 つがあります。

- **TERole**：TEM 操作へのすべての権限を与えます。
- **TEServiceOpRole**：TE アドミッション SR のみを管理する権限を与えます。

TE ポリシー

ポリシーは、一般的なトンネル属性を定義するために使用されます。帯域幅プール、保持およびセットアップ優先度、アフィニティ ビットなどの属性は、以下で説明されているように、ポリシーの作成時に手動で設定します。

この項では、次のポリシー操作について説明します。

- 「ポリシーの作成」（P.7-73）
- 「ポリシーの編集」（P.7-75）
- 「ポリシーの削除」（P.7-76）

ポリシーの作成

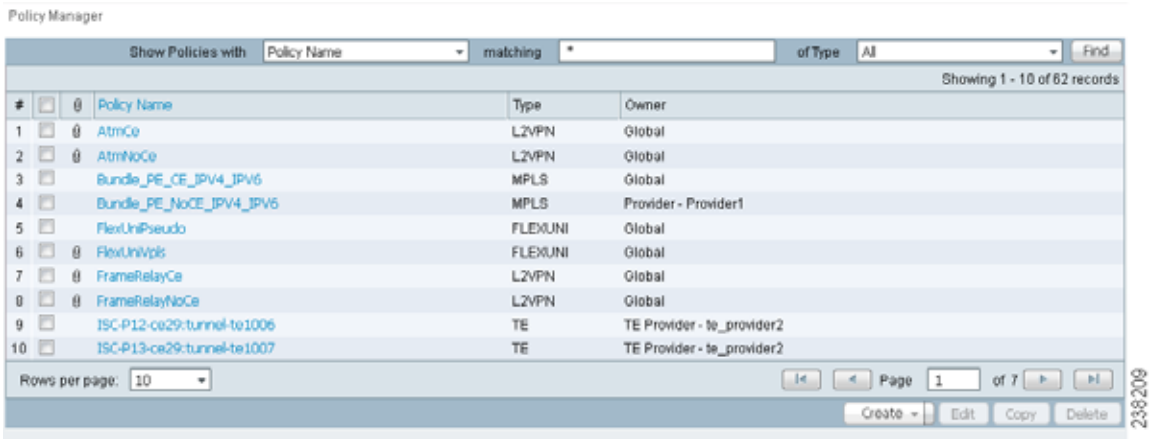
Prime Provisioning では、TE 固有のポリシーを他のポリシーと同様に作成できます。

TE ポリシーを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-21 の [Policy Manager] ウィンドウが表示されます。

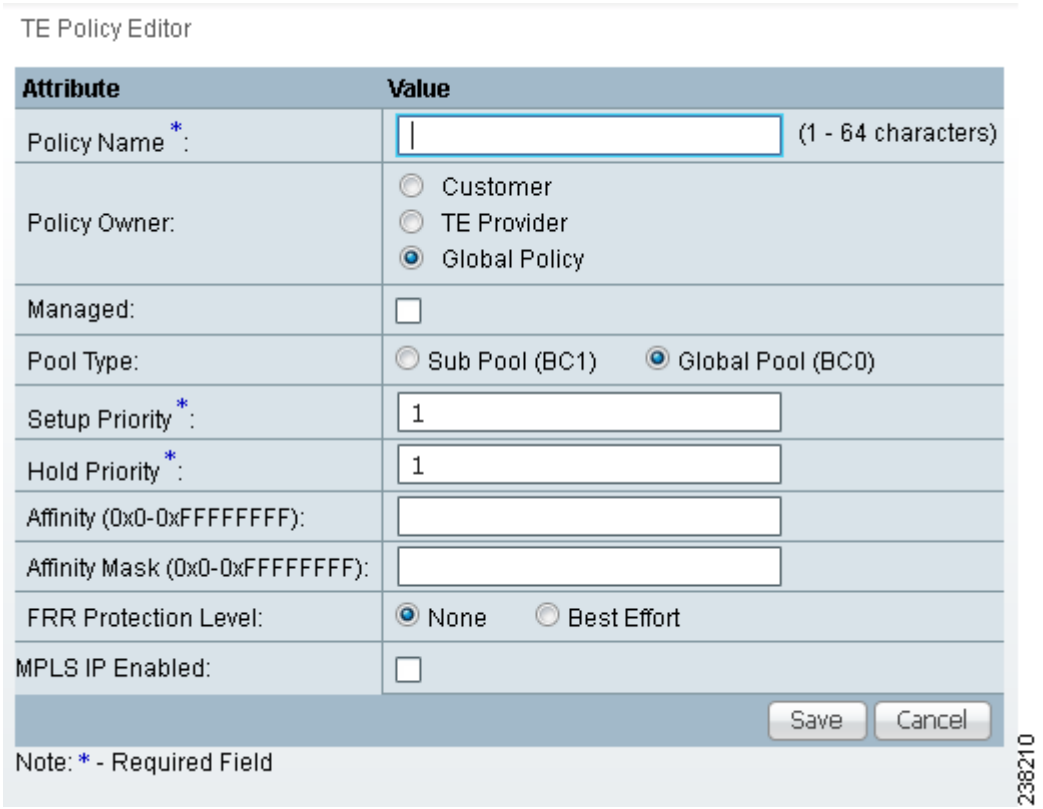
図 7-21　Policy Manager



ステップ 2　[Create] をクリックし、[TE Policy] を選択して新規 TE ポリシーを設定します。

図 7-22 の [TE Policy Editor] ウィンドウが表示されます。

図 7-22　TE Policy Editor



[TE Policy Editor] ウィンドウには、次のフィールドが含まれます。

- [Policy Name]：ユーザが選択する TE ポリシーの名前。

- [Owner]：TE ポリシーの所有者。
- [Managed]：このチェックボックスをオンにすると、ポリシーが管理対象トンネルにより使用されます。オンにした場合は、セットアップ プライオリティおよび保持プライオリティの両方にゼロが設定されて、編集不可になります。このチェックボックスがオフの場合は、セットアップおよび保持の優先度を 1 ～ 7 の値に設定できます。

  [Managed] チェックボックスをクリックすると、[FRR Protection Level]（Fast Re-Route）の 2 つの追加保護レベルに対応する TE Policy Editor のいくつかの特別なフィールドと新しいフィールド [Delay Constraint] が追加されます。
- [Pool Type]：このポリシーのトンネル帯域幅プール タイプ。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。
  - [Sub Pool (BC1)]：帯域幅はサブプールから予約されます。
  - [Global Pool (BC0)]：帯域幅はグローバル プールから予約されます。
- [Setup Priority]：優先する既存のトンネルを判別するために、トンネルの LSP をシグナリングするときに使用される優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。したがって、セットアップ プライオリティが 0 の LSP は、0 以外の保持プライオリティのすべての LSP より優先されます。
- [Hold Priority]：シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定するため、トンネルの LSP に関連付けられた優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。
- [Affinity]：トンネルを伝送するリンクで必要な属性値（ビット値は 0 または 1 のいずれか）。
- [Affinity Mask]：確認する属性値を決定します。マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。マスクのビットが 1 の場合、そのビットに対するリンクの属性値とトンネルに必要なアフィニティは一致する必要があります。
- [FRR Protection Level]：プライマリ トンネルで必要な高速再ルーティング保護のレベル。
  - [None]：バックアップ トンネルは必要ありません。
  - [Best Effort]：可能な場合に、バックアップ トンネルを使用します。
  - [Link & SRLG]：プライマリ トンネルは FRR 保護されたリンクまたは SRLG だけを通過する必要があります。
  - [Link, SRLG & Node]：プライマリ トンネルは、中間ノードと、FRR 保護されたリンクまたは SRLG だけを通過する必要があります。
- [MPLS IP Enabled]：**mpls ip** コマンド（有効な場合）でトンネルを設定します。

ポリシーの編集

ポリシーは、トンネルに関連付けられていない場合にのみ編集できます。

TE ポリシーを編集するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-22 の [Policies] ウィンドウが表示されます。

ステップ 2　必要なポリシーを選択し、[Edit] をクリックします。

[TE Policy Editor] ウィンドウが表示されます。ポリシー エディタについては、「ポリシーの作成」（P.7-73）で説明されています。作成プロセスと編集プロセスの唯一の違いは、ポリシーの編集時にポリシー名と所有者を編集できないことです。

ステップ 3　ポリシー属性に適切な変更を加え、[Save] をクリックします。

保存操作が正常に行われた場合は、新しい TE ポリシーが [Policies] ウィンドウに表示されます。成功しない場合は、発生したエラーのタイプと修正可能な場合の修正措置が [Status] ボックスに示されます。

ポリシーの削除

ポリシーは、トンネルに関連付けられていない場合にのみ削除できます。

TE ポリシーを削除するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-22 の [Policies] ウィンドウが表示されます。

ステップ 2　必要なポリシーを選択し、[Delete] 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 3　削除とマークされたポリシーのチェックボックスをオンにし、[OK] をクリックします。

[Policies] ウィンドウが更新され、選択されたポリシーが非表示になります。

TE タスク

Prime Provisioning には、現時点では、他のタスクと同様な方法で使用する TE 固有のタスクが 3 つあります。

- [TE Discovery (Full and Incremental)] : TE ネットワークからデータをリポジトリに入力します。不一致が調整または報告されます。
- [TE Functional Audit] : 特定の状態において、TE プライマリまたはバックアップ SR で機能監査を実行します。
- [TE Interface Performance] : インターフェイスまたはトンネルの帯域使用率を計算します。

この項では、TE 機能監査および TE インターフェイス パフォーマンス タスクの作成方法について説明します。TE 検出タスクの作成方法は、「TE ネットワーク検出」（P.7-11）に記載されています。

TE タスクの作成

TE タスクは、Task Manager で管理されます。ISC Task Manager にアクセスするには、[Operate] > [Task Manager] を選択します。

[Tasks] ウィンドウが表示されます。

[Tasks] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

このページには、実行されたすべての収集および展開タスクが表示されます。タスクは 1 回だけ行うようにスケジュールしたり、複数回行うようにスケジュールしたりできることに注意してください。スケジュールは、タスクを選択し、[Schedules] をクリックして表示できます。

TE 機能監査タスクの作成

SR の各トンネルに対して、TE 機能監査タスクはルータで現在使用されている LSP とリポジトリに格納された LSP を照合します。

- [tunnel down]：無視します（オンにしません）。
- [tunnel up]：ルータで使用されている LSP とリポジトリに格納された LSP を照合します。
  - これらの LSP が同じ場合、トンネルと SR は両方とも [Functional] に設定されます。
  - 異なる場合は、トンネルおよび SR の両方に [Broken] が設定されます。
- [tunnel missing from router]：SR はそのまま通過します。トンネルの状態は、Lost に設定されます。

このタスクでは、次のいずれかの状態でない TE プライマリまたはバックアップ SR に対してのみ機能監査を実行します。

- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

TE 機能監査タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Audit] > [TE Functional Audit] をクリックして [Create Task] ウィンドウを開きます。

[Create Task] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

ステップ 3　必要に応じて [Name] または [Description] フィールドの内容を変更し、[Next] をクリックします。

[Task Service Requests] ウィンドウが表示されます。

ステップ 4　[Add] をクリックしてタスク サービス要求を追加します。

[Select Service Request(s)] ウィンドウが表示されます。

ステップ 5　[Select] ボタンを使用して SR を選択します。

（注）　タイプ TE トンネルまたは TE 保護の SR のみが受け入れられます。

[Selected Service Request(s)] ウィンドウが閉じられ、選択されたタスクが [Task Service Requests] ウィンドウに表示されます。他の SR を追加するには、ステップ 4 とステップ 5 を繰り返します。

ステップ 6　[Task Service Requests] ウィンドウで、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 7　[Now] をクリックしてタスクをすぐに開始するか、[Create] をクリックしてタスク スケジュールを作成します。

[Now] を選択すると、行が [Task Schedules] ウィンドウに追加されます。[Create] を選択すると、[Task Schedule] ウィンドウが表示されます。

ステップ 8　[Task Schedule] ウィンドウで、タスクを実行するタイミングと頻度を指定します。

ステップ 9　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

（注）　デフォルト設定では、単一の TE 機能監査タスクをすぐに実行します（[Now]）。

ステップ 10　[Next] をクリックします。

[Task Schedule] ウィンドウの作成済みタスクのリストに新しいタスクが表示されます。スケジュールされたタスクの概要が表示されます。

ステップ 11　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

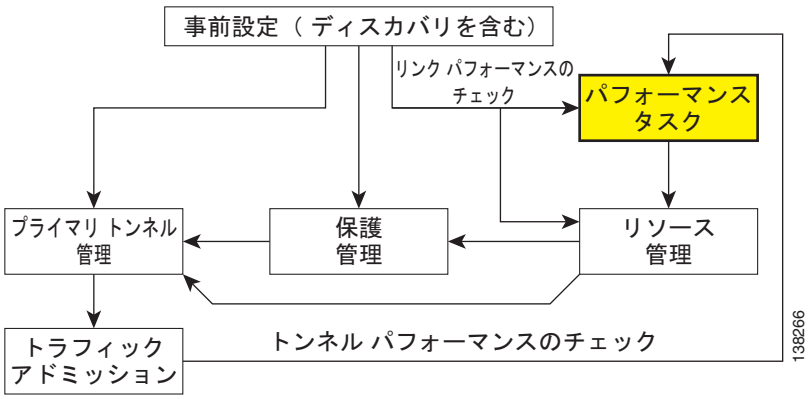
作成済みタスクのタスク ログを表示する場合は、「タスク ログの表示」（P.10-48）を参照してください。

TE インターフェイス パフォーマンス タスクの作成

このタスクでは、簡易ネットワーク管理プロトコル（SNMP）を使用してインターフェイスおよびトンネルの帯域使用率を計算します。

図 7-3 で強調表示されたボックスは、トラフィック アドミッションが Prime Provisioning のどこで行われるかを示しています。

図 7-23　Prime Provisioning プロセス図：TE インターフェイス パフォーマンス



使用率の計算は、測定するオブジェクトのデータの表現方法に依存します。インターフェイス使用率は、ネットワーク使用率に使用される主要な測定単位です。MIB-II 変数はカウンタとして格納されるため、2 つのポーリング サイクルを測定し、その差を計算する必要があります（つまり、方程式で使用される差分）。

次の 3 つの変数が必要です。

- タスク時間：タスクが実行される時間の長さ（秒単位）
- 頻度：データが収集される頻度（秒単位）
- 間隔：2 つのポーリング サイクル間の差（ミリ秒単位）

計算式で使用される変数の説明は次のとおりです。

- 差分（着信トラフィック）：SNMP 入力オブジェクトを収集する 2 つのポーリング サイクル間の差分であり、トラフィックの着信単位の数を表します。
- 差分（発信トラフィック）：SNMP 出力オブジェクトを収集する 2 つのポーリング間隔の差分で、トラフィックの発信単位の数を表します。
- 帯域幅：インターフェイスの速度。

次の式を使用して入力使用率と出力使用率を別々に測定する方式により、さらに高い精度を得られます。

$$\text{入力使用率} = \frac{\text{差分（着信トラフィック）} \times 8 \times 100}{\text{（差分の秒数）} \times \text{帯域幅}}$$

$$\text{出力使用率} = \frac{\text{差分（発信トラフィック）} \times 8 \times 100}{\text{（差分の秒数）} \times \text{帯域幅}}$$

TE インターフェイス パフォーマンス タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Create] > [TE Interface Performance] をクリックして、新しい TE インターフェイス パフォーマンス タスクに対して [Create Task] ウィンドウを開きます。

[Create Task] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

ステップ 3　必要に応じて名前と説明を変更し、[Next] をクリックします。

[Select TE Provider] 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て TE プロバイダーを選択します。

ステップ 5　[Next] をクリックします。

[TE Performance Collection] ウィンドウが表示されます。

ステップ 6　[Task Duration]、[Task Frequency]、および [Task Interval] の各フィールドに必要な値を入力します。

（注）　[Task Interval] フィールドの設定値が小さすぎる場合は、MIB を更新できず、TE パフォーマンス レポートでトラフィックが示されません。IOS ルータ上のトンネルまたはリンクの場合は、間隔に 1000 ms を設定することを推奨します。IOS XR ルータの場合は、間隔に 5000 ms を設定することを推奨します。お使いの特定の環境に合わせてこれらの値を調整する必要がある場合があることに注意してください。

ステップ 7　[Add] ボタンを使用して、インターフェイス パフォーマンス タスクを実行するトンネルまたはリンクを選択します。

- [TE Tunnel]：TE トンネルを追加します。[Select Tunnel(s)] ウィンドウが表示されます。
- [TE Link]：TE リンクを追加します。[Select Link(s)] ウィンドウが表示されます。

ステップ 8　1 つまたは複数のトンネルおよびリンクを選択し、[Next] をクリックします。

選択されたトンネルおよびリンクは、[TE Performance Collection] ウィンドウの [Targets] リストに追加されます。[Task Schedules] ウィンドウが表示されます。

ステップ 9　[Now] または [Create] をクリックしてタスク スケジュールを作成します。

[Create] を選択してスケジュールをカスタマイズする場合は、[Task Schedule] ウィンドウが表示されます（[Now] の場合、このステップはスキップされます）。

（注）　デフォルト設定では、単一の TE インターフェイス パフォーマンス タスクをすぐに実行します（[Now]）。

ステップ 10　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

ステップ 11　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 12　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 13　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

TE インターフェイス パフォーマンス タスクに対して生成された TE パフォーマンス レポートを表示するには、「TE パフォーマンス レポート」（P.10-49）を参照してください。

作成済みタスクのタスク ログを表示する場合は、「タスク ログの表示」（P.10-48）を参照してください。

SR 履歴およびコンフィグレット

個々のサービス要求に関連する履歴とコンフィグレットは、[Service Requests] ウィンドウでサービス要求を選択し、[Details] ボタンをクリックして表示できます。

サービス要求の履歴は、実質的に状態の変更レポートです。SR に関連付けられた要素が遷移したさまざまな状態がリストされ、これらの状態の遷移に関する詳細が報告されます。

サービス要求に関連付けられたデバイスのコンフィグレットは、スクロール可能な単純なテキスト形式で保存されます。

これらの機能についておよびサービス要求を管理する方法の詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

ロック メカニズムの管理

データベース更新を伴うタスクの実行は、リソースに影響し、したがってトンネル計算の結果に影響することがあるため、更新の前にタスクによってシステムがロックし、更新の完了時に解放します。何らかの理由でロックがリリースされない場合は、ロックを必要とする他の更新がブロックされます。

ロック機能は、相互に矛盾する計画アクティビティを同時にデータベースにコミットさせないことを目的としています。つまり、各ユーザがリポジトリの同じスナップショットを取得し、計算を実行して結果をコミットしようとした場合に、ロック メカニズムは、コミットを同期するため、および他のコミットが原因で無効になるコミットをなくすために有用です。

システムが長時間ロックされる場合、管理者は、計画タスクを長時間実行しているユーザの存在を確認し、システムをロックしたプロセスをメモして報告する必要があります。管理者は、システムを使用しているユーザがいないことを確認し、ロック マネージャを使用してロックを解除できます。

Prime Provisioning には、2 種類のロックがあります。

- TE プロバイダー ロック：管理対象トンネル、バックアップ トンネル、リソース SR、および TE 検出をロックします。
- TE ルータ ロック：管理対象外トンネルをロックします。

各システム ロックは、TE プロバイダーにリンクされます。次に、各システム ロックをロック解除する手順を示します。

TE プロバイダー ロックのロック解除

TE プロバイダーをロック解除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Providers] を選択します。

[TE Providers] ウィンドウが表示されます。

ステップ 2　対応するチェックボックスをオンにして、ロックされている TE プロバイダーを選択します。

ステップ 3　[Manage Lock] をクリックします。

[System Lock Management] ウィンドウが表示されます。

このウィンドウのテキスト フィールドは読み取り専用です。

ステップ 4　ロックを解除するために [Unlock] ボタンをクリックします。

[System Lock Management] ウィンドウが閉じられ、[TE Providers] ウィンドウの [System Lock Status] フィールドが適宜更新されます。

TE ルータ ロックのロック解除

TE ルータ ロックをロック解除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Nodes] を選択します。

[TE Nodes List] ウィンドウが表示されます。

ステップ 2　対応するチェックボックスをオンにして、ロックされている TE ノードを選択します。

ステップ 3　[Manage Lock] をクリックします。

[System Lock Management] ウィンドウが表示されます。このウィンドウのテキスト フィールドは読み取り専用です。

ステップ 4　ロックを解除するために [Unlock] ボタンをクリックします。

[System Lock Management] ウィンドウが閉じられ、[TE Nodes List] ウィンドウの [System Lock Status] フィールドが適宜更新されます。

操作エラーのロック

TEM では、保存操作および導入操作の間、TE プロバイダーまたは TE ルータ オブジェクトをそれぞれロックして、データベースの一貫性を保ちます。

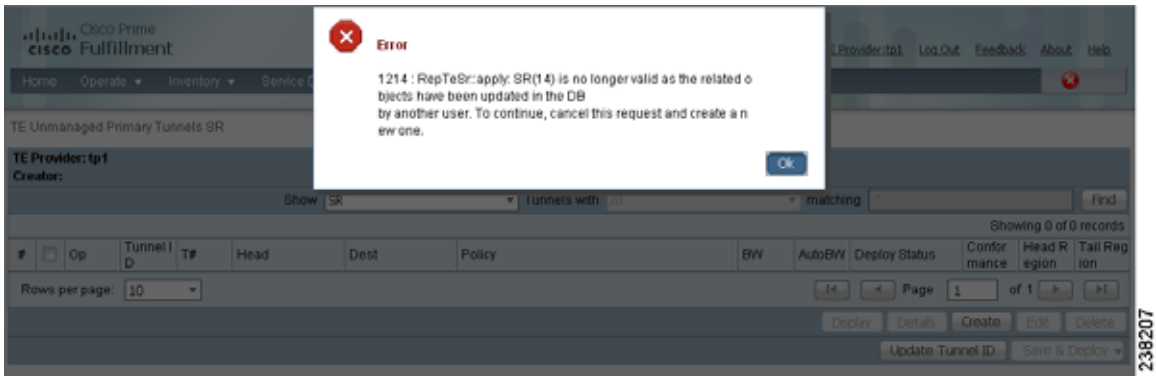
この項では、次のエラーについて説明します。

- 「ロックされたオブジェクトの変更」（P.7-82）
- 「ロックが解放されたオブジェクトの変更」（P.7-83）
- 「関連 TE オブジェクトのあるリンクの削除」（P.7-83）
- 「関連 TE オブジェクトのないリンクの削除」（P.7-84）

ロックされたオブジェクトの変更

ロックされたオブジェクトを変更しようとした場合は、別のユーザによって変更中であるため、オブジェクトを変更できないと通知されます。図 7-24 のエラー メッセージが表示されます。

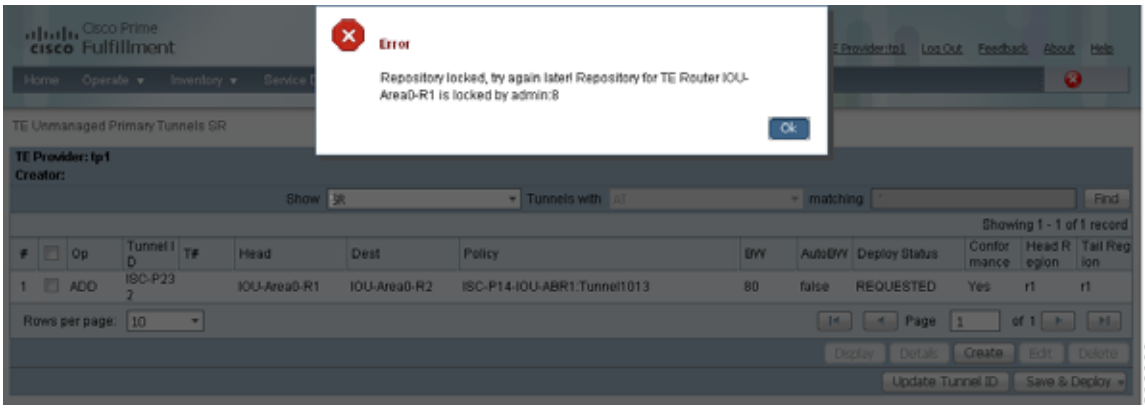
図 7-24　ロックされたオブジェクトの変更



ロックが解放されたオブジェクトの変更

ロックの解放後にオブジェクトを変更しようとした場合、Prime Provisioning では、現在作業中のオブジェクトのバージョンが最新であるかどうかをチェックします。バージョンが最新でない場合は、データが最新でないため、オブジェクトの新しいバージョンで再び作業を始めるよう指示されます。図 7-25 のエラー メッセージが表示されます。

図 7-25　ロックが解放されたオブジェクトの変更

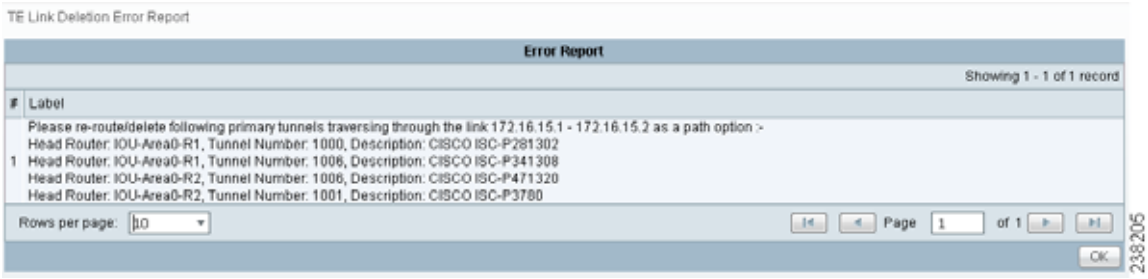


関連 TE オブジェクトのあるリンクの削除

明示的パスと関連付けられているリンクや、トンネルが通過しているリンクは削除できません。

1 つまたは複数のオブジェクトが関連付けられたリンクを削除しようとすると、図 7-26 のエラー メッセージが表示されます。

図 7-26　関連 TE オブジェクトのあるリンクの削除

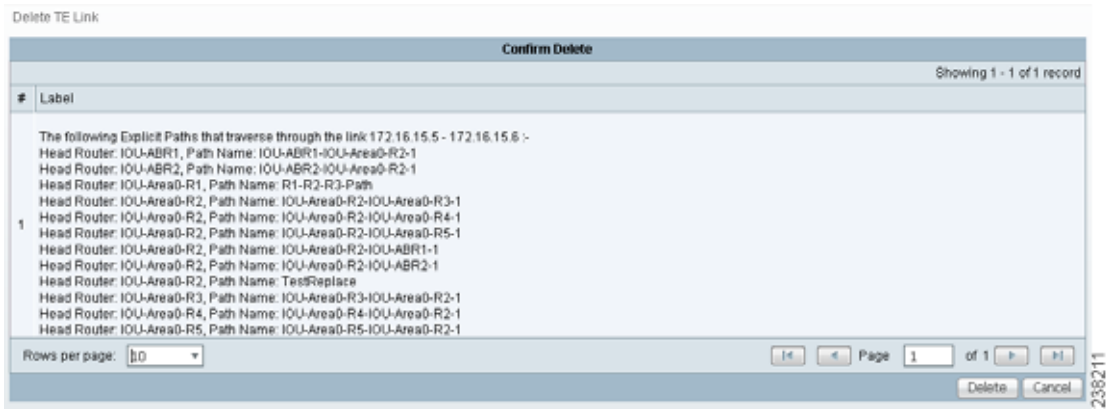


関連 TE オブジェクトのないリンクの削除

トンネルが通過していないリンクは、明示的パスと関連付けられていても削除できます。

このようなリンクを削除しようとしたときに、図 7-27 示すレポートのタイプが表示されます。

図 7-27　関連 TE オブジェクトのないリンクの削除



TE トポロジ

TE トポロジ ツールは、Cisco Prime Provisioning Web クライアントを通じてネットワーク設定のグラフィカル ビューを提供します。デバイス、リンク、およびトンネルなどさまざまなネットワーク要素がグラフィカルに表示されます。Prime Provisioning では識別できないが、TE 検出ツールでネットワークの一部として検出されたデバイスも表示されます。

TE トポロジ ツールには、[Traffic Engineering] メニューからアクセスします。

TE トポロジ ツールは、リポジトリに含まれるデータに基づいて TE ネットワークを視覚化するために使用されます。この目的のために、グラフ レイアウトに対するアルゴリズムの適用、マップのインポートなど、表示を操作するさまざまな方法が用意されています。

このツールは、ブラウザ内の Java アプレットを介して TE トポロジを表示する TE トポロジ インターフェイス アプレットからアクセスします。

ここでは、トポロジ ツールを使用する方法について説明します。

内容は次のとおりです。

TE トポロジ インターフェイス アプレットの使用

TE トポロジ インターフェイス アプレット（トポロジ アプレット）は、ネットワークおよびネットワークに存在しているトンネルを視覚化する手段を備えています。Web ベースの GUI は、ネットワーク情報を視覚化する主要な手段です。トポロジ アプレットでは単に Web ベースの GUI を拡張してさまざまなプレゼンテーション形式を実現します。

トポロジ アプレットを介して次の機能が提供されます。

- TE トポロジのレンダリング
- ネットワーク要素の強調表示
- トンネル オーバーレイ（管理対象外、プライマリ、およびバックアップ）
- トポロジ レイアウトのパーシステンス
- Web ページ コンテンツとの統合

トポロジ アプレットにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Topology] を選択します。

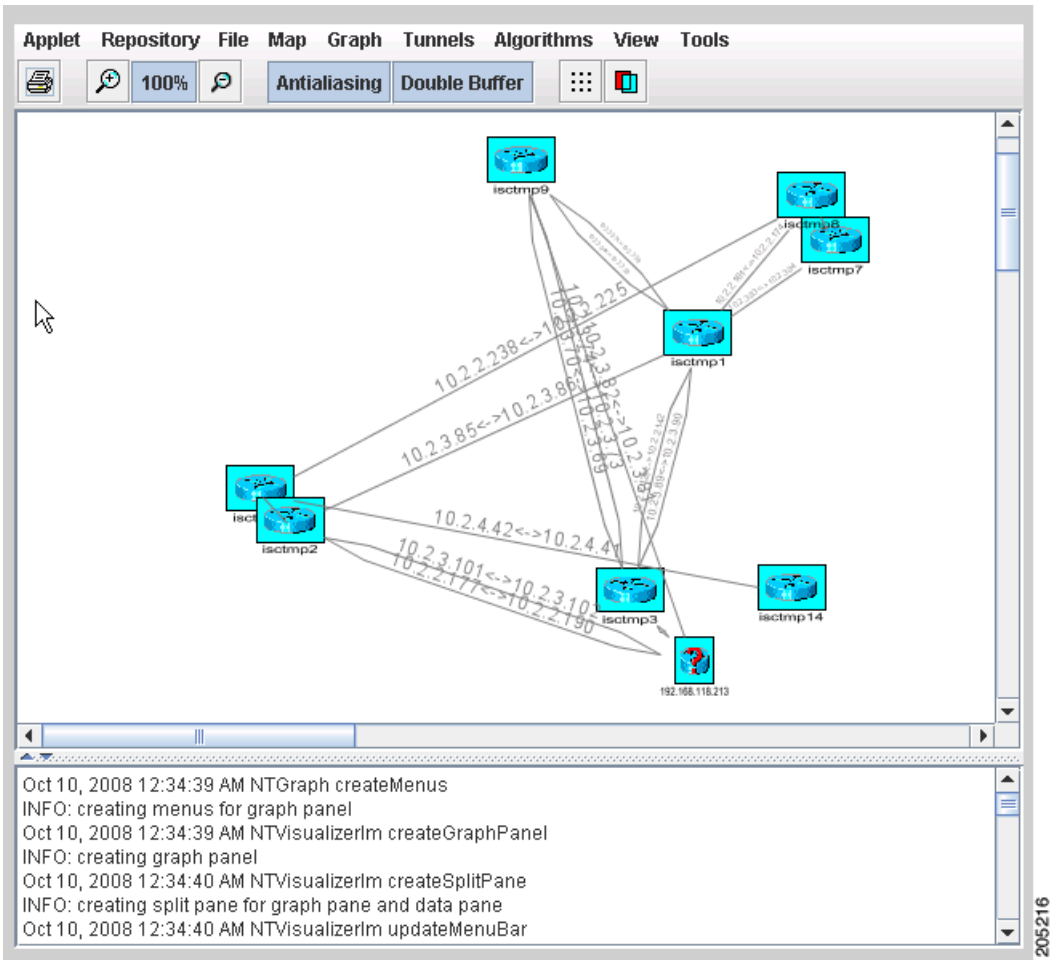
ステップ 2　[TEM Topology Interface Applet] をクリックします。

トポロジ アプレットのセキュリティ証明書をまだ受け入れていないために、セキュリティ警告ウィンドウが表示されることがあります。

ステップ 3　[Yes] または [Always] をクリックして、セキュリティ証明書の信頼性を受け入れます。

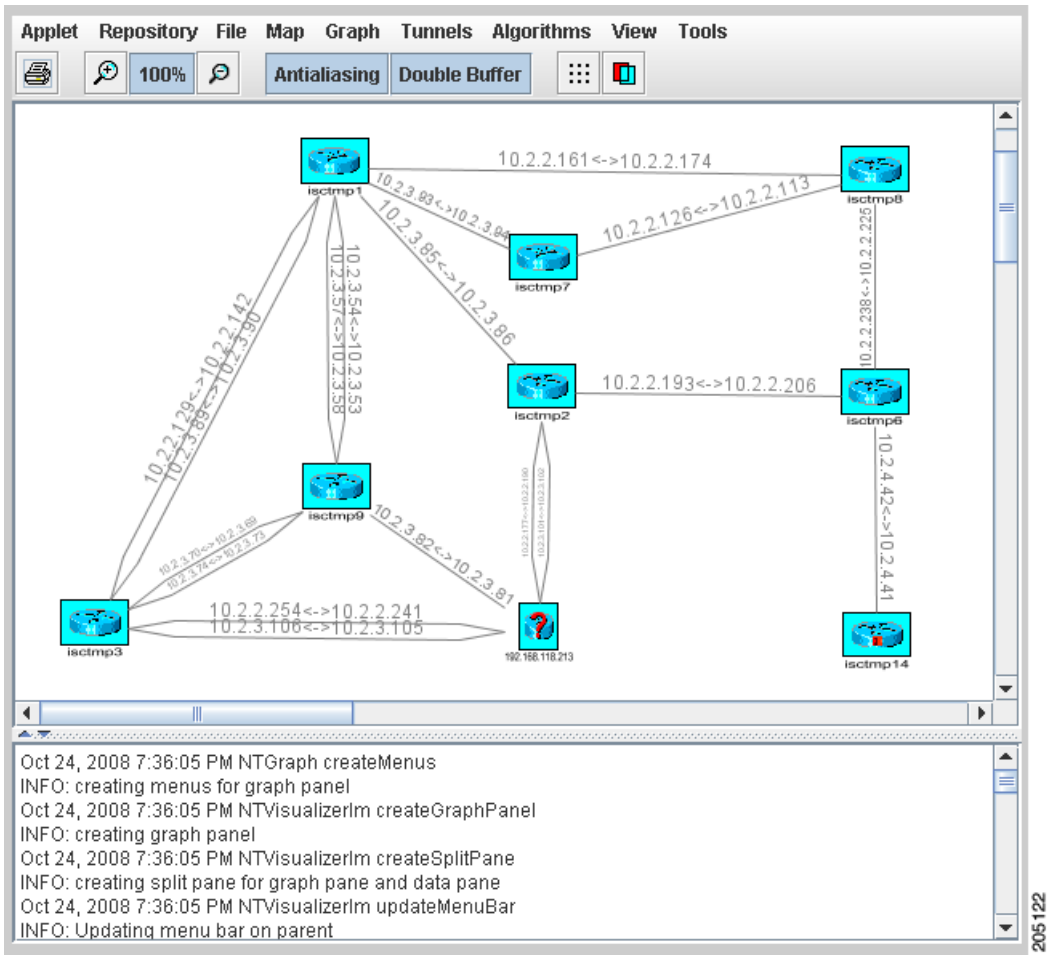
図 7-28 の [Topology Display] アプレット ウィンドウが表示されます。

図 7-28　順序付けられていない状態のトポロジ表示アプレット



好みに合わせてノードを配置し終えると、トポロジ表示は図 7-29 のようになります。

図 7-29　トポロジ表示アプレットとユーザが編成したトポロジ



レイアウトの表示および保存

[Repository] メニューの 2 つの操作 [Layout Graph] および [Save Graph Layout] を使用して、ネットワーク グラフの現在のレイアウトを表示または保存します。

グラフ レイアウトを生成する前に、各ネットワーク デバイスの座標を設定する必要があります。そうでない場合、グラフはランダムにレイアウトされます。

- [Layout Graph] : グラフはリポジトリからレイアウトされます。すでにグラフ レイアウトが存在する場合、[Clear Graph Layout] 確認ボックスで [Yes] をクリックすると、そのレイアウトはクリアされます。レイアウトが以前に保存されていない場合は、リポジトリの内容のランダムなレイアウトが取得されます。以前にレイアウトを保存した場合は、保存されたレイアウトが再描画されます。
- [Save Graph Layout] : 現在のグラフ レイアウトを保存します。そうすることで、[Layout Graph] またはトポロジ アプレットを閉じると常にグラフ レイアウトがクリアされ、アプレットの再起動時に同じレイアウトが作成されるように保証されます。マップが使用された場合、そのマップも再描画されます。

マップの使用

各ビューには、マップを 1 つ関連付けることができます。現在、トポロジ ビューアでは、Environmental Systems Research Institute, Inc.（ESRI）のシェープ形式のマップのみサポートされています。以降の章では、マップをロードし、マップ レイヤと各マップに関連付けられているデータを選択的に表示する方法について説明します。

マップの機能は、[Topology] ウィンドウの [Map] メニューからアクセスします。

[Map] メニューにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [TE Topology] を選択します。

ステップ 2　[TM Topology Interface Applet] を起動します。

ネットワークのリンクとノード データがリポジトリにすでに存在する場合、進行状況レポートは、対応するデータがロードされるときに、さまざまなネットワーク要素を示します。

ステップ 3　[Map] メニューを選択します。

メニューが表示されます。

[Map] メニューでは、次に説明するように、マップをロードまたはクリア（削除）できます。

マップのロード

表示されたデバイスの物理的な位置を表示したバックグラウンド マップの設定が必要になることがあります。マップをロードするには、次のステップを実行します。

ステップ 1　メニュー バーで、[Map] > [Load] を選択します。

Web マップ サーバが動作している場合は、[Map Chooser] ウィンドウが表示されます。

ステップ 2　[Map Chooser] ウィンドウで必要な選択を行います。

ウィンドウの右側部分には、小さいコントロール パネルがあり、マップを表示する投影法を選択できます。マップの投影では、平面に球体がマップされます。一般的な投影法には、メルカトル、ランベルト、およびステレオ投影があります。

投影法の詳細については、次の場所にある、Eric Weisstein による「World of Mathematics」の「Map Projections」の項を参照してください。

http://mathworld.wolfram.com/topics/MapProjections.html

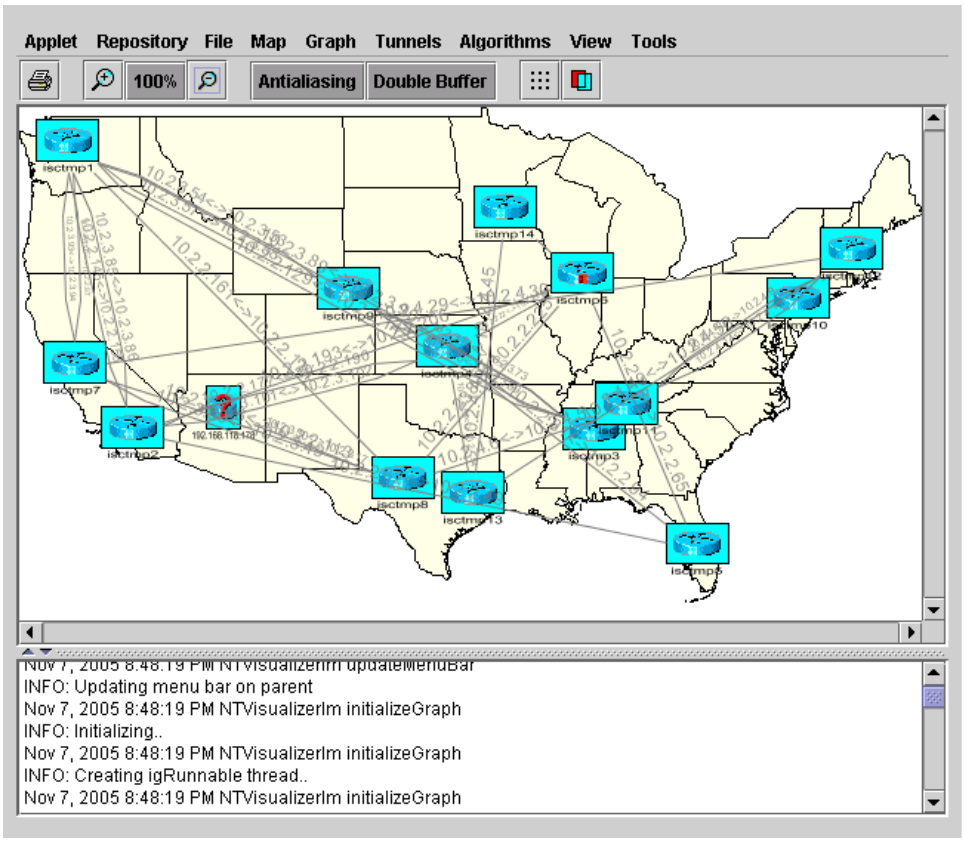
必要に応じて、[Longitude Range] フィールドと [Latitude Range] フィールドの設定を変更します。

ステップ 3　マップ ファイルを選択し、[Open] をクリックして、マップをロードします。

マップ ファイルを選択し、[Open] ボタンをクリックすると、ファイルのロードが開始されます。マップは複数コンポーネントで構成されている場合があるため、ロードされたマップ ファイルの部分を通知する進捗ダイアログが表示されます。

図 7-30 のようなマップが表示されます。

図 7-30　　ロードされたマップ



ステップ 4　トポロジ ビューの表示内容を操作するには、[Topology Display] ウィンドウのメニューで、各種機能を使用します。一部については、以降で説明します。

新規マップの追加

トポロジ ツールで使用できるように、マップの選択肢に独自のマップを追加することが必要になる場合があります。これは、マップ ファイルを **$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** ディレクトリまたは、Prime Provisioning インストール内のサブディレクトリに配置することによって行います。この例をわかりやすく説明するために、クイーンズランド州の州都ブリスベンの郊外にあるトゥーウォンのマップを追加するとします。最初のステップとして、マップ ベンダーからマップを入手します。すべてのマップは ESRI シェープ ファイル形式でなければなりません（『**ESRI Shapefile Technical Description**』を参照）。また、各シェープ ファイルにはデータ ファイルを付属させることもできます。データ ファイルには、オブジェクト、およびシェープ ファイル内に含まれている対応するシェープに関する情報が含まれます。ベンダーが次の 4 つのファイルを提供しているとします。

- toowong_city.shp
- toowong_city.dbf
- toowong_street.shp
- toowong_street.dbf

マップのレイヤに関する情報を TE トポロジ ツールに伝える .map ファイルを作成する必要があります。この例では、City と Street という 2 つのレイヤがあります。マップ ファイル（たとえば、Toowong.map）は、次のような内容になります。

```
toowong_city
toowong_street
```

このファイルには、トゥーウォンのマップを構成するレイヤがすべてリストされます。最初のファイルがバックグラウンド レイヤになり、他のレイヤは先行するレイヤの上に配置されるため、順序が重要です。

シェープ ファイルとデータ ファイルを取得し、マップ ファイルを書き込んでから、5 つのファイルすべてを **$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** ディレクトリに配置します。マップ ファイルはすべて、このフォルダに配置する必要があります。これが終了すると、自動的にトポロジ ビューアからこのマップにアクセスできるようになります。

マップのクリア

アクティブなマップをクリアするには、[Map] > [Clear] を選択します。

この機能を使用してアクティブ マップをクリア（削除）することにより、ノードおよびリンクだけが対応するネットワークに残る状態にします。

強調表示および属性の使用

[Graph] メニューは、グラフを管理し、操作するさまざまなツールへのアクセスを提供します。

JavaServer Pages を使用してノード、リンク、およびトンネルのリストを参照します。JSP ページからウィンドウの下部にある [display] ボタンを選択して要素を強調表示します。

[Graph] メニューのツールは、トポロジの表示を変更します。

これらについては、次の項を参照してください。

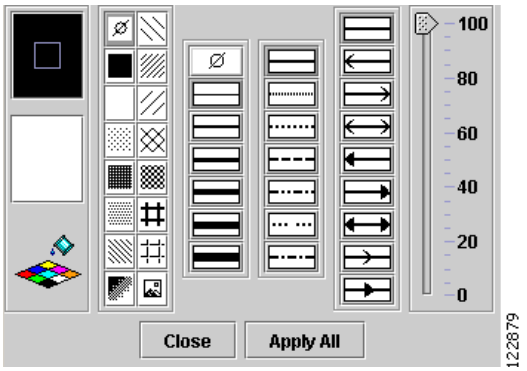
強調表示の解除

[Clear Highlighting] は、サブメニューにリストされている特定の要素で、強調表示を解除します。

属性の追加 / 変更

[Graph] メニューから [Attributes] を選択すると、図 7-31 の [Graphic Attributes] ウィンドウが表示されます。

図 7-31　Graphic Attributes



属性の追加/変更ツールは、次のように使用します。

ステップ 1　トポロジ表示にあるグラフ要素（ノードまたはリンク）を選択します。

複数の要素を選択するには、Ctrl/Shift を使用します。

ステップ 2　[Graph] > [Attributes] を選択し、[Graphic Attributes] ウィンドウを開きます。

ステップ 3　目的の属性を変更し、[Apply All] をクリックします。

（注）　選択したリンク（ステップ 1）だけが影響を受けます。

現在のグラフ レイアウトのクリア

現在のビューからトポロジ グラフを削除するには、[Graph] メニューの [Clear] 機能を使用します。

[Repository] メニューの [Layout Graph] でもグラフは削除されますが、[Layout Graph] ではグラフのクリアに加えて、リポジトリに最後に保存されたグラフの再作成も行われます。

[AntiAlias]、[BackingStore]、[DoubleBuffer] の使用

[Graph] メニューの [AntiAlias] は、パフォーマンスを犠牲にして、より滑らかなラインと気持ちのよい外観を生み出すために使用します。

[BackingStore] では、バックグラウンドになるとグラフィック コンテンツを自動的に保存し、フォアグラウンドに戻るとそれを再生成することができます。これによって、不必要な更新を回避できます。

[DoubleBuffer] は、グラフに要素をドラッグするためのダブルバッファリングを有効にします。

アルゴリズムの使用

[Algorithms] メニューでは、さまざまなアルゴリズムを使用して、グラフィック レイアウトを拡張する、およびそれ以外の場合は変更することができます。

（注）　アルゴリズムは、ノードがリンクと相互接続されている場合に限り機能します。

[Spring] は、重みに基づいてグラフィック レイアウトを最適化するグラフ レイアウト アルゴリズムです。

[Randomize] は現在のトポロジ レイアウトのノードをランダムに再配置します。

重複したリンクがある場合は、[Optimize Links] を選択してレイアウトを最適化できます。

スプリング設定は、ユーザの好みに従ってトポロジ表示の外観を拡張する場合に使用します。[Spring Settings] を選択すると、[Spring Settings] ウィンドウが表示されます。

サンプル コンフィグレット

この項に含まれ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

この項のすべてのサンプルでは、MPLS-TE コアの存在を想定しています。

（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。

ここでは、Cisco Prime Provisioning でのトラフィック エンジニアリング サービス プロビジョニングのコンフィグレットの例について説明します。

内容は次のとおりです。

プライマリ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE プライマリ トンネル
- 機能：プライマリ トンネルを導入するための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** ip explicit-path name isctmp2-isctmp8-1 enable next-address 10.2.2.145 next-address 10.2.2.174 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。 この明示的パスは、前述したプライマリ トンネルにより使用されます。
! **Primary tunnel:** interface Tunnel1000 description CISCO ISC-P24 ip unnumbered Loopback0 no ip directed-broadcast tag-switching ip tunnel destination 192.168.118.183 tunnel mode mpls traffic-eng tunnel mpls traffic-eng priority 0 0 tunnel mpls traffic-eng bandwidth 10 tunnel mpls traffic-eng affinity 0x0 mask 0x0 tunnel mpls traffic-eng path-option 1 explicit name isctmp2-isctmp8-1 tunnel mpls traffic-eng path-option 2 dynamic tunnel mpls traffic-eng record-route !	次の属性を使用して TE プライマリ トンネルを作成します。 - タグ スイッチング：このコマンドが生成されているのは、ポリシーで「mpls ip」フラグがイネーブルになっているためです。これにより、MPLS VPN トラフィックに対して TE トンネルを使用できるようになります。 - 宛先 192.168.118.183 - TE カプセル化 - セットアップ プライオリティと保持プライオリティはともに 0 - 帯域幅のグローバル プールは 10 kbps - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション - 動的な 2 番目のパス オプション

帯域幅保護バックアップ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：このトンネルは、リンクまたはノードのいずれかの障害発生時にプライマリ トンネル トラフィックを保護します。
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! Explicit path: ip explicit-path name isctmp5-isctmp4-1 enable next-address 10.2.2.145 next-address 10.2.2.174 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。 この明示的パスは、前述したバックアップ トンネルにより使用されます。
! Backup tunnel: interface Tunnel1001 description CISCO ISC-B30 ip unnumbered Loopback0 tunnel destination 192.168.118.213 tunnel mode mpls traffic-eng tunnel mpls traffic-eng backup-bw sub-pool 30000 tunnel mpls traffic-eng priority 0 0 tunnel mpls traffic-eng affinity 0x0 mask 0x0 tunnel mpls traffic-eng path-option 1 explicit name isctmp5-isctmp4-1 tunnel mpls traffic-eng record-route !	次の属性を使用して TE バックアップ トンネルを作成します。 - 宛先 192.168.118.213 - TE カプセル化 - サブプールの帯域幅を 30000 kbps 保護 - セットアップ プライオリティと保持プライオリティはともに 0 - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション
interface POS0/1 mpls traffic-eng backup-path tunnel 1001 !	バックアップ トンネル 1001 でインターフェイス POS0/1 を保護

接続保護バックアップ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：接続保護バックアップ トンネルおよび関連する除外アドレス パスを導入するための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** ip explicit-path name L47-excl enable exclude-address 192.168.1.18 ! !	除外アドレス（パスで回避する必要がある IP アドレスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。

! **Backup tunnel:**
interface Tunnel1000
  description CISCO ISC-B1
  ip unnumbered Loopback0
  tunnel mode mpls traffic-eng
  tunnel destination 10.52.96.38
  tunnel mpls traffic-eng priority 0 0
  no tunnel mpls traffic-eng bandwidth
  tunnel mpls traffic-eng path-option 1
explicit name L47-excl
  tunnel mpls traffic-eng affinity 0x0 mask
0x0
  tunnel mpls traffic-eng backup-bw
sub-pool unlimited
  tunnel mpls traffic-eng record-route
!
interface ATM4/0.1 point-to-point
  mpls traffic-eng backup-path Tunnel1000
	次の属性を使用して TE バックアップ トンネルを作成します。
	- 宛先 10.52.96.38
	- TE カプセル化
	- セットアップ プライオリティと保持プライオリティはともに 0
	- バックアップ トンネルによる帯域幅の予約なし
	- 明示的な最初のパス オプション
	- トンネル アフィニティは 0x0
	- サブプール保護のためのバックアップ帯域幅は無制限
	
	ATM インターフェイスにバックアップ パスを設定します。

CBTS を使用した TE トラフィック アドミッション コンフィグレット（IOS）

設定

- サービス：TE トラフィック アドミッション
- 機能：Class-Based Tunnel Selection（CBTS; クラスベース トンネル選択）を使用してトラフィックをアドミッションするための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **TE Traffic Admission using CBTS:** interface Tunnel1000 tunnel mpls traffic-eng exp 1 2 3 ! ! **Static route:** ip route 192.168.118.189 255.255.255.255 Tunnel1000	EXP ビット 1、2 または 3 のトラフィックを選択した場合のクラスベース トンネル選択 スタティック ルートを作成し、192.168.118.189 宛ての全トラフィックを上記で設定したトンネル 1000 に向けて許可します。

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS）」（P.7-93）のような既存のプライマリ トンネルに展開されます。

TE トラフィック アドミッション コンフィグレット（IOS）

設定

- サービス：TE トラフィック アドミッション
- 機能：TE トラフィック アドミッションの MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.2(33)SRA を稼働する OSR-7609

コンフィグレット

IOS デバイスの設定	コメント

! **TE Traffic Admission:**
interface Tunnel1000
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng autoroute metric relative 0
	相対メトリック 0（デフォルト）を使用した自動ルート通知

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS）」（P.7-93）のような既存のプライマリ トンネルに展開されます。

プライマリ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE プライマリ トンネル
- 機能：プライマリ トンネルを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** explicit-path name isctmp12-isctmp7-1 index 1 next-address ipv4 unicast 10.163.25.109 index 2 next-address ipv4 unicast 10.163.25.106 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。この明示的パスは、前述したプライマリ トンネルにより使用されます。
! **Primary tunnel:** interface tunnel-te133 description CISCO ISC-P2 ipv4 unnumbered Loopback0 priority 0 0 signalled-bandwidth 13 destination 192.168.118.214 fast-reroute path-option 1 explicit name isctmp12-isctmp7-1 path-option 2 dynamic record-route !	次の属性を使用して TE プライマリ トンネルを作成します。 - 宛先 192.168.118.214 - TE カプセル化 - セットアップ プライオリティは 0 - 保持プライオリティは 0 - グローバル プールから 13 kbps 予約 - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション - 動的な 2 番目のパス オプション - トンネルで FRR をイネーブル化
mpls ldp interface tunnel-te 133 !	トンネル インターフェイスで LDP（ラベル配布プロトコル）をイネーブルにします。このコマンドが生成されているのは、ポリシーで「mpls ip」フラグがイネーブルになっているためです。これにより、MPLS VPN トラフィックに対して TE トンネルを使用できるようになります。

帯域幅保護バックアップ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：バックアップ トンネルを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント

! **Explicit path:**
explicit-path name isctmp8-isctmp9-1
 index 1 next-address ipv4 unicast
10.163.25.109
 index 2 next-address ipv4 unicast
10.163.25.106
!
! **Backup tunnel:**
interface tunnel-te1009
 description CISCO ISC-B1411
 ipv4 unnumbered Loopback0
 priority 0 0
 backup-bw 9600000
 destination 10.163.24.131
 path-option 1 explicit name
isctmp8-isctmp9-1
 record-route
 affinity 0 mask 0
!
mpls traffic-eng
  interface POS0/1/0/1
  backup-path tunnel-te 1009
	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。
	
	次の属性を使用して TE バックアップ トンネルを作成します。
	- 宛先 10.163.24.131
	- TE カプセル化
	- 任意のプールの帯域幅を 9600000 kbps 保護
	- セットアップ プライオリティと保持プライオリティは 0
	- トンネル アフィニティは 0x0
	- 明示的な最初のパス オプション

接続保護バックアップ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：接続保護バックアップ トンネルおよび関連する除外アドレス パスを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント

! **Explicit path:**
explicit-path name L96-excl
  index 1 exclude-address ipv4 unicast 192.168.1.42
!
!
! **Backup tunnel:**
interface tunnel-te1000
  description CISCO ISC-B2
  ipv4 unnumbered Loopback0
  destination 10.52.96.37
  priority 0 0
  no signalled-bandwidth 0
  path-option 1 explicit name L96-excl
  affinity 0 mask 0
  backup-bw sub-pool unlimited
  record-route
!
mpls traffic-eng
  interface POS0/1/0/2
  backup-path tunnel-te 1000
!
	除外アドレス（パスで回避する必要がある IP アドレスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。
	次の属性を使用して TE バックアップ トンネルを作成します。
	- 宛先 10.52.96.37
	- TE カプセル化
	- セットアップ プライオリティは 0
	- 保持プライオリティは 0
	- 明示的な最初のパス オプション
	- トンネル アフィニティは 0x0
	- 無制限のサブプールがバックアップ帯域幅として機能
	
	トンネル 1000 でインターフェイス POS0/1/0/2 を保護

PBTS を使用した TE トラフィック アドミッション コンフィグレット（IOS XR）

設定

- サービス：TE トラフィック アドミッション
- 機能：ポリシーベース トンネル選択（PBTS）を使用してトラフィックをアドミッションするための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント

! **TE Traffic Admission using PBTS:**
interface tunnel-te133
  autoroute announce
  autoroute metric absolute 100
  policy-class 2
!
	絶対メトリック 100 を使用した自動ルート通知

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS XR）」（P.7-98）のような既存のプライマリ トンネルに展開されます。

TE トラフィック アドミッション コンフィグレット（IOS XR）

設定

- サービス：TE トラフィック アドミッション
- 機能：TE トラフィック アドミッションの MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS XR デバイス設定	コメント

`! TE Traffic Admission Using Static Route:`
`router static`
`  address-family ipv4 unicast`
`  1.2.3.4/32 tunnel-te 1000 123`
`  !`
`!`
	スタティック ルートを使用してトンネル 1000 に TE トラフィック アドミッションを設定

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS XR）」（P.7-98）のような既存のプライマリ トンネルに展開されます。

警告および違反

このセクションは、Prime Provisioning で計画ツール（計算エンジン）を使用する場合に、呼び出されることがある違反と警告を示します。

警告と違反は、計画ツールに関連付けられます（「トラフィック エンジニアリング管理の概念」（P.7-115）の計画ツールの項を参照）。これらは、次の状況で発生します。

- プライマリ管理対象トンネルの監査、配置、修復、または調整の試行時。
- 選択したネットワーク要素（リンク、ルータ、または SRLG）の保護の試行時。ここでは、これらが、失敗した保護の原因の判断に役立ちます（「保護計画」（P.7-60）を参照）。

  特定の要素を保護できるかどうかを判断する場合にオフライン バックアップのルート生成が呼び出されると、バックアップ ルート ジェネレータは、各要素と、一連の要素を保護するトンネルまたは要素を保護できなかった理由の判断に役立つ一連の違反および警告のいずれかに応答します。

（注） 以下、用語 DirectedLink はルータ インターフェイスを示します。

ここでは、次の内容について説明します。

警告

このクラスの特徴は、すべてのレポートが警告であることです。警告は保護パスの計算の妨げにならないという点で、違反に比べて深刻でないと見なされます。

保護計算の警告

WarningFixVetoed

この要素の修正により、ネイバー要素が保護されなくなりました。この修正は拒否され、変更は提示されません。

WarningRouterNotConformant

この要素またはいずれかの隣接ルータはプロトコルに適合していません。したがって、保護できません。

フィールド：

- [Report Type]：レポート タイプの名前。
- [Description]：違反によって通知された問題の説明。
- [Non-conformant router]：トラフィック エンジニアリングをサポートしないルータ。

WarningTunnelBandwidthQuotaTooSmall

この要素を保護するバックアップ トンネルの帯域幅が、許容される最小の帯域幅キャパシティを下回っています。

フィールド：

- [Minimum allowed bandwidth quota]：当該の要素の保護に許可された最小帯域幅。
- [Actual tunnel bandwidth quota]：バックアップ トンネルの実際の帯域幅。

WarningTunnelNumberTooLarge

この要素を通過するフローに対するバックアップ トンネルが多すぎます。

フィールド：

- [Maximum tunnel number allowed]：特定のネットワーク要素に対して許可されるトンネルの最大数。
- [Actual Tunnel Count]：このネットワーク要素に課されるトンネルの実際の数。
- [Flow]：
  - [Maximum Bandwidth]：保護する必要のあるトラフィック フローの最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

WarningZeroProtectedFlow

この要素を通過するフローはバックアップ トンネルによって保護されていますが、最大フローが 0 です。

フィールド：

- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

違反

このクラスの特徴は、すべてのレポートが違反であることです。警告と異なり保護パスの計算の妨げとなるため、これらは警告よりも「深刻」であると見なされます。

初期配置計算違反

ViolationFrrProtectionInadequate

トンネルの FRR 保護は、指定された保護レベルを満たしていません。

フィールド：

- [Report Type]：レポート タイプの名前。
- [Description]：違反によって通知された問題の説明。
- [Required FRR Protection Level]：バックアップ トンネルが存在しており、リンク障害が発生した場合に、MPLS トラフィック エンジニアリング トンネルで、バックアップ トンネルの使用をイネーブルにするために使用します。可能なレベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
- [Path]：トンネルパス。
  - [Node]：デバイスのホスト名。保護レベルが [Link, SRLG & Node] の場合に限り表示されます。
  - [Protected (Node)]：各ノードが保護されている（[Yes]）か、保護されていない（[No]）かを示します。保護レベルが [Link, SRLG & Node] の場合に限り表示されます。
  - [Link Label]：リンクのインターフェイスの IP アドレス。
  - [Protected (Link)]：各リンクが保護されている（[Yes]）か、保護されていない（[No]）かを示します。

ViolationInconsistentResourceAttributeChanges

リソース上の 1 つ以上の属性を変更しようとするトポロジ変更が原因で、属性のペアの 1 つが一致しなくなります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Resource]：
  - [Id]：ネットワーク リソースを表すヘッド デバイスまたはヘッド インターフェイスの ID。
  - [Type]：リソース デバイスまたはインターフェイス。
- [Attributes]：
  - [Attribute]：一致していない属性の名前。
  - [New Value]：ユーザが指定する新規属性値。

ViolationInconsistentTunnelAttributeChanges

トンネル上の 1 つ以上の属性を変更しようとするトンネル変更が原因で、属性のペアの 1 つが一致しなくなります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
- [Attributes]：
  - [Attribute]：一致していない属性の名前。
  - [New Value]：ユーザが指定する新規属性値。

ViolationLinkAffinityMismatch

プライマリ トンネルのパスに含まれている有向リンクの少なくとも 1 つに、トンネルのアフィニティ ビットおよびマスクと一致する属性フラグがありません。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Affinity Bits/Mask]：トンネルのアフィニティ ビットおよびマスク。
- [Path]：トンネル パスの名前。
  - [Outgoing Interface]：発信インターフェイスのホスト名や IP アドレス。
  - [Attribute Flags]：比較する属性とトンネルのアフィニティ ビットをリンクします。有効なパスを持たせるには、すべてが同一でなければなりません。少なくとも 1 つが異なる場合、違反がトリガーされます。

ViolationLinkPoolOversubscribed

有向リンクに指定された帯域幅プールが、パススルーするプライマリ トンネルによってオーバー サブスクライブされました。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Directed Link]：
  - [Head Device/Interface]：ヘッド デバイスのホスト名およびインターフェイスの IP アドレス。
  - [Tail Device/Interface]：宛先（テール）デバイスまたはインターフェイスのホスト名。
  - [Pool]：グローバル プールまたはサブプール。
  - [Pool Bandwidth]：リンク上で割り当てられたグローバル プールまたはサブプールの帯域幅。
- [Primary Tunnel (table)]：リンク リソースを使用しているトンネルの数を指定します。
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Pool]：グローバル プールまたはサブプール。
  - [Path]：トンネル パスの名前。

ViolationMaxReRoutesExceeded

このソリューションのプライマリ トンネル リルートの数は、指定された最大数を超えています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Number of re-routes in solution]：計算エンジンによって推奨されたリルートの数。
- [Specified maximum number of re-routes]：許容されるリルートの最大数。

ViolationNoPathInLayout

トポロジにすでに配置されている他のプライマリ トンネルがある場合、要求したプライマリ トンネルに正規パスは使用できません。（注）ユーザ要求のパスに示されたこの違反は、他のプライマリ トンネルが存在するために、要求したパスにプライマリ トンネルを配置できなかったことだけを意味します。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。

- [Pool]：グローバル プールまたはサブプール。
- [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Propagation Delay]：トラフィックがリンクに沿ってヘッド インターフェイスからテール インターフェイスまで移動する時間。
- [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationNoPathInTopology

トポロジに配置されている他のプライマリ トンネルにかかわらず、要求したプライマリ トンネルに有効なパスは使用できません。（注）ユーザ要求のパスに示されたこの違反は、他のトンネルとは関係なく、要求したパスにプライマリ トンネルを配置できなかったことだけを意味します。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：（宛先）テール ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。
  - [Pool]：グローバル プールまたはサブプール。
  - [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
  - [Propagation Delay]（任意）：トラフィックが要求されたパスに沿って移動するときに許容される最大時間。
  - [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationNoTunnelForDemand

ネットワークにはこのトンネルで使用できる有効なパスはありますが、要求されたプライマリ トンネルを実装しているパスはありません。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。
  - [Pool]：グローバル プールまたはサブプール。

- [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Propagation Delay]（任意）：トラフィックが要求されたパスに沿って移動するときに許容される最大時間。
- [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationPathMismatch

プライマリ トンネルのパスが、ユーザ指定パスに指定されたパスと異なります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Actual Path]：違反と関連付けられたトンネルの実際のパス。
  - [Requested Path]：トンネルのユーザ指定のパス。

ViolationPathNotConnected

プライマリ トンネルのパスが「接続」されていません。つまり、アップ管理ステータスのリンクによる接続シーケンスがトンネルのヘッドとテールの間に形成されていないか、ループを含んでいます。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Path]：トンネル パスの名前。

ViolationPathUsesMissingLinks

トンネル変更により、パスまたは「ユーザ要求のパス」がこのトポロジに存在しない 1 つ以上の有向リンクを使用するようにトンネルを作成または変更しようとしています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Change Type]：[Add Tunnel] または [Modify Tunnel]。

- [Path Type] : [Requested] または [Actual]。
- [Path] : トンネル パスの名前。
- [Outgoing Interface] : リンクが欠落しているかどうかに従い [Yes] または [No]。
- [Incoming Interface] : リンクが欠落しているかどうかに従い [Yes] または [No]。

ViolationPrimaryTunnelDelayTooLong

プライマリ トンネルの伝搬遅延は、指定されている [Maximum Propagation Delay] を超えています。

フィールド :

- [Report Type] : 品質レポート、警告レポート、または違反レポート。
- [Description] : 違反によって通知された問題の説明。
- [Required Max Propagation Delay] : トラフィックが要求したパスに沿って移動するときに許容される最大時間。
- [Primary Tunnel] :
  - [Name] : 名前とトンネル番号で構成されたトンネル識別子。
  - [Head] : ヘッド ルータのホスト名。
  - [Tail] : 宛先（テール）ルータのホスト名。
  - [Path] : トンネル パスの名前。
  - [Actual Propagation Delay]（テーブル）: トラフィックがパス全体の各リンクに沿って移動するときにかかる時間。
    - [Link] : パス内のリンク セグメント。
    - [Propagation Delay] : トラフィックが各リンク セグメントを移動する時間。

ViolationResourceIdUnknown

ID を指定してリソース（リンク、ルータ、または SRLG）を削除または変更しようとしたときに、指定された ID のリソースが存在していません。

フィールド :

- [Report Type] : 品質レポート、警告レポート、または違反レポート。
- [Description] : 違反によって通知された問題の説明。
- [Resource to be removed] :
  - [Id] : ネットワーク リソースを表すヘッド デバイスまたはヘッド インターフェイスの ID。
  - [Type] : リソース デバイスまたはインターフェイス。

ViolationTunnelIdInUse

すでに存在している ID を指定してプライマリ トンネルを追加しようとしています。

フィールド :

- [Report Type] : 品質レポート、警告レポート、または違反レポート。
- [Description] : 違反によって通知された問題の説明。
- [Tunnel to Add] :
  - [Name] : 名前とトンネル番号で構成されたトンネル識別子。
  - [Head] : ヘッド ルータのホスト名。

  - [Tail] : 宛先（テール）ルータのホスト名。
- 既存のトンネル：
  - [Name] : 名前とトンネル番号で構成されたトンネル識別子。
  - [Head] : ヘッド ルータのホスト名。
  - [Tail] : 宛先（テール）ルータのホスト名。

ViolationTunnelIdUnknown

ID を指定してプライマリ トンネルの削除または変更しようとしたときに、指定された ID のトンネルが存在していません。

フィールド：

- [Report Type] : 品質レポート、警告レポート、または違反レポート。
- [Description] : 違反によって通知された問題の説明。
- [Tunnel to Remove] :
  - [Id] : Prime Provisioning で使用される一意のトンネル識別子。

保護計算違反

ViolationAggregateBandwidthOnLink

この要素は、このリンクを通過しますが、バックアップ トンネルの帯域幅に設定されている最大帯域幅クォータは、このリンクのバックアップ帯域幅を超えています。

フィールド：

- [Required Bandwidth]（トンネル起因）: リンク上のトンネルの必須帯域幅。
- [Link] :
  - [Backup Bandwidth] : リンクの使用可能な合計帯域幅。
  - [Head Router] : ヘッド ルータのホスト名。
  - [Head Interface] : ヘッド インターフェイスの IP アドレス。
  - [Tail Router] : 宛先（テール）ルータのホスト名。
  - [Tail Interface] : 宛先（テール）インターフェイスの IP アドレス。
  - [Label] : リンク上のインターフェイスの IP アドレス。
  - [Admin Status] : リンクが**アップ**なのか**ダウン**なのかを示します。

ViolationBadBackupTunnel

トンネルは、この要素越しのフローを保護しません。

ViolationBandwidthProtectionMismatch

フローを保護しているすべてのトンネルのトンネル バックアップ帯域幅クォータの合計は、フローの最大帯域幅と一致していません。

フィールド：

- [Protected bandwidth] : 保護パスの保護可能な帯域幅。
- [Flow] :
  - [Maximum Bandwidth] : 要素で使用可能な最大帯域幅。

- [Head Links]：このフローの保護済みインターフェイス。
- [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
- [Tail Router]：宛先（テール）ルータのホスト名。
- [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationLinkLevelTunnelDelayTooLarge

バックアップ トンネルの遅延は許容値を超えています。

フィールド：

- [Maximum allowed delay]：バックアップ トンネルで許容される最大遅延。
- [Actual delay of tunnel]：バックアップ トンネルの実際の遅延。

ViolationNoBackupTunnels

要素を通過するこのフローを保護しているバックアップ トンネルはありません。

フィールド：

- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationPassesThroughSRLG

バックアップ トンネルは、Shared Risk Link Group（SRLG; 共有リスク リンク グループ）に含まれるリンクから開始されているこの要素を通過するフローを保護しています。一方、このトンネルは、同じ SRLG 内の別のリンクも通過しています。

フィールド：

- [Link]：
  - [Backup Bandwidth]：リンクの使用可能な合計帯域幅。
  - [Head Router]：ヘッド ルータのホスト名。
  - [Head Interface]：ヘッド インターフェイスの IP アドレス。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Tail Interface]：宛先（テール）インターフェイスの IP アドレス。
  - [Label]：リンク上のインターフェイスの IP アドレス。
  - [Admin Status]：リンクが**アップ**なのか**ダウン**なのかを示します。
- [SRLG]：ユーザ定義の SRLG 名。
- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。

- [Head Links]：このフローの保護済みインターフェイス。
- [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
- [Tail Router]：宛先（テール）ルータのホスト名。
- [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationUsesFailedElement

この要素を保護するバックアップ トンネルでもこの要素を使用しています。

ドキュメント タイプ定義（DTD）ファイル

ドキュメント タイプ定義（DTD）ファイルは、Prime Provisioning へのバルク データ インポート用の XML インポート ファイルに必要なルールを提供します。

Prime Provisioning へのトンネルのインポート方法の手順については、「プライマリ トンネルのインポート」（P.7-52）を参照してください。

ここでは、次の内容について説明します。

DTD ファイル

これは、Prime Provisioning に付属している DTD ファイルです。

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Data Definition for file based tunnel import -->

<!-- Import File Structure -->
<!ELEMENT IMPORT_DATA (TUN_ADD|TUN_CHANGE|TUN_DELETE|TUN_MIGRATE)+ >

<!-- Notes on attributes:
     importId:must be unique within the file,
          it is alphanumeric, must begin with alpha character,
          and no special character
     head, tail:hostname of valid TE enabled device
     policy:name of existing managed tunnel policy
     bw: must be numeric and values between 0-2147483647
     tnum:is the number portion of a tunnel interface
          E.g. for "interface tunnel3", use tnum="3"
          must be numeric and values between 0-65535
-->


<!-- Tunnel Add

   - #IMPLIED attributes are optional, if not specified, defaults to null
   - If tnum is not specified, system will generate tunnel number
   - To enable auto bandwidth, specify AUTOBW element
```

```
   - bw is required if autobw is not enabled
   - By default, tunnel will be created with a system path and a dynamic path

-->

<!ELEMENT TUN_ADD (AUTOBW?)>
<!ATTLIST TUN_ADD
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tail CDATA #REQUIRED
    policy CDATA #REQUIRED
    bw CDATA #IMPLIED
    tnum CDATA #IMPLIED>


<!-- Tunnel Change

  - #IMPLIED attributes are optional, if not specified, value on existing
    tunnel is kept
  - To enable auto-bw, or to change auto-bw parameters, specify AUTOBW element
  - To disable auto-bw, set disableAutoBw="yes" and do not specify AUTOBW element
  - Existing tunnel path cannot be changed directly, setting reroutable="true"
    will enable system to reroute the tunnel if necessary

-->

<!ELEMENT TUN_CHANGE (AUTOBW?)>
<!ATTLIST TUN_CHANGE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED
    policy CDATA #IMPLIED
    bw CDATA #IMPLIED
    disableAutoBw (yes) #IMPLIED
    reroutable (true|false) #IMPLIED>


<!-- Tunnel Delete

  - all attributes are required to identify tunnel to be deleted

-->

<!ELEMENT TUN_DELETE EMPTY>
<!ATTLIST TUN_DELETE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED>


<!-- Tunnel Migrate

  - #IMPLIED attributes are optional, if not specified, value on existing
    tunnel is kept
  - All comments under Tunnel Change (above) applies to Tunnel Migrate
  - only unmanaged primary tunnel can be migrated
  - for tunnels with unmanaged tunnel policy, must specify a managed policy
  - for tunnels that was non-conformant:
         . if bw was zero, specify a new bw or enable auto-bw
         . if path was dynamic or non-conformant, the path options will be
           replaced with a system path and a dynamic path, and reroutable will
           be set to true.
  - reroutable attribute applicable only for tunnel that had a conformant first
         explicit path (i.e. explicit path with no loopback)
```

```
-->

<!ELEMENT TUN_MIGRATE (AUTOBW?)>
<!ATTLIST TUN_MIGRATE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED
         policy CDATA #IMPLIED
         bw CDATA #IMPLIED
    disableAutoBw (yes) #IMPLIED
         reroutable (true|false) #IMPLIED>


<!-- Auto Bandwdith

  - #IMPLIED attributes are optional, if not specified, value is set to null
    for TUN_ADD and existing value is kept TUN_CHANGE
  - maxBw is required when used in TUN_ADD or if existing tunnel is not auto-bw
    enabled
  - minBw and maxBw must be numeric and values between 0-2147483647
  - maxBw must be greater than minBw if specified
  - freq must be numeric and values between 300-604800

-->

<!ELEMENT AUTOBW EMPTY>
<!ATTLIST AUTOBW
    freq CDATA #IMPLIED
    minBw CDATA #IMPLIED
    maxBw CDATA #IMPLIED>
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!--  Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!--  Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!--  Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!--  Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>
```

例

次に、「DTD ファイル」（P.7-112）で指定した DTD ファイルに準拠する、トンネル インポートの XML ファイルの例を示します。これは、追加、変更、削除、および移行操作の各サンプル ブロックで構成されています。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!--  Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!--  Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!--  Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!--  Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>
```

トラフィック エンジニアリング管理の概念

この章では、Cisco Prime Provisioning の概要と、このマニュアルで使用されるいくつかの概念について説明します。この章の内容は、次のとおりです。

- 「Prime ProvisioningTEM の概要」（P.7-116）
- 「Prime Provisioning の機能」（P.7-116）
- 「Prime ProvisioningTEM の基礎」（P.7-116）
  - 「管理対象 / 管理対象外プライマリ トンネル」（P.7-116）
  - 「Conformant/Non-Conformant トンネル」（P.7-117）
  - 「複数の同時実行ユーザ」（P.7-118）
  - 「複数の OSPF 領域」（P.7-119）
  - 「帯域幅プール」（P.7-121）
  - 「計画ツール」（P.7-121）
  - 「接続保護（CSPF）バックアップ トンネル」（P.7-122）
  - 「クラスベース トンネル選択」（P.7-123）

– 「ポリシーベース トンネル選択」（P.7-123）。

Prime ProvisioningTEM の概要

TEM は、Prime Provisioning のトラフィック エンジニアリング管理モジュールです。トラフィックの Service Level Agreement（SLA; サービス レベル契約）に基づく保証の提供を目的として Multiprotocol Label Switching Traffic Engineering（MPLS TE; マルチプロトコル ラベル スイッチング）プライマリ トンネルおよびバックアップ トンネルを管理するためのツールです。帯域幅保護管理、ネットワーク検出、および MPLS TE の設定のサポートを提供します。また、高度なプライマリ パス計算ツールや要素保護のためのバックアップ トンネル計算機能など、多くの強力な計画ツールが含まれています。

予測可能性の要件、QoS 要件に適合するトラフィック フロー、および保証帯域幅による迅速な復旧をサポートするための MPLS TE メカニズムを搭載しており、厳格な SLA パフォーマンス基準（アベイラビリティ、遅延、ジッター）を確実に満たします。

Prime Provisioning の機能

Prime Provisioning は、さまざまな MPLS TE プライマリ管理機能を追加します。

- トンネル監査：トンネルの変更後に不一致を検出します。
- トンネル アドミッション：新しいトンネルをネットワークに受け入れます。
- トンネル修復：ネットワークやサービスの変更後にトンネルの不一致を解決します。
- ネットワーク グルーミング：ネットワーク全体の利用を最適化します。

さらに、Prime Provisioning は次のような Prime Provisioning 機能との連携および統合も実現します。

- サービス アクティベーション フォーカス
- 他の Prime Provisioning モジュールとの統合
- データ パーシステンス
- ユーザの目的のロギング
- サービス状態の管理
- サービスの監査
- Web ベースの GUI
- Role Based Access Control（RBAC; ロール ベース アクセス コントロール）

Prime ProvisioningTEM の基礎

Prime Provisioning の動作方法を理解するには、最初に特定の重要な概念を知っておく必要があります。

管理対象 / 管理対象外プライマリ トンネル

Prime Provisioning では、管理対象トンネルの概念が TE 計画アクティビティの中心にあります。

次の違いを理解しておくことが重要です。

- 管理対象 TE トンネル：

  - （設定 / 保持）優先順位が 0
  - 0 以外の RSVP 帯域幅
  - 明示的な最初のパス オプション
  - 自動帯域幅には最大値が必要
- 管理対象外トンネル：他のすべてのトンネル。

Prime Provisioning のグラフィカル ユーザ インターフェイス（GUI）には、管理対象トンネルと管理対象外トンネルを操作するための別個のエントリ ポイントがあります。

Conformant/Non-Conformant トンネル

Conformant トンネルと Non-Conformant トンネルについて理解することは、Prime Provisioning を効率的に使用するために不可欠です。

Prime Provisioning は Conformant トンネルのみを作成できます。Non-conformant トンネルは、TE 検出プロセスを介して導入できます（ユーザ ガイドの「TE ネットワーク検出」（P.7-11）を参照）。

Conformant/Non-Conformant トンネルの定義

Prime Provisioning の設計では、Conformant トンネルと Non-Conformant トンネルは明確に区別されています。

- Conformant トンネル：Prime Provisioning の TE 管理パラダイム（下記を参照）を満たす正常に動作するトンネルです。管理対象トンネルは Conformant トンネルにのみなることができます。0 以外の優先順位の管理対象トンネルも Conformant トンネルになることができます。ただし、Conformant トンネルは必ずしも管理対象トンネルではありません。

  接続保護トンネルは、トンネル帯域幅が 0 で、バックアップ帯域幅が無制限であり、最初のパス オプションが「exclude address」である場合は、Conformant = true とマークされます。BW 保護設定では、トンネルに 0 以外のバックアップ帯域幅、およびストリクト パス オプション 1 が定義されている必要があります。
- Non-Conformant トンネル：Prime Provisioning の帯域幅保証を満たす能力に影響する可能性のある TE トンネルです。自動帯域幅に最大帯域幅が未設定、プリエンプションの可能性、ダイナミック パスなど、未知の帯域幅要件が原因で発生することがあります。優先順位が 0 である管理対象外トンネルも Non-Conformant トンネルになることがあります。

  次に、Non-Conformant トンネルの例を示します。
  - 設定および保持優先順位が 0 で、最初のパス オプションが明示パスであるが、帯域幅は 0 であるトンネル
  - 設定および保持優先順位が 0 で、帯域幅は 0 以外であるが、最初のパス オプションがダイナミック パスであるトンネル
  - 設定および保持優先順位が 0 で、明示パス オプションが 1 であり、自動帯域幅の最大値が定義されていないトンネル
  - Conformant = false とマークされた接続保護トンネルは、バックアップ トンネルのために予約されており、トンネル帯域幅 0、無制限のバックアップ帯域幅、最初のパス オプション「exclude address」のいずれも設定されていません。

  上記のトンネルは、なぜ Non-Conformant なのでしょうか。Prime Provisioning は、設定および保持優先順位が 0 であるトンネルをすべて管理し、それらが通過するリンクがいずれも十分な帯域幅を持ち、アフィニティが一致、TE ポリシーに定義された遅延または FRR 制約に違反しないことを確認するからです。

ただし、トンネルのパスがダイナミック パスであるか、トンネルが必要とする帯域幅の量が定義されていない場合、Prime Provisioning はトンネルの管理に必要な情報を得られないため、そのトンネルを Non-Conformant とマークします。すべての Non-Conformant トンネルは [TE Unmanaged Primary Tunnels SR] ウィンドウに表示されます。

Non-Conformant トンネルの管理

Non-Conformant トンネルは、SLA 違反の原因となる可能性があるだけでなく、管理対象トンネルに悪影響（帯域幅を奪うなど）を与えるおそれもあることを理解しておくことが重要です。

ただし、Non-Conformant トンネルが検出されると、警告がログに記録されます。Prime Provisioning は、Non-Conformant トンネルを追跡して廃棄します。

したがって、Conformant トンネルの方が望ましいと言えます。Conformant トンネルによって、システムは管理対象トンネルの帯域幅保証を提供できます。管理対象外の Non-Conformant トンネルは、必要な帯域幅を提供したりしなかったりするため、帯域幅保証は提供されません。

Non-Conformant トンネルがある場合は、設定および保持優先順位を 0 以外の値に変更する（管理対象トンネルに対するプリエンプション処理を実行できないようにするため）か、管理対象トンネルに移行させてツールが適切な明示パスを検出できるようにします。

複数の同時実行ユーザ

以前のリリースでは、TEM は単一の GUI ユーザしかサポートしていませんでした。本リリースは、ブラウジング、更新、プロビジョニングのいずれの操作においても複数の同時実行ユーザをサポートします。

管理対象トンネルと管理対象外トンネルの同時使用

複数ユーザ機能が TEM にどのように実装されているかを理解するためには、Managed トンネルと Unmanaged トンネルの違いを理解することが重要です。これについては、「管理対象 / 管理対象外プライマリ トンネル」（P.7-116）で説明しています。

複数のユーザのサポートでは管理対象および管理対象外トンネルの処理方法に重要な違いがあります。

- 管理対象トンネルは、すべて SR によってカプセル化されます。SR の操作により、Router Generator サーバによるパス計算の後にスナップショット内のすべてのオブジェクトが最適化される可能性があります。
- 管理対象外トンネルの場合、SR はトンネルヘッド エンド ルータとして定義されます。そのため、管理対象外トンネルには、いくつかの制限があります。たとえば、2 人のユーザが同じデバイスで同時にプロビジョニングすることはできません。
- TEM は、管理対象外トンネル SR が同じデバイスで同時にプロビジョニングすることを許可しませんが、管理対象外トンネル SR による複数のデバイスでの同時プロビジョニングはサポートします。
- 管理対象トンネルは、すべて各 TE プロバイダーの共有管理対象 TE トンネル SR 内に存在します。管理対象外トンネルの場合は、ヘッド デバイスごとに別個の管理対象外 TE トンネル サービス要求が作成されます。TEM は、1 つの TE プロバイダーにつき複数の SR をサポートします。

複数の TEM ユーザが TEM でブラウジングおよびプロビジョニングを実行できます。最大 20 人までの同時ユーザがサポートされ、そのうちの 7 人までがプロビジョニング タスクを実行できます。

以前は、管理対象と管理対象外の両方のプライマリ トンネルがすべて TE プロバイダーごとに 1 つの TE トンネル SR に存在していました。現在は、管理対象トンネルへの複数の同時変更を可能にするために、TE トンネル SR が TE プロバイダーあたり 1 つの管理対象トンネル SR とヘッド TE ルータあたり 1 つの管理対象外トンネル SR に分割されています。

同じ SR で並行プロビジョニングを行うことはできませんが、管理対象外トンネルについては SR がルータ レベルで存在するため、管理対象外トンネルを同時に複数のルータにプロビジョニングすることができます。

ロッキング メカニズム

管理対象外トンネルをプロビジョニングすると、そのトンネルのヘッド TE ルータがロックされます。ロックされていることは、[TE Nodes] ウィンドウの [System Lock Status] 列で確認できます。ロッキングによって、プロビジョニング タスクが完了し、TE ルータのロックが解除されるまで、他のユーザはそのルータにどのような種類のトンネルも配置できなくなります。

ロッキング メカニズムは、バックアップ トンネル、リソース SR、リンク削除、TE トラフィック アドミッションなどの Prime Provisioning 機能にも適用されます。リソース SR には、明示パスの削除/編集、保護要素の削除、SRLG の削除/編集などが含まれます。

リンク削除の場合、一定レベルのインテリジェンス機能が組み込まれています。ユーザまたは Prime Provisioning によって再ルーティングまたは削除できるトンネルが存在せず、TE 関連オブジェクトだけが残っている場合、リンクを削除するためには、ユーザによる介入が必要となります。このとき、削除対象として選択されたインターフェイスを保護するバックアップ トンネルがある場合は、バックアップ トンネルを配置する操作の実行中、ロッキング メカニズムが働きます。TE リンクの削除の詳細については、ユーザ ガイドの 「TE リンクの削除」（P.7-25）を参照してください。

発生する可能性のあるエラーについては、ユーザ ガイドの 「操作エラーのロック」（P.7-82）を参照してください。

管理対象プライマリ トンネルまたはバックアップ トンネルをプロビジョニングすると、そのトンネルに関連付けられている TE プロバイダーがロックされます。ロックされていることは、[TE Provider] ウィンドウの [System Lock Status] 列で確認できます。TE プロバイダー レベルのロックによって、トンネルがどの TE ルータを起点としているかに関係なく、別のユーザがその TE プロバイダーでトンネルを変更することを防止できます。

管理対象トンネルおよびバックアップ トンネルのロッキング メカニズムと管理対象外トンネルのロッキング メカニズムが異なるのは、管理対象トンネルとバックアップ トンネルがすべての制約を満たす最適なルートを見つけるためにパス生成アルゴリズムを使用し、そのアルゴリズムが、ルーティング決定基準として、TE トポロジとそこに含まれるすべてのトンネルの安定したグローバル ビューを必要とするからです。これを実現する唯一の方法は、一度に 1 人のユーザだけが変更を実行できるようにすることです。

Prime Provisioning のロッキング メカニズムを管理する方法の詳細については、ユーザ ガイドの 「ロック メカニズムの管理」（P.7-81）を参照してください。

複数の OSPF 領域

Prime Provisioning は、複数の Open Shortest Path First（OSPF）内での TE トンネルの検出、管理、プロビジョニングをサポートします。

Prime Provisioning の管理対象となるのは、OSPF 領域の範囲内にあるプライマリ TE トンネルとバックアップ TE トンネルだけです。複数の OSPF 領域にまたがる検出および作成はサポートしていません。

Prime Provisioning では、OSPF 領域は TE プロバイダーによって表されます。領域を TE プロバイダーに割り当てた後で変更することはできません。1 つの Prime Provisioning プロバイダーに複数の TE プロバイダーを関連付けることができます。

TE 検出に適したデバイス

複数の OSPF 領域があるネットワークでは、各 OSPF 領域が TE プロバイダーで表されるため、OSPF 領域内のどのルータでも TE 検出に使用できます。1 つのプロバイダーに属する複数の TE プロバイダー（複数の OSPF 領域）を使用することにより、複数の領域にまたがる L3VPN のプロビジョニングが可能になります。

（注）　Prime Provisioning は、複数の領域にまたがる TE トンネル（ある領域にヘッド ルータがあり、別の領域にテール ルータがあるトンネル）を検出またはプロビジョニングしません。

複数の領域があるネットワークを検出するためには、TE 検出を使用して各領域を順に検出する必要があります（ユーザ ガイドの「TE ネットワーク検出」（P.7-11）を参照）。シード ノードは、Area Border Router（ABR; エリア境界ルータ）を含め、領域内のどのデバイスでもかまいません。

TE 検出と TE 領域 ID

TE 検出には TE プロバイダーが関連付けられ、各 TE プロバイダーには領域が割り当てられます。この領域は TE プロバイダーの作成プロセスで割り当てられます（ユーザ ガイドの「TE プロバイダーの作成」（P.7-8）を参照）。この領域は単純な整数値またはドット付き 10 進表記（領域 0.6.0.0 など）です。

TE プロバイダー オブジェクトは、作成時の指定または検出時の自動入力によって対象とする領域を認識し、ドット表記と 10 進表記の変換に対応します。デフォルトはネットワークで使用されている表記です。

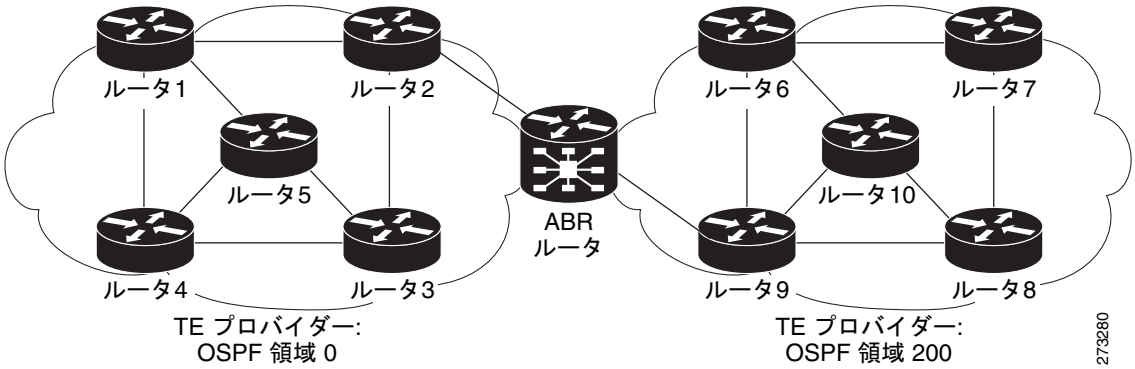
選択した TE プロバイダーがある領域に対して検出を実行すると、その領域に関連付けられたすべてのトンネルおよび明示パスが Prime Provisioning データベースにインポートされます。領域単位の検出の実行手順については、ユーザ ガイドの「エリア別ディスカバリの管理」（P.7-16）を参照してください。

複数の OSPF 領域があるネットワークの例

TE プロバイダー内の TE ルータを複数のリージョン（地域など）に割り当てることにより、デバイスを論理的な基準に基づいてリージョンにグループ化できます。また、Prime Provisioning ではリージョンに基づくフィルタリングが可能です。オブジェクトを特定のリージョンに割り当てるには、検出の実行後、[Inventory] > [Provider Devices] から手動で行います。PE デバイスのリージョンは、[Select Region] ポップアップ ウィンドウで変更できます。

次の図 7-32 に示す例では、2 つの TE プロバイダーがそれぞれ 1 つの Prime Provisioning プロバイダー内に作成され、視覚化された 1 つの OSPF 領域を担当します。

図 7-32　複数の OSPF 領域があるネットワーク



TE の管理方法については、ユーザ ガイドの 「TE プロバイダーの作成」（P.7-8）を参照してください。

帯域幅プール

各 TE 対応のインターフェイスの帯域幅には、ネストされた複数の帯域幅プールが割り当てられます。現在、IOS は、グローバル プールとサブ プールという 2 種類の帯域幅プールをサポートしています。

帯域幅プールについての理解を深めるために、図 7-33 を参照してください。

図 7-33　帯域幅プール

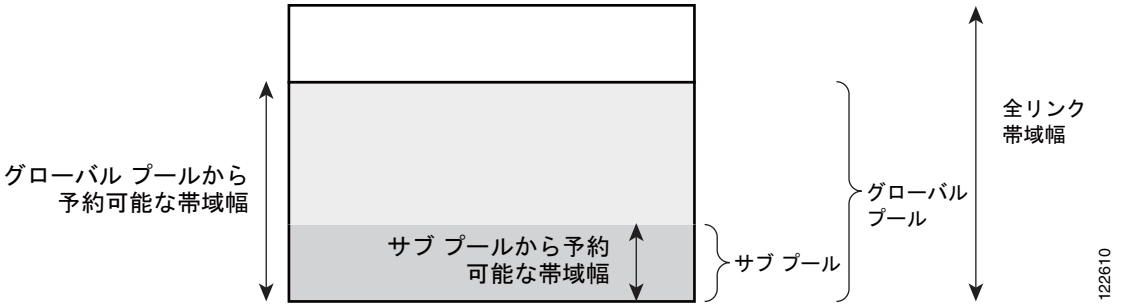


図 7-33 に示すように、サブ プールはグローバル プール内にネストされています。したがって、プライマリ トンネルがサブ プールから帯域幅を予約すると、同じ帯域幅がグローバル プールでも予約されます。

サブ プールでの帯域予約（プライマリ トンネル）は、合計でサブ プールのサイズを超えてはなりません。同様に、グローバル プールでの帯域予約は、合計でグローバル プールのサイズを超えてはなりません。

計画ツール

ここでは、トラフィック エンジニアリングされたネットワークの改善計画を What-If シナリオを基づいて評価するためのツールについて説明します。

計画ツールには、次の機能が含まれます。

- プライマリ計画ツール：

  - トンネル監査：トンネルまたはリソースの変更が提案されているかどうかにかかわらず、既存のネットワークのプライマリ配置に不一致がないかどうか調べます。
  - トンネル配置：通常は、新しいトンネルに使用します。トンネル配置機能では、新しいルートを生成できます。この機能は、それまでパスがなく、配置することが必要なトンネルに使用できます。
  - トンネル修復：トンネル監査の実行後（問題が検出された場合）に実行します。トンネル修復機能には再ルーティング機能があり、トンネルの移動に使用できます。
  - グルーミング：ネットワーク全体を対象とする最適化ツールです。これは、トンネル属性が変更されていない場合にだけ利用できます。
- 保護計画ツール：
  - 監査 SR：手動で追加、変更、削除されたバックアップ トンネルについて、配置前に保護の状態を調べます。
  - バックアップ計算：選択されたネットワーク要素に最適なバックアップ トンネルを自動的に計算します。
  - 保護監査：選択された要素の保護を既存のバックアップ トンネルの観点から監査します。

これらの計画ツールは Prime Provisioning に完全に統合されており、次のような GUI のさまざまな場所から使用できます。

- TE Protected Elements（Compute Backup および Audit Protection）
- Create Managed TE Tunnel（Tunnel Audit、Tunnel Placement、Tunnel Repair、Grooming）
- Create TE Backup Tunnel（Audit SR）

接続保護（CSPF）バックアップ トンネル

TEM によって作成される帯域幅保護のバックアップ トンネルに加え、一連の CSPF-routed バックアップ トンネルも Prime Provisioning 内に作成できます。CSPF-routed バックアップ トンネルは、[TE Protection SR] ウィンドウで管理します。

接続保護バックアップ トンネルは「exclude-address」明示的パスを使用します。この明示パスは [TE Explicit Path List] ウィンドウで作成します。exclude address パスは、パスが使用するホップではなくパスが回避するホップを示す点で strict パスと異なります。どのパスが最適であるかはルータ上の CSPF アルゴリズムによって決定されますが、このアルゴリズムには exclude address パス設定のホップを使用できないという制約があります。この種のパスは、特にバックアップ トンネルで役に立ちます。exclude address パスが回避する必要のあるインターフェイスは、バックアップ トンネルの保護対象である可能性があるからです。

Prime Provisioning では、これらのバックアップ トンネルに無制限のバックアップ帯域幅が設定されます。無制限とは帯域幅が保証されないことを意味しますが、障害発生時に使用可能な最大限の帯域幅が使用されます。そのため、帯域幅保護は実質的にベスト エフォートです。ただし、接続は保証されます。接続保護バックアップ トンネルは、帯域幅保護バックアップ トンネルへの追加または代替として使用できます。

帯域幅保護バックアップ トンネルと接続保護バックアップ トンネルには、次のような違いがあります。

- 帯域幅保護バックアップ トンネルの最初のパス オプションはストリクト明示パスであるのに対し、接続保護バックアップ トンネルの最初のパス オプションは exclude address 明示パスです。
- 帯域幅保護バックアップ トンネルにはバックアップ帯域幅が定義されているのに対し、接続保護バックアップ トンネルでは無制限のバックアップ帯域幅がベスト エフォート方式で使用されます。

- 帯域幅保護バックアップ トンネルは、最適なバックアップ トンネルを生成して既存のトンネルが要素を完全に保護することを確認するルート ジェネレータ アルゴリズムに渡されるのに対し、接続保護バックアップ トンネルはルート ジェネレータ アルゴリズムに渡されないため、トンネルが目的を果たしていることをユーザが確認する必要があります。

クラスベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Class-Based Tunnel Selection（CBTS; クラスベース トンネル選択）を使用すると、同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルに、さまざまなサービス クラス（CoS）値を指定して、トラフィックを動的にルーティングおよび転送できます。パケットの CoS 値は EXP ビット内にあります。8 個の EXP ビットがあり、0 ～ 7 の番号が付いています。

同一ヘッド エンドから同一テール エンドへの TE（または DS-TE）トンネルは、複数の CoS 値を持つように設定できます。設定後、CBTS は、次の要件を満たすトンネルに各パケットを動的にルーティングして転送します。

- 標準の自動ルートまたはスタティック ルートを使用してトラフィック アドミッションの対象として選択されている。
- EXP ビットがパケットの EXP ビットと一致している。

したがって、CBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

CBTS は DS-TE トンネル経由でダイナミック ルーティングを行い、設定が最小限で済むので、大規模なネットワークにおいて DS-TE の配置が大幅に軽減されます。CBTS は、すべての CoS 値をさまざまな種類のトンネルに配布できます。

CBTS 機能には次の制限があります。

- 1 つの宛先について、同じテール エンドで終端するトンネルを使用してすべての CoS 値が伝送されます。すべての CoS 値がトンネルで伝送されるか、またはトンネルでまったく値が伝送されないかのいずれかです。したがって、1 つの宛先について、一部の CoS 値を DS-TE トンネルでマッピングし、その他の CoS 値を最短パス優先（SPF）ラベル配布プロトコル（LDP）または SPF IP パスでマッピングすることはできません。
- CBTS では、複数のトンネルで特定の EXP 値のロードバランスを図ることはできません。2 つ以上のトンネルが特定の experimental（EXP）値を伝送するように設定されている場合、CBTS はその中から 1 つのトンネルを選択して、この EXP 値を伝送します。
- Any Transport over MPLS（AToM）、MPLS TE Automesh、または Label-Controlled（LC）-ATM では、CBTS の動作はサポートされません。

グローバル スタティック ルートを使用してトンネルへのトラフィック アドミッションが行われ、特定の宛先に対し、管理上の重みが同じであるトンネルが複数ある場合は、CBTS 属性がトンネルの選択基準となります （上記の CBTS でのロードバランスに関する説明を参照してください）。

ポリシーベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Policy-Based Tunnel Selection（PBTS; ポリシーベース トンネル選択）を使用すると、トラフィックを同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルにポリシーに基づいて動的にルーティングおよび転送できます。ルーティング アルゴリズムは、フォワーディング ルックアップの前にヘッドエンド ルータの入力インターフェイスで実行されます。

Prime Provisioning の PBTS 実装では、トラフィックはインターフェイス コマンド policy-class を使用して特定の TE トンネルに転送されます。CBTS は IOS デバイスを対象としていますが、PBTS は IOS XR デバイス用に厳密に設計されています。

CBTS と同じように、PBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

（注）　Prime Provisioning は、ポリシー クラスをプロビジョニングするわけではなく、トンネルに既存のポリシー クラスを関連付けるだけです。そのためには、policy-class 属性を 1 ～ 7 の値に設定します。

CBTS の詳細については、「クラスベース トンネル選択」（P.7-123）を参照してください。

PBTS および IOS XR の一般的な情報については、http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/mpls/configuration/guide/gc37te.html#wp1325561 を参照してください。

CHAPTER 8

サービス要求の管理

この章では、[Service Request Manager] ウィンドウを使用して Prime Provisioning のサービス要求を管理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。

[Service Request Manager] ウィンドウへのアクセス

サービス要求を管理するには、[Operate] > [Service Requests] > [Service Request Manager] を選択します。

図 8-1 は、[Service Request Manager] ウィンドウを示しています。

図 8-1　[Service Request Manager] ウィンドウ

[Service Request Manager] ウィンドウには、このユーザ名のサービス要求の現在のリストが表示されます。このウィンドウには、各サービス要求に関する次の情報が表示されます。

- [JobID]：Prime Provisioning によってサービス要求に割り当てられたジョブ番号。

- [Data Files]：データ ファイルがサービス要求に関連付けられているかどうかを示します。サービス要求に 1 つ以上のテンプレートが関連付けられている場合、[Data Files] カラムにペーパー クリップ アイコンが表示されます。サービス要求と連携したテンプレートおよびデータ ファイルの使用方法の詳細については、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。
- [State]：サービス要求の遷移状態。詳細については、「サービス要求状態」（P.8-13）を参照してください。
- [Type]：サービス要求のタイプ。たとえば、[MPLS VPN]、[L2VPN]、[VPLS]、[VRF]、[TE]、または [EVC] などがあります。
- [Operation Type]：サービス要求の操作タイプ。たとえば、[ADD] はこのサービス要求を追加することを意味し、[MODIFY] はサービス要求が以前の状態から変更されたことを意味し、[DELETE] はこのサービス要求をデコミッションすることを意味します。
- [Creator]：サービス要求を作成した、または最後に変更したユーザのユーザ名 ID。
- [Customer Name]：サービス要求のカスタマー名。
- [Policy Name]：このサービス要求に割り当てられたポリシーの名前。
- [Last Modified]：サービス要求が作成または最後に変更された日付と時間。
- [Description]：サービス要求のオプションのテキスト説明。

[Service Request Manager] ウィンドウの最下部にあるボタンを使用して、サービス要求に対して次の操作を実行できます。

- [Create]：Prime Provisioning サービス要求を作成します。特定のサービスのサービス要求の作成の詳細については、このマニュアルの他の章を参照してください。
- [Details]：サービス要求の履歴レポートの表示、サービス要求の監査、およびコンフィグレットの表示を実行します。詳細については、「サービス要求の詳細の表示」（P.8-2）を参照してください。
- [Status]：選択されたサービス要求のリンクの表示および利用可能なログへのアクセスを実行します。詳細については、「サービス要求のステータスの表示」（P.8-8）を参照してください。
- [Configlet Preview]：特定のサービス要求に対してデバイスに送信されたコンフィグレットをプレビューします。詳細については、「コンフィグレットのプレビュー」（P.8-9）を参照してください。
- [Edit]：サービス要求を編集します。詳細については、「サービス要求の編集」（P.8-9）を参照してください。
- [Deploy]：サービス要求を展開します。詳細については、「サービス要求の展開」（P.8-10）を参照してください。
- [Decommission]：サービス要求をデコミッションします。詳細については、「サービス要求のデコミッション」（P.8-12）を参照してください。
- [Delete]：サービス要求を削除します。詳細については、「サービス要求の削除」（P.8-13）を参照してください。

サービス要求の詳細の表示

サービス要求の詳細には、サービス要求の展開操作の過程で生成されたサービス要求、履歴、およびコンフィグレットのリンクの終端が含まれます。サービス要求の詳細を使用して、サービス要求の問題やエラーのトラブルシューティングに役立てたり、コンフィグレットのコマンドを確認したりできます。

この項では、履歴、リンク詳細、およびコンフィグレットを含むサービス要求の詳細を表示する方法について説明します。

サービス要求の詳細を表示するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

ステップ 2　サービス要求を選択し、[Details] をクリックします。

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

[Service Request Details] ページから、次の項目の詳細な情報を表示できます。

- [Details] > [Links]：サービス要求でレポートをリンクします。
- [Details] > [History]：サービス要求の履歴のレポート。
- [Details] > [Audit]：Prime Provisioning ではサポートされません。
- [Details] > [Configlets]：サービス要求に対して Prime Provisioning により生成されたコンフィグレットを表示します。

次の項では、サービス要求のリンク、履歴、監査、およびコンフィグレットの詳細について説明します。

サービス要求リンクの詳細の表示

サービス要求リンクの詳細には、リンクの終端、PE 保護インターフェイス、VLAN ID、および CE の存在有無が含まれます。

この情報を表示するには、次のステップを実行します。

ステップ 1　[Service Request Details] ウィンドウで [Links] をクリックします。

[Service Request Link] ウィンドウが表示されます。

ステップ 2　リンクを選択して、[Details] をクリックします。

[Service Request Link Details] 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、[Service Request Link] ウィンドウに戻ります。

ステップ 4　別のリンクを選択して表示するか、[OK] をクリックして [Service Request Details] ウィンドウに戻ります。

サービス要求履歴情報の表示

サービス要求に関する履歴情報を表示するには、次のステップを実行します。

ステップ 1　[Service Request Details] ウィンドウで [History] をクリックします。

[Service Request State Change Report] ウィンドウが表示されます。

履歴レポートでは、サービス要求に関する次の情報が示されます。

- [Element name]：サービス要求に含まれるデバイス、インターフェイス、およびサブインターフェイス。
- [State]：要素が経過した遷移状態。

- [Create Time]：このサービス要求に対して要素が作成された時間。
- [Report]：このサービス要求の要素に対する Prime Provisioning の操作。

ステップ 2　[OK] をクリックして、[Service Request Details] ウィンドウに戻ります。

監査レポートのサービス要求の表示

この項では、Prime Provisioning サービス要求のコンフィギュレーションおよび機能監査レポートを表示する方法について説明します。

設定監査報告の表示

設定監査では、サービス（サービス インテント）のすべてのコマンドが、サービスに参加しているネットワーク要素に含まれているかどうかが確認されます。サービス要求が Prime Provisioning に展開されるたびに、設定監査が行われます。設定監査が行われると、Prime Provisioning はすべての Cisco IOS コマンドが存在し、正しい構文であることを確認します。監査では、展開の過程でエラーが発生しなかったことも確認します。デバイス コンフィギュレーションがサービス リクエストの定義と一致していない場合、監査は警告フラグを付け、サービス リクエストを Failed Audit 状態または Lost 状態に設定します。

設定監査は、プロビジョニングの後に一部のコマンドがネットワーク要素から削除された場合、失敗する可能性があります。これはコマンドが手動で削除されるか、他のサービスのプロビジョニングの一部として削除された場合に発生する可能性があります。設定監査が失敗する可能性がある別の理由としては、Prime Provisioning がコンフィギュレーション ファイルのコマンドを認識できない場合があります。Prime Provisioning のデフォルトの動作では、設定監査中にコンフィギュレーション ファイル内の認識されないコマンドはスキップされます。このような認識されないコマンドは、既存のコンフィギュレーションに存在していたか、コンフィギュレーション ファイルに手動で挿入された可能性があります。認識されないコマンドがコマンド ブロックの先頭にある場合、Prime Provisioning は initial コマンドを省略し、ブロック内でサブコマンドを解析します。これにより、Prime Provisioning はコンフィギュレーション ファイル内の論理フローにエラーがあると想定し、その結果監査は失敗します。

[Prime Provisioning Task Manager] を使用して、設定監査を手動で実行できます。設定監査を手動でスケジュールするためのタスクを作成する方法については、「タスク マネージャ」（P.10-25）を参照してください。

サービス要求の設定監査レポートを表示するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

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

ステップ 2　設定監査を行うサービス要求を選択します。

ステップ 3　[Details] 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　[Audit] ボタンをクリックして、ドロップダウン リストから [Config] を選択します。

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

ウィンドウには、デバイス名、ロール、および設定監査のステータスに関するメッセージが表示されます。監査に失敗した場合、メッセージ フィールドには失敗した監査の詳細が表示されます。監査失敗メッセージには、見つからないコマンドおよび設定の問題が表示されます。メッセージ フィールドの情報をよく注意して確認します。監査に失敗した場合、すべてのエラーを修正して、サービス要求を再展開する必要があります。

ステップ 5　[OK] をクリックして、[Service Request Details] ウィンドウに戻ります。

機能監査レポートの表示

機能監査によって、サービス要求または VPN のリンクが正常に動作していることが検証されます。監査では、PE デバイスの VRF ルート テーブルでのリモート CE へのルートが確認されます。Prime Provisioning は、サービス要求が展開、または強制的に再展開するたびに自動的に監査機能を行います。監査機能は、BGP ピアリングが正しくない、コアでの MPLS 設定が間違っている、またはリモート リンクがダウンしている場合に失敗する可能性があります。

[Prime Provisioning Task Manager] を使用して、機能監査を手動で実行できます。機能監査を手動でスケジュールするためのタスクを作成する方法については、「タスク マネージャ」（P.10-25）を参照してください。

サービス要求の機能監査レポートを表示するには、次の手順を実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

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

ステップ 2　機能監査を行うサービス要求を選択します。

ステップ 3　[Details] 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　[Audit] ボタンをクリックして、ドロップダウン リストから [Functional] を選択します。

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

ウィンドウには、デバイス名、ロール、および設定監査のステータスに関するメッセージが表示されます。監査に失敗した場合、メッセージ フィールドには失敗した監査の詳細が表示されます。監査失敗メッセージには、見つからないコマンドおよび設定の問題が表示されます。メッセージ フィールドの情報をよく注意して確認します。監査に失敗した場合、すべてのエラーを修正して、サービス要求を再展開する必要があります。

ステップ 5　[OK] をクリックして、[Service Request Details] ウィンドウに戻ります。

サービス要求コンフィグレットの表示

サービス要求を展開したら、Prime Provisioning は Cisco IOS または IOS XR コマンドを生成して、サービス要求に関係するすべてのネットワーク デバイス上で、該当するサービスをオンにします。

（注）　IOS デバイスの場合、コンフィグレットは CLI コマンドとして表示されます。IOS XR デバイスの場合、コンフィグレットは XML または CLI 形式で表示できます。IOS XR デバイスのコンフィグレットの表示については、「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。

生成されたコンフィグレットを表示するには、次のステップを実行します。

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。

[Service Request Configlet] ウィンドウで、コンフィグレットの表示が更新されます。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。

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　コンフィグレットの表示が完了したら、[OK] をクリックします。

IOS XR デバイスでのコンフィグレットの表示

デフォルトでは、IOS XR デバイスのサービス要求では、XML 形式でデバイスに送信される設定をログに記録します。したがって、コンフィグレットが IOS XR デバイスに表示される場合は、未加工の XML 形式で表示されます。Prime Provisioning では、コンフィグレットを CLI 形式で表示することもできます。この機能は、DCPL プロパティ **DCS/getCommitCLIConfigAfterDownload** を True に設定することでイネーブルになります（デフォルト設定）。

（注）　コンフィグレットを CLI 形式で表示するには、DCPL プロパティ **DCS/getCommitCLIConfigAfterDownload** を True に設定する必要があります。DCPL プロパティを True に設定する場合、CLI コンフィグレットは後続のサービス要求の展開に対してのみ使用できるようになります。これらは、DCPL プロパティが True に設定される前に展開されたコンフィグレットには使用できなくなります。

IOS XR デバイスのコンフィグレットを XML 形式または CLI 形式で表示するには、次のステップを実行します。

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　IOS XR 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、IOS XR デバイスを選択し、[View Configlet] ボタンをクリックします。

CLI 形式でコンフィグレットが示された [Service Request Configlet] ウィンドウが表示されます。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。

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　XML 形式でコンフィグレットを表示するには、[XML Configlet] オプション ボタンをクリックします。

ウィンドウが更新され、XML 形式でコンフィグレットが表示されます。

ステップ 8　異なる形式に切り替えるには、次のオプション ボタンを使用します。

- [XML Configlet] : XML 形式でコンフィグレットを表示します。
- [CLI Configlet] : CLI 形式でコンフィグレットを表示します。これがデフォルトの選択肢です。
- [Both] : XML と CLI の両方の形式で、コンフィグレットを並べて表示します。

ステップ 9　コンフィグレットの表示が完了したら、[OK] をクリックします。

設定ファイルの編集

既存のルータ コンフィギュレーション ファイルを表示または編集するには、次の手順を実行します。

（注）　特に、編集したファイルを実行コンフィギュレーション ファイルにするように選択した場合、コンフィギュレーション ファイルを編集するときには慎重に行ってください。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] をクリックします。

[Devices Inventory] ウィンドウが表示されます。

ステップ 2　デバイス名の横にあるチェックボックスをオンにして、表示するコンフィギュレーション ファイルのバージョンを選択します。

ステップ 3　[Config] をクリックします。

[Device Configurations] ウィンドウが表示されます。

[Device Configurations] ウィンドウに、選択したデバイスのコンフィギュレーション ファイルの現在のバージョンのリストが表示されます。設定は日時ごとに表示されます。最初にリストされているコンフィギュレーション ファイルが最新バージョンです。

ステップ 4　表示するコンフィギュレーション ファイルのバージョンを選択し、[Edit] をクリックします。

選択されているコンフィギュレーション ファイルの内容が表示されます。

表示されたデバイスのコンフィギュレーション ファイルを表示または編集できます。

ステップ 5　必要に応じて、コンフィギュレーション ファイルを編集します。

ステップ 6　ファイルの編集が完了したら、[Save] をクリックします。

サービス要求のステータスの表示

[Service Request Manager] ウィンドウから、次の項で説明されているように、サービス要求のステータス情報を取得できます。

リンクの表示

サービス要求に関連付けられたリンクに関する情報を表示するには、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、関連付けられたリンクを表示するサービス要求を選択します。

ステップ 3　[Status] ボタンをクリックして、[Links] を選択します。

[SR Link] ウィンドウが表示されます。

このウィンドウには、このサービス要求に関連付けられたリンクのリストが表示されます。

ステップ 4　情報の確認が終わったら、[Return to SRs] ボタンをクリックします。

ログの表示

サービス要求に関連付けられたログを表示するには、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、関連付けられたリンクを表示するサービス要求を選択します。

ステップ 3　[Status] ボタンをクリックして、[Logs] を選択します。

[Task Logs] ウィンドウが表示されます。

このウィンドウには、タスクの [Runtime Task Name]、[Action]、[Start Time]、[End Time]、および [Status] ごとにタスクが表示されます。このウィンドウを使用して、ログを表示または削除できます。

ステップ 4　ログを表示するには、タスクを表す行にあるチェックボックスをオンにして、[View Log] ボタンをクリックします。

[Task Log] ページが表示されます。

表示するログ レベルのタイプを設定できます。[Log Level] を指定し、[Filter] ボタンをクリックして表示する情報を表示します。

ステップ 5　[Return to Logs] をクリックして、表示する別のログを指定します。

ステップ 6　ログ情報の確認が終わったら、[Close] ボタンをクリックします。

コンフィグレットのプレビュー

コンフィグレットのプレビュー操作では、デバイスが実際にプロビジョニングされる前に選択したサービス要求のデバイスに送信されるコンフィグレットをプレビューすることができます。これにより、適用される可能性のあるすべてのテンプレートを含む必要なコンフィグレットがサービス要求で生成されることを確認することができます。

次の警告に注意してください。

- コンフィグレットのプレビュー機能は、[In Progress] および [Closed] を除くすべての状態でサービス要求に使用できます。
- コンフィグレットのプレビュー機能は、TEM サービス要求ではサポートされていません。

サービス要求のコンフィグレットをプレビューするには、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 Request Manager] ウィンドウで、サービス要求を選択し、[Configlet Preview] をクリックします。

ステップ 3　ドロップダウン リストから、次のいずれかのオプションを選択します。

- [For Deploy] : [Deploy] 操作によって生成されるコンフィグレットを生成します。
- [For Force Deploy] : [Force Deploy] 操作によって生成されるコンフィグレットを生成します。

これらの選択肢では、利用可能な 2 つの異なる展開オプションを疑似します。これは、展開のタイプが生成されるコンフィグレットに影響を与える可能性があるためです。

[Configlet Preview] ウィンドウが表示されます。ウィンドウには、サービス要求で生成された各デバイスのコンフィグレットが含まれます。

（注）　コンフィグレットはデバイスからアップロードする必要があるため、この操作には少し時間がかかる場合があります。

ステップ 4　コンフィグレットを確認したら [OK] をクリックして、[Service Request Manager] ウィンドウに戻ります。

選択されたサービス要求を展開するタスクが作成されると、この機能は [Deploy Service Request] ウィンドウからも利用できます。[Service Request Manager] ウィンドウで 1 つ以上のサービス要求を選択して、[Deploy Service Request] ウィンドウに移動します。次に、[Deploy] > [Deploy] または [Deploy] > [Force Deploy] を選択します。表示される [Deploy Service Request] ウィンドウには、選択されたサービス要求を示すテーブルが含まれます。このテーブルの [Configlet Preview] リンクをクリックして、プレビューのコンフィグレットを表示します。

サービス要求の編集

サービス要求を編集するには、次のステップを実行します。

ステップ 1　[Service Operate] > [Service Requests] > [Service Request Manager] を選択します。

ステップ 2　変更するサービス要求を選択して、[Edit] をクリックします。

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

（注）　このウィンドウの正確な名前と内容は、編集されるサービス要求のタイプに応じて異なります。

ステップ 3　エディタで必要な変更を加え、[Save] をクリックします。

対応するサービス要求の状態が [In Progress] に設定され、[Operation Type] が [Modify] に変更された [Service Requests] ウィンドウが再び表示されます。

ネットワークに変更をプロビジョニングするには、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方法については、「サービス要求の展開」（P.8-10）を参照してください。展開後、サービス要求の状態が [Deployed] に遷移したら、展開は正常に完了したことを示しています。

サービス要求の展開

ポリシーをネットワーク デバイスに適用するには、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。

デバイスの変更をネットワーク デバイスに適用するには、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。

サービス展開

サービス要求をすぐに展開するか、展開をスケジュール設定するには、次のステップを実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

[Service Requests Manager] ウィンドウが表示されます。

ステップ 2　展開するサービス要求のジョブ ID の横にあるチェックボックスをオンにします。

ステップ 3　[Deploy] ドロップダウン リストをクリックします。

次の 2 つの展開オプションがあります。

- [Deploy]：サービス要求の状態が [Requested] または [Invalid] の場合、[Deploy] を使用します。
- [Force Deploy]：サービス要求の状態が [Deployed] または [Failed Audit] の場合は、[Force Deploy] を使用します。

ステップ 4　[Deploy] を選択します。

[Deploy Service Request] ダイアログボックスが表示され、選択されたサービス要求を展開するスケジュールの設定ができます。

ステップ 5　必要に応じて、このダイアログボックスのフィールドに入力して、サービス要求のスケジュールを設定します。

ステップ 6　スケジュール設定が終わったら、[Save] をクリックします。

[Service Request Manager] ウィンドウに戻ります。

ウィンドウの下部隅にあるポップアップ ウィンドウで [Status] の表示を確認します。サービス要求が正常に完了した場合、[Status] ディスプレイが表示され、[Succeeded] チェックボックスがオンになっています。

ステップ 7　[State] を [Requested] から [Deployed] に更新するには、[Auto Refresh] チェックボックスをオンにします。

（注）　ログを表示して、タスクのステータスとタスクが正常に完了したかどうかを確認します。ログの表示については、「ログの表示」（P.8-8）を参照してください。

サービス要求のモニタリング

展開中のサービス要求をモニタするには、タスク ログを使用する必要があります。タスク ログでは、サービス要求が失敗した理由のトラブルシューティングを実施したり、サービス要求の詳細を表示したりできます。

サービス要求をモニタするには、次のステップを実行します。

ステップ 1　[Operate] > [Tasks] > [Task Manager] を選択します。

[Task Logs] ウィンドウが表示されます。

ステップ 2　ウィンドウを更新するには、[Find] をクリックします。

Prime Provisioning で実行されているタスクのリストの中で、処理中のタスクが最初に表示されます。

ステップ 3　モニタするタスクを選択して、[Logs] をクリックします。

ステップ 4　モニタする実行中のタスクを選択して、[View Log] をクリックします。

ステップ 5　[Log Level] ドロップダウン リストからログ レベルを選択して、[Filter] をクリックします。

ログ レベルには、[All]、[Severe]、[Warning]、[Info]、[Config]、[Fine]、[Finer]、および [Finest] があります。

ステップ 6　[Return to Logs] をクリックします。

ステップ 7　[Task Logs] ウィンドウで [Close] をクリックします。

サービス要求のシミュレートされた展開

サービス要求を展開する場合、[Simulate deploy] オプションを使用することもできます。この機能を使用するには、まず、DCPL プロパティ **Services\Common\allowSimulateDeploy** を True に設定する必要があります。イネーブルにすると、標準の導入操作によって展開できるすべてのサービス要求（たとえば、[Requested] 状態から [Deployed] 状態にサービス要求を移行する操作）は、シミュレーション モードでも展開することもできます。シミュレートされた展開で、プロビジョニング フローはコンフィグレットがデバイスにダウンロードされる時点まで、通常どおり続行します。たとえば、ライブ設定はデバイスからアップロードされます。ただし、コンフィグレットをダウンロードするときに、Prime Provisioning はエコー モードであるかのように動作します（つまり、設定は実際のデバイスにダ

ウンロードされません）。実際に、これはサービス要求ベースごとにエコー モードです。標準およびシミュレートの両方で、エコー ベースの転送とライブ デバイス対話の組み合わせを使用し、複数の展開操作を同時に実行することができます。

サービス要求の展開をシミュレートするには、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 Requests Manager] ウィンドウが表示されます。

ステップ 2　展開するサービス要求のジョブ ID の横にあるチェックボックスをオンにします。

ステップ 3　[Deploy] ドロップダウン リストをクリックします。

DCPL プロパティ **Services\Common\allowSimulateDeploy** が True に設定されていると想定すると、次の 3 つの展開オプションを使用できます。

- Deploy
- Force Deploy
- Simulate Deploy

ステップ 4　[Simulate Deploy] を選択します。

[Deploy Service Request] ダイアログボックスが表示され、選択されたサービス要求の展開をシミュレーションするスケジュールの設定を行えるようになります。

ステップ 5　必要に応じて、このダイアログボックスのフィールドに入力して、サービス要求のスケジュールを設定します。

ステップ 6　スケジュール設定が終わったら、[Save] をクリックします。

[Service Request Manager] ウィンドウに戻ります。

ウィンドウの下部隅にあるポップアップ ウィンドウで [Status] の表示を確認します。サービス要求が正常に完了した場合、[Status] ディスプレイが表示され、[Succeeded] チェックボックスがオンになっています。

ステップ 7　[State] を [Requested] から [Deployed] に更新するには、[Auto Refresh] チェックボックスをオンにします。

（注）　ログを表示して、タスクのステータスとタスクが正常に完了したかどうかを確認します。ログの表示については、「ログの表示」（P.8-8）を参照してください。

サービス要求のデコミッション

サービス要求をデコミッションするには、次のステップを実行します。

ステップ 1　[Operate] > [Service Requests] > [Service Request Manager] を選択します。

ステップ 2　[Service Request Manager] ウィンドウで、デコミッションするサービス要求を選択して [Decommission] をクリックします。

[Confirm Decommission Service Request(s)] 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、サービス要求のデコミッションを確認します。

対応する [Operation Type] が [Delete] に変更された [Service Request Manager] ウィンドウが再び表示されます。

ステップ 4　サービス要求を選択して、[Deploy] > [Deploy] をクリックすることで、サービス要求を展開します。

この作業は、ネットワークに変更をプロビジョニングするために必要です。

ステップ 5　[Deploy Service Request] ウィンドウで、展開を実行する時間（デフォルトは即時）を選択して、[Save] をクリックします。

ステップ 6　展開後、サービス要求の状態が [Closed] に遷移したら、サービス要求のデコミッションが正常に完了したことを示しています。

サービス要求の削除

削除操作は、ネットワークに影響を与えずにリポジトリからサービス要求を削除するように設計されています。

サービス要求を削除するには、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 Request Manager] ウィンドウで、デコミッションするサービス要求を選択して [Delete] をクリックします。

ドロップダウン リストから、次のいずれかを選択します。

- [Delete]：通常の削除は、[Closed] 状態にあるサービス要求のみに使用できます。

  （注）　通常の削除は、TE Resource、TE Tunnel、TE Protection サービス要求には使用できません。これらのサービスはデコミッションできないためです。これらの 3 つのサービス要求タイプは、強制削除のみ可能です。

- [Force Purge]：強制削除では、リポジトリでサービス要求に対する必要な依存関係を検査してから削除が可能になります。したがって、サービス要求を削除できない場合は、エラー メッセージが出されます。

[Delete Service Request(s)] 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、削除または強制削除の操作を確認します。

サービス要求状態

サービス要求の遷移状態は、プロビジョニングのプロセスでサービス要求が遷移するさまざまな段階を示しています。たとえば、サービス要求を導入すると、Prime Provisioning はリポジトリ（Prime Provisioning データベース）内のデバイス情報を現在のデバイスのコンフィギュレーションと比較して、コンフィグレットを生成します。コンフィグレットが生成され、デバイスにダウンロードされると、サービス リクエストは [Pending] 状態になります。デバイスが監査されると、サービス要求は [Deployed] 状態に遷移します。

Prime Provisioning サービス要求は、複数のサービス要求が同一のデバイスを設定しようとしている場合を除き、並列に処理されます。この場合、サービス要求はシーケンシャルに処理されます（つまり、デバイスへの書き込みは一度に 1 つだけ実行されます）。

図 8-2 の「サービス要求状態遷移図」は、Prime Provisioning サービス要求の状態間の関係および移行に関する概要図を示しています。

図 8-2　サービス要求状態遷移図

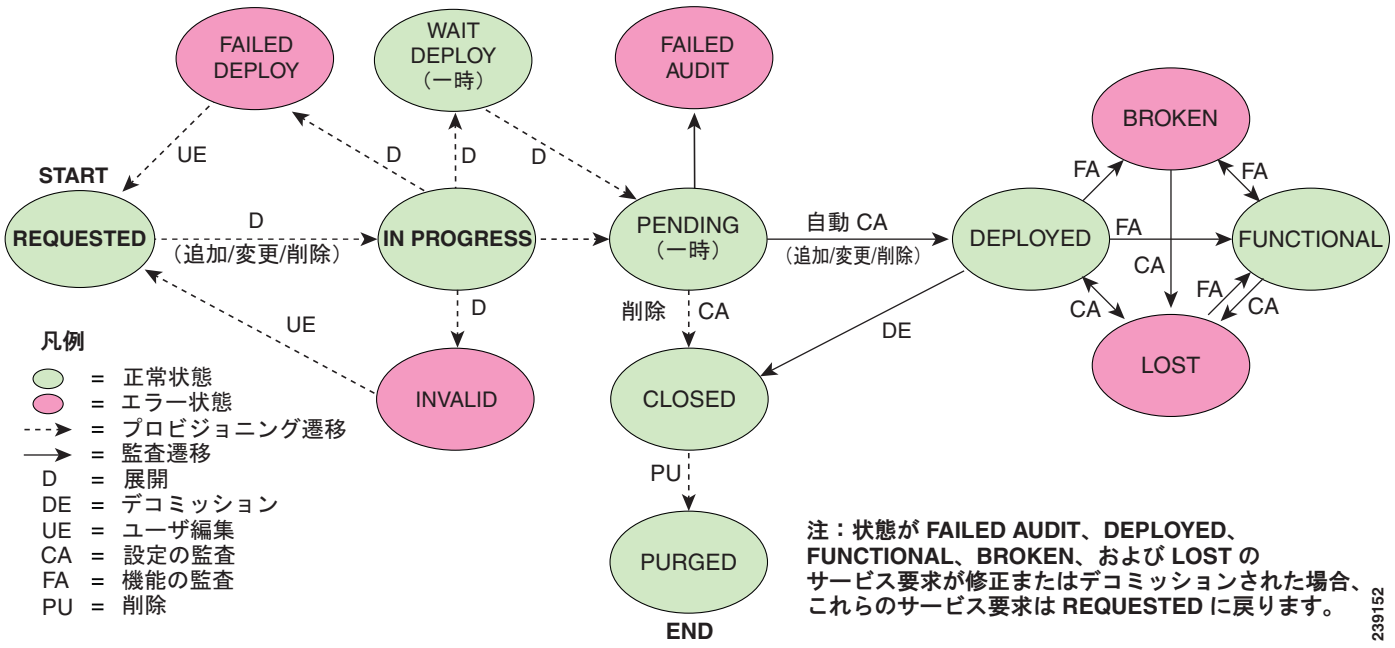


表 8-1 の「Prime Provisioning サービス要求状態の概要」は、Prime Provisioning サービス要求の状態ごとの機能を示しています。これらの機能は、アルファベット順に記載されています。

表 8-1　Prime Provisioning サービス要求状態の概要

サービス要求タイプ	説明
Broken （MPLS サービスの場合のみ有効）	ルータは正しく設定されていますが、サービスは利用できません（ケーブルの損傷やレイヤ 2 の問題などが原因）。 このサービスのルーティングおよび転送テーブルがオーディタによって検出され、サービスの目的と一致しない場合、MPLS サービス要求は [Broken] に移行します。
Closed	サービス要求がプロビジョニングまたは監査のプロセスで使用されなくなった場合、そのサービス要求は [Closed] に移行します。サービス要求は、サービス要求の中止の監査が正常に終了した場合のみ、[Closed] 状態に移行します。Prime Provisioning は、サービス要求をさらに監査できるように、データベースからサービス要求を削除しません。特定の管理者の削除操作のみによって、サービス要求を削除できます。

表 8-1　Prime Provisioning サービス要求状態の概要 （続き）

サービス要求タイプ	説明
Deployed	サービス要求の目的がルータのコンフィギュレーション ファイルに見つかった場合、サービス要求は [Deployed] に移行します。[Deployed] は、コンフィギュレーション ファイルがルータにダウンロードされ、リクエストの目的がコンフィギュレーション レベルで確認されたことを示します。つまり、Prime Provisioning がコンフィグレットをルータにダウンロードし、サービス要求が監査プロセスを通過したことを示します。
Failed Audit	この状態は、Prime Provisioning はルータにコンフィグレットを正常にダウンロードしたが、サービス要求が監査を通過しなかったことを示しています。そのため、サービスは [Deployed] 状態に移行しませんでした。[Failed Audit] 状態は、[Pending] 状態から開始されます。サービス要求は、正常に導入された後に再び [Failed Audit] 状態になることはありません（サービス要求が再導入された場合を除く）。
Failed Deploy	[Failed Deploy] 状態の原因は、（接続の切断、正しくないパスワードなどによる）初期コンフィギュレーション ファイルのルータからのアップロード失敗、またはコンフィギュレーション更新のルータへのダウンロード失敗のいずれかを DCS がレポートしていることです。
Functional （MPLS サービスの場合のみ有効）	このサービスの VPN Routing and Forwarding（VRF; VPN ルーティング / 転送）テーブルがオーディタによって検出され、サービスの目的と一致する場合、MPLS サービス要求は [Functional] に移行します。この状態は、コンフィギュレーション ファイル監査とルーティング監査が両方とも正常に完了している必要があります。
Invalid	[Invalid] は、サービス要求の情報が正しくないことを示します。リクエストがそれ自体矛盾している場合、または他の既存のネットワークやルータのコンフィギュレーションと不整合である場合（たとえば、ルータ上で使用できるインターフェイスがない場合など）、サービス要求は [Invalid] に移行します。プロビジョニング ドライバは、この要求に提供するコンフィギュレーション アップデートを生成できません。
Lost	オーディタがルータのコンフィギュレーション ファイル内でコンフィギュレーション レベルでの目的の確認を検出できなかった場合、サービス要求は [Lost] に移行します。サービス要求は [Deployed] 状態でしたが、一部または全部のルータのコンフィギュレーション情報が見つかりません。サービス要求が [Deployed] となっていた場合のみ、[Lost] 状態に移行する可能性があります。
Pending	プロビジョニング ドライバが、リクエストが一致していると見なし、このリクエストに必要なコンフィギュレーション更新を生成できた場合、サービス要求は [Pending] に移行します。[Pending] は、サービス要求がコンフィギュレーション更新を生成し、コンフィギュレーション更新がルータに正常にダウンロードされていることを示します。 保留中のサービス要求を新規の要求と見なして、監査が開始されます。サービスが新規にプロビジョニングされ、監査されていない場合は、エラーにはなりません（監査の保留）。ただし、監査が実行され、サービスが保留中のままである場合は、エラー状態です。
Requested	サービスが新規登録され、まだ展開されていない場合は、エラーにはなりません。ただし、[Deploy] が実行され、[Requested] のままである場合は、サービスはエラー状態です。

表 8-1　Prime Provisioning サービス要求状態の概要 （続き）

サービス要求タイプ	説明
In Progress	現在の状態に関係なく、展開にサービス要求が要求されるたびに、[In Progress] 状態が表示されます。[In Progress] 状態は、[Requested] および [Deployed] の中間の状態です。複数のサービス要求の展開が同時に要求されるたびに、すべてのサービス要求に対して [In Progress] 状態が表示されます。
Wait Deploy	このサービス要求状態は、Cisco Configuration Engine を使用してコンフィグレットをダウンロードしている場合のみに関連します。[Wait Deploy] は、コンフィグレットは生成されたが、デバイスが現在オンラインでないためダウンロードされていないことを示します。コンフィグレットは、Cisco Configuration Engine が Prime Provisioning にデバイスが稼働中であることを通知するまで、レポジトリに一時保管されます。[Wait Deploy] 状態のコンフィグレットが、デバイスにダウンロードされます。

表 8-2 の「Prime Provisioning サービス要求に対するユーザ操作」は、ユーザ操作と Prime Provisioning サービス要求に与える影響について示しています。

表 8-2　Prime Provisioning サービス要求に対するユーザ操作

ユーザ操作	説明
Decommission	このユーザ操作は、サービス要求のすべてのデバイスからサービスを削除します。
Force Deploy	このユーザ操作により、[Closed] を除くすべての状態からサービス要求を [Deploy] できます。これは、状態図の再起動と同等の操作です。サービス要求は、現在の状態からその他のあらゆる状態に移行できます。ただし、[Requested] 状態に移行することはありません。
Force Delete	このユーザ操作は、サービス要求の状態にかかわらず、データベースからサービス要求を削除します。サービス要求をデコミッションする前に Prime Provisioning リポジトリからサービス要求を強制削除（[Force Purge]）した場合、サービスはネットワーク上で稼働し続けたままになります（具体的には、サービスがプロビジョニングされたデバイス上にコンフィギュレーションは残ったままになります）。ただし、サービスを作成したサービス要求のすべてのレコードは Prime Provisioning から削除されます。
Delete	サービス要求が削除されると、Prime Provisioning データベースからサービス要求が削除されます。

CHAPTER 9

テンプレートおよびデータ ファイルの管理

この章では、Prime Provisioning でのテンプレートとデータ ファイルの使用について説明します。次の事項について説明します。

概要

テンプレートを使用すると、Prime Provisioning が通常はサポートしていないコマンドおよびコンフィギュレーションをデバイスに展開できます。テンプレートは Velocity Template Language（VTL）で記述され、通常は IOS および IOS XR デバイス CLI コンフィギュレーションで構成されます。

テンプレートは、テンプレート フォルダ、テンプレート、およびデータ ファイルの参照、作成、および削除をサポートしており、また、テンプレートにより生成されたコンフィギュレーションの表示をサポートしています。これは、IOS と IOS XR の両方に適用されます。IOS XR デバイスの場合、テンプレート データ ファイルから生成されるコンフィグレットは、XML コマンドではなく CLI コマンドです。

テンプレートおよびデータ ファイルから作成されるコンフィギュレーションを、デバイスにダウンロードできます。サービス要求の作成時、テンプレートおよびデータ ファイルのリストから選択を行い、選択対象をサービス要求に関連付けることができます。展開時、テンプレートおよびデータ ファイルはインスタンス化され、コンフィギュレーションが、Prime Provisioning により生成されるコンフィグレットの末尾または先頭に追加されます。もう 1 つの方法は、「テンプレートのダウンロード」（P.13-3）に説明されているように、[Device Console] 機能を使用してサービス要求とは関係なくテンプレートをダウンロードすることです。

Prime Provisioning には、テンプレートを Prime Provisioning コンフィグレットと統合する方法が用意されています。

特定のカスタマー エッジ ルータやプロバイダー エッジ ルータについて、次を指定します。

- テンプレート名

- テンプレート データ ファイル名
- テンプレート コンフィギュレーション ファイルを Prime Provisioning コンフィグレットの末尾に追加するか、または先頭に追加するか。
- テンプレート コンフィギュレーション ファイルを、エッジ デバイスへのダウンロードで、アクティブにするか、または非アクティブにするか。

テンプレート データ ファイルは、対応するテンプレートに緊密にリンクされます（データ ファイルは複数のテンプレートにリンクできません）。データ ファイルとそれに関連付けられているテンプレートを使用して、テンプレート コンフィギュレーション ファイルを作成できます。テンプレート コンフィギュレーション ファイルは、Prime Provisioning コンフィグレットにマージ（末尾または先頭に追加）されます。Prime Provisioning により、結合された Prime Provisioning コンフィグレットとテンプレート コンフィギュレーション ファイルがエッジ デバイス ルータにダウンロードされます。

- テンプレート コンフィギュレーション ファイルはルータにダウンロードできます。
- 同じテンプレートを複数のエッジ ルータに適用できます。各デバイスに対し適切なテンプレート データ ファイルが割り当てられます。各テンプレート データ ファイルには、特定デバイス用の専用データが含まれます（たとえば、各デバイスの管理 IP アドレスまたはホスト名）。

テンプレート コマンドは、サービス作成に関連付けられているコマンドとは独立して処理されます（Multi Protocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）、Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）、Virtual Private LAN Service（VPLS; 仮想プライベート LAN サービス）、トラフィック エンジニアリング（TE）など）。したがって、テンプレート コマンドは、サービス デコミッション時にデバイスから個別に削除する必要があります。先行するテンプレート コマンドを削除するには、個別のテンプレートがデコミッション プロセス時に必要になります。サービス要求をデコミッションしても、元のテンプレート コマンドは自動的に削除されません。個別の negate テンプレートをデコミッション プロセスに追加する必要があり、元のテンプレートを削除する必要があります。元のテンプレートで追加された任意の不要な IOS コマンドを正しく削除するには、必要な NO コマンドが negate テンプレートに含まれている必要があります。

テンプレート マネージャの機能の概要

この項では、Prime Provisioning でサポートされるテンプレートとデータ ファイルの主要な機能に焦点をあて、特に、ポリシーおよびサービス要求の処理に影響のある機能について説明します。

テンプレートの属性

Prime Provisioning テンプレートのメカニズムでは、テンプレートに次の属性を指定（任意）することによって複数のテンプレートを区別できます。

- デバイス タイプ
- ラインカード タイプ
- ポート タイプ
- ソフトウェア バージョン（IOS または IOS XR）

これらの属性は、テンプレート マネージャでテンプレートを設定するとき、ドロップダウン リストを通じて設定します。Prime Provisioning は、サービス要求内に定義されているデバイスに最も一致する、テンプレートまたはデータ ファイルをこの属性を使用して自動的に選択します。

ポリシー レベルでのテンプレートの関連付け

Prime Provisioning は、テンプレートおよびデータ ファイルのポリシーでの関連付けをサポートしています。

U-PE および PE-AGG デバイス ロール用テンプレートの選択的決定

Prime Provisioning の柔軟性が強化されたことから、ユーザは、デバイスに UNI インターフェイスがあるかどうかに応じて、（リング環境などで）U-PE および PE-AGG のデバイスにテンプレートを選択的に適用できます。

拡張サブテンプレートのサポート

テンプレート エディタで新しい属性を使用することで、サブテンプレートをテンプレートに関連付けることができます。Prime Provisioning では、デバイスの属性に基づく動的なインスタンス化をサポートしています。サブテンプレートを作成するとき、オペレータは、これらの識別子の値を指定する必要があります。

データ ファイルの動的作成

ユーザは、サービス要求作成時にデータ ファイルを作成し、それを関連するポリシーからコピーされたテンプレートに関連付けることができます。この機能により、テンプレート ウィザードからのデータ ファイル作成が拡張され、サービス要求ウィザードの [Template Association] 画面から直接データ ファイルを作成できます。さらに、サービス要求に関連付けられているテンプレートおよびデータ ファイルに含まれる任意またはすべての変数を変更し、更新されたテンプレートおよびデータ ファイルを、サービス全体を削除せずに適用できます。

negate テンプレートの自動適用

テンプレートおよびデータ ファイルから作成されたコンフィギュレーションを削除するには、negate テンプレートを既存のサービスに適用する必要があります。現在、この操作は Prime Provisioning で自動化されています。positive テンプレートと negate テンプレートの両方を作成します。positive テンプレートおよびデータ ファイルをポリシーに割り当てることができます。negate テンプレートは deploy テンプレートに直接関連付けられるため、Prime Provisioning は、適切なときに適切な negate テンプレートを呼び出します。Prime Provisioning は、要求されたサービス要求のアクション（サービスの導入または中止など）に基づいて、どの negate テンプレートを使用するかを判別します。negate テンプレートの名前はテンプレートと同じで、サフィクスとして .Negate が付加されます。negate テンプレートは、deploy テンプレートのデータ ファイルを共有しません。negate テンプレートには、専用のデータ ファイルを定義する必要があります。

テンプレート メカニズムと Prime Provisioning の前のリリースとの互換性

Prime Provisioning は、テンプレート メカニズムの互換性を以前の Prime Provisioning のリリースとの間で維持しています。Prime Provisioning の前のバージョンで作成されたテンプレートは、テンプレートやワークフローを変更せずに「そのまま」使用できます。前のリリースの Prime Provisioning システムで作成されたポリシーの場合、テンプレートおよびデータ ファイルの関連付けを行う GUI ワークフローは表示されません。このような場合、Prime Provisioning の前のリリース同様、オペレータがサービスの導入中にテンプレートとデータ ファイルを追加します。

IOS および IOS XR のテンプレート サポート

テンプレート メカニズムは、IOS デバイスと IOS XR デバイスの両方に対してサポートされます。IOS XR デバイスの場合、テンプレートおよびデータ ファイルから生成されるコンフィグレットには、XML ステートメントではなく CLI コマンドが含まれます。IOS XR デバイスの場合、テンプレート サポートは CLI コマンドとして提供されます。IOS デバイスの場合、オペレータは、Device Console を使用してテンプレート コンフィグレットをダウンロードできます。

（注）　IOS XR デバイスの場合、次の既知の問題に注意してください。不適切なコンフィギュレーションまたはサポートされていないコンフィギュレーションを含むテンプレートを使用してサービス要求が展開された場合でも、サービス要求は [DEPLOYED] 状態になります。これは、IOS XR デバイスが、不適切なコンフィギュレーションの展開に関するエラー レポートを発行しないためです。

テンプレート使用に関する RBAC サポート

適切な RBAC ロールを持つユーザのみ、テンプレートおよびデータ ファイルにアクセスできます。データ ファイルの権限タイプは追加済みです。データ ファイルについて付与される権限は、表示、作成、変更、および削除です。オペレータは、他のロールに割り当てられているテンプレートおよびデータ ファイルを表示できません。また、アクセス権のないテンプレートおよびデータ ファイルは展開できません。

テンプレート変数

テンプレート型変数は、MPLS、L2VPN、VPLS、および FlexUNI/EVC のほとんどの Prime Provisioning リポジトリ変数をサポートします。サポートされるテンプレート変数の一覧については、「リポジトリ変数の概要」（P.9-35）を参照してください。

DCPL プロパティ

テンプレートを制御する複数の Dynamic Component Properties Library（DCPL）プロパティがあります。これらの DCPL プロパティは、テンプレートの適用時に、negate テンプレートが後ろまたは前に追加されるか、また、サービスが複数行あり、1 行だけが編集されたときにテンプレートが適用されるかどうか、などに影響します。テンプレートに関連する DPLC プロパティの資料は、次を参照してください。Appendix B, “Property Settings.”

テンプレートのインポートとエクスポート

Prime Provisioning は、テンプレートおよびデータ ファイルをインポートおよびエクスポートするメカニズムを提供しています。詳細については、「サンプル テンプレート」（P.9-34）を参照してください。

テンプレートおよびデータ ファイルのワークフロー

この項では、テンプレート、データ ファイル、negate テンプレートの設定および使用に関する Prime Provisioning の基本操作の概要を示します。

テンプレート マネージャの基本機能

- 各種コンフィギュレーション用のテンプレートおよび negate テンプレートを作成する機能。
- テンプレートのデバイス属性を指定する機能。
- 適用可能な場合、サブテンプレートをテンプレートに関連付ける機能。
- サブテンプレートのデータ ファイルを作成する機能。
- 各サブテンプレートに対し negate テンプレートを作成する機能。
- negate テンプレートのデータ ファイルを作成する機能。
- スーパー テンプレートを作成し、それにサブテンプレートを関連付ける機能。

これらの基本的な Template Manager の機能は、この章の他の項で説明されています。

ポリシー レベルのテンプレート機能

- ポリシーを作成し、ポリシーのテンプレート サポートをイネーブルにする機能。
- 必要に応じて、テンプレートおよび（オプションの）データ ファイルをポリシーに関連付ける機能。

ポリシー レベルでテンプレートおよびデータ ファイルを関連付ける方法の詳細については、この章の「ポリシーでのテンプレートの使用」（P.9-22）の項を参照してください。

サービス要求レベルのテンプレート機能

（注）　テンプレートにデータ ファイルが 1 つのみある場合で、ポリシーがテンプレートのみに関連付けられていて、データ ファイルには関連付けられていない場合、そのポリシーを使用したサービス要求の作成時に、そのテンプレートのデータ ファイルが自動的に選択されます。テンプレートにデータ ファイルがない場合、保存前に、そのテンプレートに対して 1 つのデータ ファイルを作成する必要があり、それをサービス要求に関連付ける必要があります。

- サービス要求を作成し、テンプレートをリンクに関連付ける機能。
- サービス要求をデバイス（たとえば、7600）に展開する機能。
- 7600 用のサブテンプレートおよび対応するデータ ファイルは、展開時に自動的に選択されます。
- コンフィグレットがサブテンプレートから生成されます。
- サービス要求をデコミッションします。
- サブテンプレートの negate テンプレートが自動的に選択され展開されます。

サービス要求でテンプレートおよびデータ ファイルを使用する方法の詳細については、この項の「サービス要求ワークフローでのテンプレートおよびデータ ファイルの使用」（P.9-30）を参照してください。

基本テンプレートおよびデータ ファイル タスク

この項では、テンプレートとデータ ファイルで実行できる基本的なタスクについて説明します。次の作業を行います。

テンプレート ツリーとデータ ペインの表示

テンプレートを使用するには、次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。図 9-1 に示されているウィンドウが表示されます。

図 9-1　　Templates Manager

テンプレートのツリーが、左のカラムにあります。最後の階層の情報に到達するまで、作成済みの各フォルダおよびサブフォルダの横の**矢印**記号を続けてクリックできます。最後に使用可能なレベルはテンプレート名です。データ ファイルの情報は、ツリーには保持されません。

ウィンドウの右側はデータ ペインです。フォルダまたはテンプレートの名前が左上隅に表示されます。テンプレートまたはデータ ファイル情報の横のチェックボックスをオンにすると、以降の項で説明する [Create Template]、[Create Data File]、[Edit]、または [Delete] ボタンがイネーブルになります。

フォルダに多数のテンプレートがあるか、テンプレートに多数のデータ ファイルがある場合、データ ペインの右上隅にある [Show Templates matching] または [Show Data Files matching] フィルタを使用すると非常に便利です。たとえば、[Show Templates] または [Show Data Files] のドロップダウン リストをクリックし、**名前**または**説明**とのマッチングを選択し（マッチングでは、大文字と小文字が区別されます）、その後、[matching] ボックスで、**abc** で始まるテンプレートまたはデータ ファイルの処理を選択できます。この場合、フィールドに **abc*** を入力し、[Show] ボタンをクリックします。これにより、**abc** で始まるテンプレートまたはデータ ファイルのみ表示されます。フィルタの詳細については、「フィルタ」（P.1-5）を参照してください。

（注） テンプレート検索機能は、すべてのフォルダではなく、現在選択されているフォルダに適用されます。

（注） データ ファイル検索は、すべてのフォルダおよびテンプレートではなく、現在選択されているテンプレートに適用されます。

表にデータ ファイルが表示されるとき、コンフィギュレーションも表示できます。

ステップ 2　後の項で説明されているように、テンプレートおよびデータ ファイルを使用する基本的なタスクの実行を開始できます。

フォルダおよびサブフォルダの作成

新しいフォルダまたはサブフォルダを作成するには、次の手順を実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　[Template Manager] ツリーで、空白領域を右クリックし、[New] > [Folder] を選択して新しいフォルダを作成するか、既存のフォルダまたはサブフォルダを右クリックし、[New] > [Folder] を選択してサブフォルダを作成します。

（注） 作成できるサブフォルダとフォルダのレベル数に制限はありません。

ステップ 3　[Template Manager] ツリーに表示される新しいテキスト フィールドに、新しいフォルダまたはサブフォルダの名前を入力します。

フォルダまたはサブフォルダのコピー

フォルダまたはサブフォルダをコピーし、別のフォルダまたはサブフォルダ内に貼り付けるには、次のステップを実行します。

ステップ 1　フォルダまたはサブフォルダを選択し、右クリックしてコピー項目を表示します。[Copy] をクリックします。

ステップ 2　コピーしたフォルダまたはサブフォルダとそのすべての内容を貼り付ける先のフォルダまたはサブフォルダを右クリックし、[Paste] をクリックします。

選択した場所に、新しいフォルダまたはサブフォルダとそのすべての内容が表示されます。ここから編集を行うことができます。

テンプレートの作成

既存のフォルダ内に新しいテンプレートを作成すること、または新しいフォルダを作成し、その後テンプレートを作成できます。新しいフォルダを作成するには、「フォルダおよびサブフォルダの作成」の項を参照してください。

新しいテンプレートを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　[Template Manager] ツリーで、新しいテンプレートを作成する先のフォルダをクリックします。

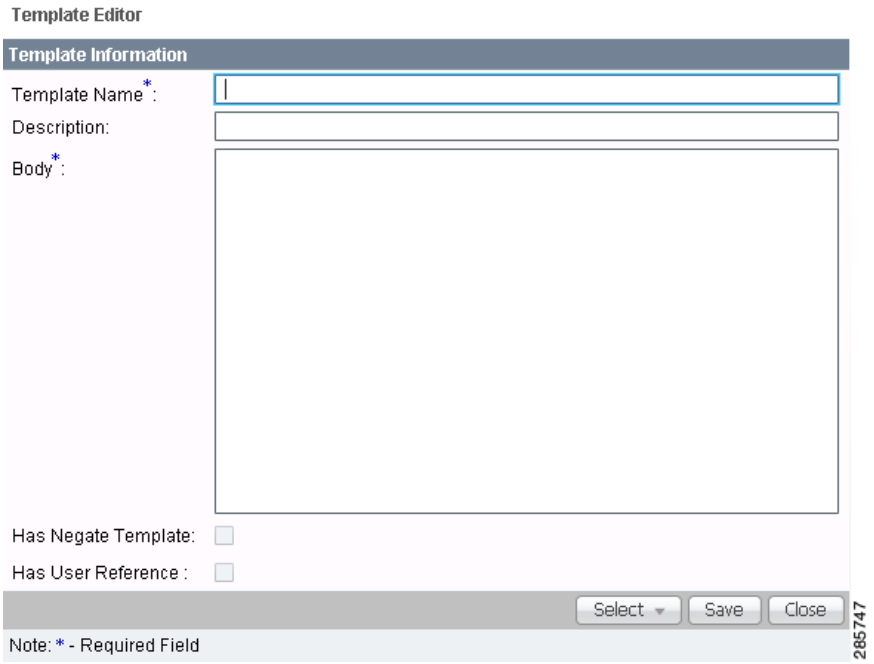
図 9-2 に示されているウィンドウが表示されます。

図 9-2　既存のテンプレートを含むフォルダ

ステップ 3　[Show Templates] ドロップダウン リストを使用して、テンプレートを**名前**順と**説明**順のどちらで表示するか選択できます（どちらの場合もアルファベット順に並べ替えられます）。次に、[Show] ボタンをクリックして、テンプレートの表示方法をアクティブにします。[Show] ボタンをクリックする前に [matching] フィールドに文字を入力すると、**名前**順または**説明**順に表示されるテンプレートのリストを最小にできます。詳細については、「テンプレート ツリーとデータ ペインの表示」（P.9-5）を参照してください。

ステップ 4　[Create Template] ボタンをクリックします。これにより、図 9-3 に示されているウィンドウが表示されます。

図 9-3　Template Editor



ステップ 5　次を入力します。

- [Template Name]（必須）：この名前は、フォルダ内で一意である必要があります。この名前は英数字で開始する必要があり、英数字、下線、およびハイフンのみ含めることができます。
- [Description]（任意）：ここに説明を入力できます。
- [Body]（必須）：組み込む必要のあるコンフィギュレーション テキスト、Velocity Template Language（VTL）ディレクティブ、および変数を入力します。

（注）　VTL は、テンプレートの記述に使用されるマークアップ言語です。VTL の説明は http://velocity.apache.org にあります。詳細については、http://velocity.apache.org/engine/devel/user-guide.html または http://velocity.apache.org/engine/devel/vtl-reference-guide.html を参照してください。

ステップ 6　[Select] ドロップダウン リストをクリックし、次の項目の中から選択します。

- 「negate テンプレート」（P.9-9）
- 「ユーザ セクション」（P.9-10）
- 「オプション属性」（P.9-10）
- 「サブテンプレート」（P.9-12）
- 「変数」（P.9-13）
- 「検証」（P.9-17）

これらの作業については、以降のサブセクションで説明します。

negate テンプレート

テンプレートまたはデータ ファイルから作成されたコンフィギュレーションを削除するには、**Negate** を既存のサービスに適用する必要があります。negate テンプレートは、<*TemplateName*>**.Negate** という形式で、元のテンプレートと同じフォルダ内に保存されます。テンプレートを削除すると、negate テンプレートも削除されます。negate テンプレートを個別に削除することもできます。データ ファイルを negate テンプレートに対し関連付けることができます。

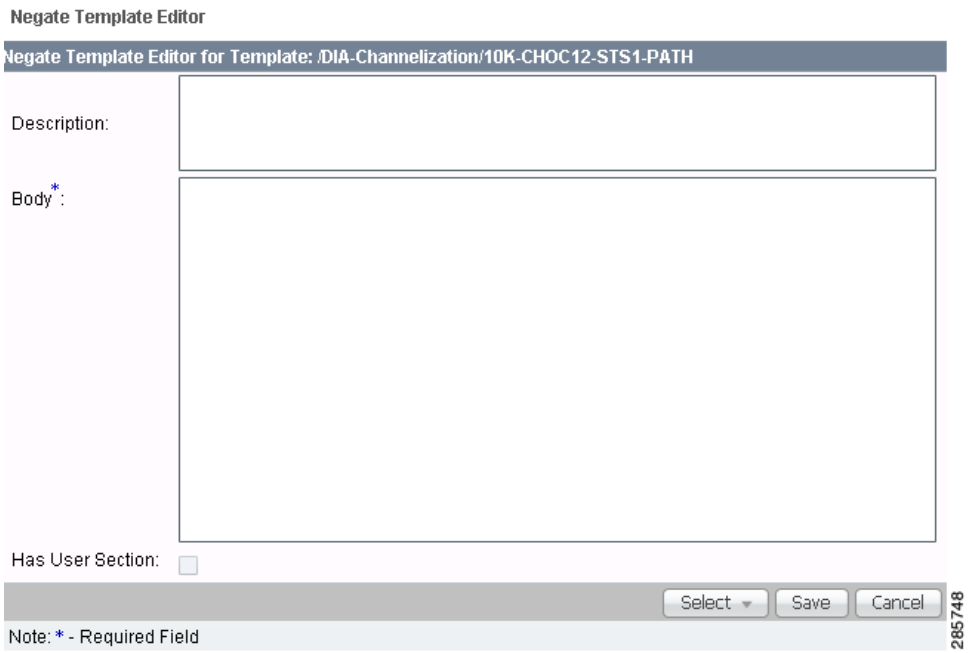
サービス ポリシーおよびサービス要求でテンプレートを関連付けると、negate テンプレートも自動的に関連付けられます（*『Cisco Prime Provisioning 6.3 User Guide』* を参照）。

デコミッション時に、negate テンプレートが展開のために使用されます。テンプレートを変更すると、negate テンプレートも、新しく選択したテンプレートの negate テンプレートに自動的に変更されます。

「テンプレートの作成」の項のステップ 6 で [Select] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[Negate] を選択し、[Go] ボタンをクリックします。図 9-4 に示されているウィンドウが表示されます。

図 9-4　Negate Template Editor



ステップ 2　（任意）[Description] に negate テンプレートの名前を追加します。

ステップ 3　必須の本文ブロックにテンプレート情報を入力します。テンプレートの行に対応する、各行の情報の前に **no** を入力して否定であることを示します。

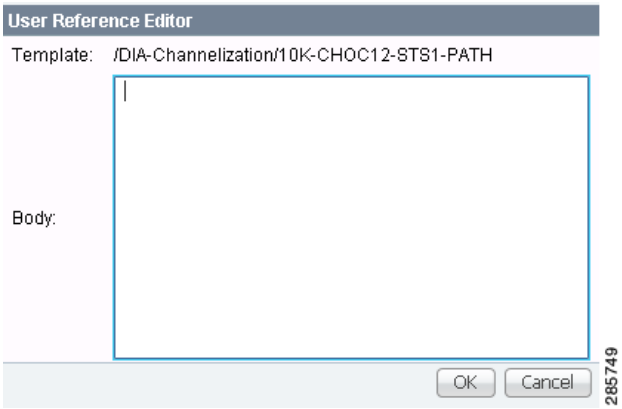
ユーザ セクション

[User Reference] を使用することで、当該テンプレートに関する情報を保持できます。

「テンプレートの作成」の項のステップ 6 で [Select] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[User Reference] を選択し、[Go] ボタンをクリックします。図 9-5 に示されているウィンドウが表示されます。

図 9-5　User Reference Editor



ステップ 2　図 9-5 で、使用可能なフィールドである、[Template] および [Body] に情報を追加できます。

ステップ 3　[OK] ボタンをクリックすると、図 9-3 で情報が更新されます。[Cancel] をクリックすると、更新は行われずに、図 9-3 に戻ります。

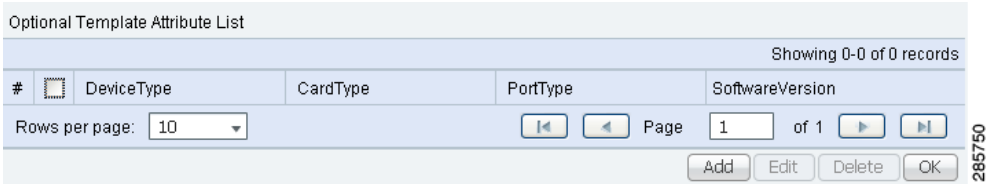
オプション属性

[Optional Attributes] を選択すると、Prime Provisioning リポジトリから読み込まれた定義済みの [Device Type]、[Card Type]、[Port Type]、および [Software Version]（IOS および IOS XR）を表示できます。4 つのカテゴリで属性値が指定されていない場合、属性はそのタイプのすべての対象に対して適用されます。たとえば、[Port Type] のドロップダウン リストに選択肢がない場合、すべてのポート タイプに対して属性値が適用されます。属性の各組み合わせは一致している必要があります。属性の各組み合わせを属性セットと呼びます。テンプレートには、複数の属性を含めることができます。たとえば、テンプレートを 7600 シリーズと 3500 シリーズに適用できます。

「テンプレートの作成」の項のステップ 6 で [Select] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[Optional Attributes] を選択し、[Go] ボタンをクリックします。図 9-6 に示されているウィンドウが表示されます。

図 9-6　Optional Template Attribute List



ステップ 2　Prime Provisioning リポジトリから読み込まれた定義済みの [Device Type]、[Card Type]、[Port Type]、および [Software Version]（IOS および IOS XR）を表示できます。4 つのカテゴリで属性値が指定されていない場合、属性はそのタイプのすべての対象に対して適用されます。テンプレートには複数の属性を設定できます。ロールに基づいた異なるテンプレートを作成し、それらをポリシーおよびサービス要求に関連付ける必要があります（*『Cisco Prime Provisioning 6.3 User Guide』* を参照）。

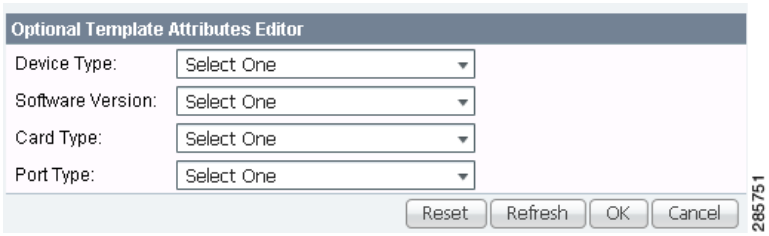
ステップ 3　以下を実行する対象の属性セット（情報の行）のチェックボックスをオンにします（[Add] は除きます。この場合、チェックボックスをオンにする必要はありません）。

- 属性を追加するためのオプション属性エディタを開くには、[Add] ボタンをクリックします。属性セットを追加すると、属性リスト ページに反映されます。
- 属性を変更するためのオプション テンプレート属性エディタを開くには、[Edit] ボタンをクリックします。1 つのプロセスで複数の編集を行うことはできません。
- 選択した属性を削除するには、[Delete] ボタンをクリックします。選択した複数の属性を一度に削除できます。
- ウィンドウを閉じ、前のページに戻るには、[OK] ボタンをクリックします。

ステップ 4　[Add] または [Edit] ボタンをクリックするとポップアップ ウィンドウが表示され、そこで、図 9-7 に示されているようにオプションの識別子を入力できます。

（注）　[Edit] ボタンをクリックする前に、図 9-6 で、編集する 1 つの属性セット（情報の行）のチェックボックスをオンにする必要があります。一度に複数の行は編集できません。

図 9-7　Optional Template Attributes Editor



ステップ 5　図 9-7 で、[Device Type]、[Software Version]、[Card Type]、および [Port Type] のそれぞれのドロップダウン リストをクリックします。

（注）　ドロップダウン リストは、前の属性の選択に基づき適切にフィルタリングされます。たとえば、[Device Type] で 7600 を選択した場合、[Card Type] の選択肢は 7600 に関連した選択肢になります。

ステップ 6　次のいずれかのボタンをクリックします。

- [Reset]：この選択プロセスをやり直すことができます。
- [Refresh]：データベースおよびユーザ定義ファイルのオプション リストを更新します。ユーザ定義属性は、**usertemplateattr.xml** ファイルから読み込まれます。

（注）　ユーザ定義属性ファイルの名前である **usertemplateattr.xml** は、DCPL プロパティの **TemplateManger\userTemplateAttrFile** を使用して変更できます（詳細については、Appendix B, “Property Settings” を参照してください）。

（注）　[Refresh] プロセスは時間がかかる場合があります。この点に注意してください。

- [OK]：選択したテンプレート属性を受け入れ、セットとしてそれらを追加し、属性セット（情報の行）が追加された、更新済みの図 9-6 に戻ります。
- [Cancel]：変更せずに前のウィンドウに戻ります。

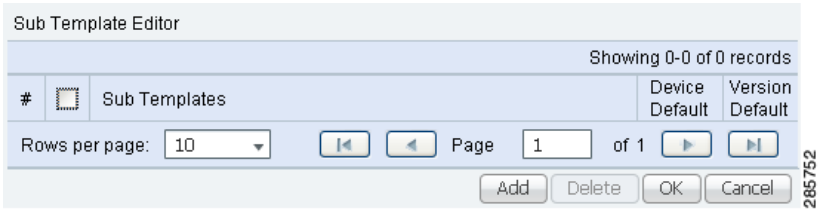
サブテンプレート

他のテンプレートを使用するテンプレートをスーパー テンプレートと呼びます。使用されるテンプレートをサブテンプレートと呼びます。スーパー テンプレートは、変数の値をサブテンプレートに渡すことで、必要なすべてのサブテンプレートをインスタンス化します。インスタンス化後、スーパー テンプレートは、サブテンプレートが生成したコンフィグレットをスーパー テンプレート内に配置します。

「テンプレートの作成」の項のステップ 6 で [Select] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[Sub-Template] を選択し、[Go] ボタンをクリックします。図 9-8 に示されているウィンドウが表示されます。

図 9-8　Sub Template Editor



ステップ 2　以下を実行する対象のサブテンプレート（情報の行）のチェックボックスをオンにします（[Add] は除きます。この場合、チェックボックスをオンにする必要はありません）。

- 新しい行を追加するには、[Add] ボタンをクリックします。次に、[Sub Templates] 列の下で、[Add link] をクリックします。新しいサブテンプレートを選択できる、新しいポップアップが表示されます。デフォルトでは、チェックボックスはオフです。[OK] ボタンをクリックして保存するまで、変更は保存されません。

- 選択した行を削除するには、[Delete] ボタンをクリックします。選択した複数の行を一度に削除できます。[OK] ボタンをクリックして保存するまで、変更は保存されません。
- フォームのすべての変更を保存するには、[OK] ボタンをクリックすると、ウィンドウが閉じ、前のページに戻ります。
- すべての変更を廃棄するには、[Cancel] ボタンをクリックします。ウィンドウが閉じ、前のページに戻ります。

ステップ 3　サブテンプレートをスーパー テンプレートに関連付けることができます。サービス プロビジョニング時にテンプレートがインスタンス化されると（*『Cisco Prime Provisioning 6.3 User Guide』* を参照）、デバイス、ラインカード、ロール、ポート、およびデバイス ソフトウェア バージョンに関する実行時情報に基づき、適切なサブテンプレートが使用されます。属性に基づく展開時に、ユーザが指定した適切なサブテンプレート属性がインスタンス化されます。次の点に注意してください。

- サブテンプレートの階層は 1 階層のみサポートされていますが、サブテンプレートの深度はチェックされません。
- スーパー テンプレートとサブテンプレートの構造が円環になっているかどうかチェックするための検証は実行されません。
- スーパー テンプレートが参照するサブテンプレートを削除しようとすると、警告メッセージが表示されます。サブテンプレートは変更できます。
- サブテンプレートは、複数のスーパー テンプレートに関連付けることができます。
- サブテンプレートでは、データ ファイルはサポートされません。複数のデータ ファイルが検出された場合、展開時のアルファベット順のソートに基づき、最初に検出されたデータ ファイルが選択されます。

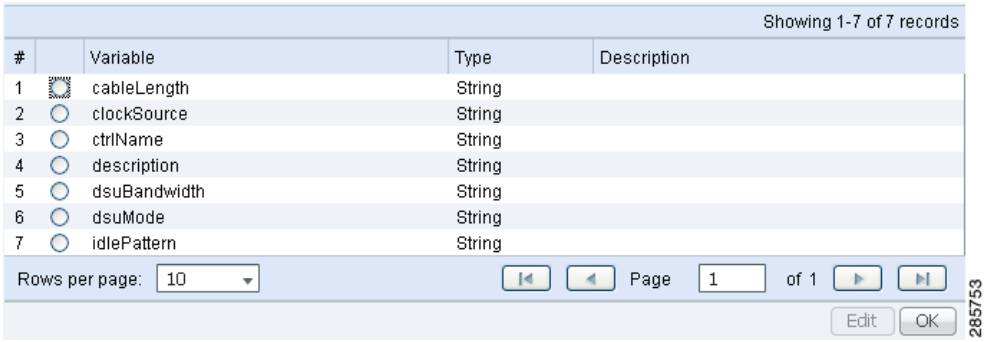
ステップ 4　サブテンプレートをデフォルトとしてマークできます。デバイス タイプおよびソフトウェア バージョン属性タイプについてはデフォルトがあります。テンプレートに対し属性がマークされていない場合、そのテンプレートはデフォルト テンプレートとして扱われます。これらのテンプレートの優先順位は、属性タイプのデフォルト サブテンプレートよりも低くなります。複数のサブテンプレートで属性がマークされていない場合、サブテンプレートは選択されません。サブテンプレートの使用方法の詳細については、「サービス プロビジョニング時のサブテンプレートの関連付け」（P.9-26）を参照してください。

変数

「テンプレートの作成」の項のステップ 6 で [Select] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[Variables] を選択し、[Go] ボタンをクリックします。図 9-9 に示されているウィンドウが表示されます。

図 9-9　テンプレート変数



ステップ 2　編集する変数のオプション ボタンをクリックし、[Edit] をクリックします。

[Variable Definition] ウィンドウが表示されます。

ステップ 3　[Type] のドロップダウン リストをクリックして、次の選択肢を表示します。

- [String]：ステップ 4 に進みます。
- [Integer]：ステップ 5 に進みます。
- [Float]：ステップ 6 に進みます。
- [IPv4 Address]：ステップ 7 に進みます。
- [Sub-Template]：ステップ 8 に進みます。

ステップ 4　表示されるデフォルトの型は [String]（グループと見なされる ASCII 文字の組み合わせ）です。これを選択すると、文字列型用の [Variable Definition] ウィンドウが表示されます。この型の変数の属性を次に示します。

- [Description]（任意）：この変数に関する説明文をここに入力できます。
- [Required]：この変数が必須の場合は、チェックボックスをデフォルトのオンの状態のままにします。それ以外の場合は、オフにします。
- [Dimension]：[0]（デフォルト）を選択すると、スカラ変数または列挙変数が指定されます。[1] を選択すると、変数は 1 次元配列になります。[2] を選択すると、変数は 2 次元配列になります。
- [Pattern]（任意）：文字列の正規表現パターンを指定します。たとえば、**isc[0-9]+** というパターンでは、先頭が **isc** で、その後に **0** ～ **9** までの 1 つ以上の数字が続く文字列が定義されます。
- [Minimum Length]（任意）：最小長を指定した場合、ここで指定した長さ未満の文字列は使用できなくなります。
- [Maximum Length]（任意）：最大長を指定した場合、ここで指定した長さを超えた文字列は使用できなくなります。
- [Default] オプション ボタン（任意）：指定した変数のデフォルト値がある場合、ここで指定します。
- [Available Values] オプション ボタン（任意）：この変数の文字列値を入力します。カンマで値を区切ります。

すべてのデータを入力した後、[OK] をクリックして、指定した変数の当該情報を受け入れます。または、引き続き、この同じ方法で変更する必要のあるすべての変数を編集し、図 9-9 などのウィンドウで [OK] をクリックします。これにより、これらの更新された変数が組み込まれます。または、[Save] をクリックして [Close] をクリックするか、[Close] をクリックして、図 9-3 などのウィンドウで保存を

要求されたら、[Save] に同意します。[Create a Data File] は「データ ファイルの作成」（P.9-17）に示され、[Edit] は「テンプレートおよびデータ ファイルの編集」（P.9-19）に示され、[Delete] は「テンプレートおよびデータ ファイルの削除」（P.9-20）に示されています。

ステップ 5　[Integer] 型を選択した場合、整数型用の [Variable Definition] ウィンドウが表示されます。この型の変数の属性を次に示します。

- [Description]（任意）：この変数に関する説明文をここに入力できます。
- [Required]：この変数が必須の場合は、チェックボックスをデフォルトのオンの状態のままにします。それ以外の場合は、オフにします。
- [Dimension]：[0]（デフォルト）を選択すると、スカラ変数または列挙変数が指定されます。[1] を選択すると、変数は 1 次元配列になります。[2] を選択すると、変数は 2 次元配列になります。
- [Minimum Value]（任意）：最小値を指定した場合、ここで指定した値未満の整数は使用できなくなります。
- [Maximum Value]（任意）：最大値を指定した場合、ここで指定した値を超える整数は使用できなくなります。
- [Default] オプション ボタン（任意）：指定した変数のデフォルト値がある場合、オプション ボタンの後のフィールド内に指定します。
- [Available Values] オプション ボタン（任意）：オプション ボタンの後のフィールド内に、この変数の文字列値を入力します。カンマで値を区切ります。

すべてのデータを入力した後、[OK] をクリックして、指定した変数の当該情報を受け入れます。または、引き続き、この同じ方法で変更する必要のあるすべての変数を編集し、図 9-9 などのウィンドウで [OK] をクリックします。これにより、これらの更新された変数が組み込まれます。または、[Save] をクリックして [Close] をクリックするか、[Close] をクリックして、図 9-3 などのウィンドウで保存を要求されたら、[Save] に同意します。[Create a Data File] は「データ ファイルの作成」（P.9-17）に示され、[Edit] は「テンプレートおよびデータ ファイルの編集」（P.9-19）に示され、[Delete] は「テンプレートおよびデータ ファイルの削除」（P.9-20）に示されています。

ステップ 6　[Float] 型、つまり、小数点の前後の桁数が固定されていない数値型を選択した場合、浮動小数点型用の [Variable Definition] ウィンドウが表示されます。この型の変数の属性を次に示します。

- [Description]（任意）：この変数に関する説明文をここに入力できます。
- [Required]：この変数が必須の場合は、チェックボックスをデフォルトのオンの状態のままにします。それ以外の場合は、オフにします。
- [Dimension]：[0]（デフォルト）を選択すると、スカラ変数または列挙変数が指定されます。[1] を選択すると、変数は 1 次元配列になります。[2] を選択すると、変数は 2 次元配列になります。
- [Minimum Value]（任意）：最小値を指定した場合、ここで指定した値未満の浮動小数点値は使用できなくなります。
- [Maximum Value]（任意）：最大値を指定した場合、ここで指定した値を超える浮動小数点値は使用できなくなります。
- [Default] オプション ボタン（任意）：指定した変数のデフォルト値がある場合、ここで指定します。
- [Available Values] オプション ボタン（任意）：この変数の文字列値を入力します。カンマで値を区切ります。

すべてのデータを入力した後、[OK] をクリックして、指定した変数の当該情報を受け入れます。または、引き続き、この同じ方法で変更する必要のあるすべての変数を編集し、図 9-9 などのウィンドウで [OK] をクリックします。これにより、これらの更新された変数が組み込まれます。または、[Save] をクリックして [Close] をクリックするか、[Close] をクリックして、図 9-3 などのウィンドウで保存を

要求されたら、[Save] に同意します。[Create a Data File] は「データ ファイルの作成」（P.9-17）に示され、[Edit] は「テンプレートおよびデータ ファイルの編集」（P.9-19）に示され、[Delete] は「テンプレートおよびデータ ファイルの削除」（P.9-20）に示されています。

ステップ 7　[IPv4 Address] 型を選択した場合、IPv4 アドレス型用の [Variable Definition] ウィンドウが表示されます。この型の変数の属性を次に示します。

- [Description]（任意）：この変数に関する説明文をここに入力できます。
- [Required]：この変数が必須の場合は、チェックボックスをデフォルトのオンの状態のままにします。それ以外の場合は、オフにします。
- [Dimension]：[0]（デフォルト）を選択すると、スカラ変数または列挙変数が指定されます。[1] を選択すると、変数は 1 次元配列になります。[2] を選択すると、変数は 2 次元配列になります。
- [Subnet Mask]（任意）：有効なサブネット マスクを入力します。
- [Class]（任意）：IP アドレスのクラスを入力します。選択肢は、[Undefined]、[A]、[B]、または [C] です。
- [Default] オプション ボタン（任意）：指定した変数のデフォルト値がある場合、ここで指定します。
- [Available Values] オプション ボタン（任意）：この変数の文字列値を入力します。カンマで値を区切ります。

すべてのデータを入力した後、[OK] をクリックして、指定した変数の当該情報を受け入れます。または、引き続き、この同じ方法で変更する必要のあるすべての変数を編集し、図 9-9 などのウィンドウで [OK] をクリックします。これにより、これらの更新された変数が組み込まれます。または、[Save] をクリックして [Close] をクリックするか、[Close] をクリックして、図 9-3 などのウィンドウで保存を要求されたら、[Save] に同意します。[Create a Data File] は「データ ファイルの作成」（P.9-17）に示され、[Edit] は「テンプレートおよびデータ ファイルの編集」（P.9-19）に示され、[Delete] は「テンプレートおよびデータ ファイルの削除」（P.9-20）に示されています。

ステップ 8　[Sub-Template] 型を選択した場合、メイン テンプレートに対して 1 つのサブテンプレートがインスタンス化されます。サブテンプレート型用の [Variable Definition] ウィンドウが表示されます。この型の変数の属性は次のようになります。

- [Description]（任意）：この変数に関する説明文をここに入力できます。
- [Required]：この変数が必須の場合は、チェックボックスをデフォルトのオンの状態のままにします。それ以外の場合は、オフにします。
- [Location]（必須）：親テンプレートのフル パス名を入力します。たとえば、**/test2/testyy** などです。

（[Variables] を選択し、[Go] をクリックすることで）変数 varName がサブテンプレート型として定義されます。前に定義したサブテンプレートを呼び出すため、サブテンプレート パスを指定する必要があります。構文は次のようになります。

$<*varName*>.callWithDatafile(<*DatafileName*>)

すべてのデータを入力した後、[OK] をクリックして、指定した変数の当該情報を受け入れます。または、引き続き、この同じ方法で変更する必要のあるすべての変数を編集し、[OK] をクリックします。これにより、これらの更新された変数が組み込まれます。または、[Save] をクリックして [Close] をクリックするか、[Close] をクリックして要求されたら、図 9-3 などのウィンドウで保存を要求されたら、[Save] に同意します。[Create a Data File] は「データ ファイルの作成」（P.9-17）に示され、[Edit] は「テンプレートおよびデータ ファイルの編集」（P.9-19）に示され、[Delete] は「テンプレートおよびデータ ファイルの削除」（P.9-20）に示されています。

検証

図 9-3（ステップ 5 を参照）で入力した情報を検証するには、「テンプレートの作成」セクションのステップ 6 で [Select & Click Go] ドロップダウン リストをクリックした後、次の手順を実行します。

ステップ 1　[Validate] を選択し、[Go] ボタンをクリックします。

ステップ 2　検証が正常に行われた場合、情報ウィンドウが表示されます。

データ ファイルの作成

既存のテンプレートから新しいデータ ファイルを作成できます。目的のテンプレートが使用できない場合、「テンプレートの作成」（P.9-7）に進みます。

データ ファイルを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　ウィンドウの左の部分にある [Template Manager] ツリーで、次のいずれかを実行します。

1. データ ファイルを作成する対象のテンプレートが存在するフォルダまたはサブフォルダをクリックします。または、
2. 選択対象のフォルダの横の矢印をクリックし、データ ファイルを作成する対象のテンプレートをクリックします。

ステップ 3　ステップ 2 で 1. を選択した場合、図 9-2 に示されているウィンドウが表示されます。

データ ファイルを作成する対象のテンプレートのチェックボックスをオンにし、[Create Data File] をクリックします。次に、に進みます。

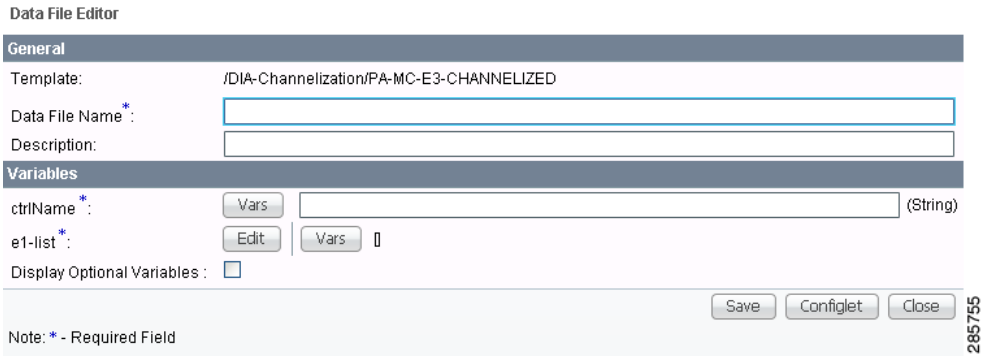
または、ステップ 4 に進みます。

ステップ 4　ステップ 2 で 2. を選択した場合、図 9-10 に示されているボタンが表示されます。

図 9-10　　既存のテンプレートの選択（別の方法）

[Create Data File] をクリックします。表示されるウィンドウの例を図 9-11 に示します。

図 9-11　テンプレート データ ファイル エディタ



ステップ 5　[General] 領域で、次に入力します。

- [Data File Name]（必須）：この名前は一意である必要があります。この名前は英数字で開始する必要があり、英数字と下線のみ含めることができます。
- [Description]（任意）：このデータ ファイルを識別できるようにする説明を入力します。

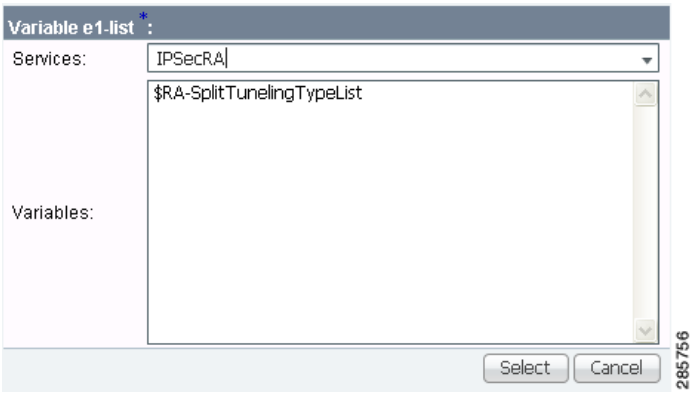
図 9-11 の例の [Variables] 領域では、**cntrlName** は文字列変数です（テンプレート作成時に定義された [Dimension] は [0] です）。1 次元配列を作成することもできます（テンプレート作成時に定義される [Dimension] は [1] です）。**t1-list** は 2 次元配列です（テンプレート作成時に定義された [Dimension] は [2] です）。

t1-list がダイナミック Java クラス変数の場合、Java クラス パッケージ名全体を入力する*必要があります*。たとえば、com.cisco.isc.class_name などです。

（注）　[cntrlName] は、文字列変数にのみすることができます。

ステップ 6　図 9-11 に示されている [Vars] をクリックすると、図 9-12 に示されているウィンドウが表示されます。

図 9-12　テンプレート データ ファイル エディタ



[Services] ドロップダウン リストをクリックすると、次の変数にアクセスできます。

- **MPLS**
- **L2VPN**

- **VPLS**
- **VRF**
- **FlexUNI**

次に、[Variables] で、使用するエントリをクリックし、[Select] をクリックします。

0 次元エントリを使用する場合（テンプレート作成時に [Dimension 0] として設定）、用意されているフィールドに変数を入力することのみできます。

ステップ 7　図 9-11 に示されている [Edit] をクリックします。この結果表示されるウィンドウは、**1** 次元配列と **2** 次元配列のどちらを編集するかに基づきます。

1 次元配列の場合、ステップ 8 に進みます。

2 次元配列の場合、ステップ 11 に進みます。

ステップ 8　1 次元配列の場合（テンプレート作成時に [Dimension 1] として設定）、[Edit] をクリックすると、ウィンドウが表示されます。

ステップ 9　変数を追加するには、[Add] をクリックします。これにより、変数を追加できるウィンドウが表示されます。次に [OK] をクリックします。

ステップ 10　変数を編集または削除するには、変数を強調表示し、[Edit] または [Delete] をクリックします。[Edit] の場合、ウィンドウが表示されます。次に [OK] をクリックします。[Delete] の場合、削除する必要があるかどうか*確認します*。[Delete] をクリックすると、削除が自動的に実行され、ウィンドウが更新されます。ステップ 16 に進みます。

ステップ 11　2 次元配列の場合（テンプレート作成時に [Dimension 2] として設定）、[Edit] をクリックすると、ウィンドウが表示されます。

ステップ 12　[Add Row] をクリックします。これにより、ウィンドウが表示されます。値を入力し、[OK] をクリックします。

ステップ 13　[Add Column] をクリックします。これにより、ウィンドウが表示されます。

ステップ 14　値を入力し、[OK] をクリックします。この結果、ウィンドウが表示されます。

ステップ 15　チェックボックス（トグル）をオンにした後、その行または列を**編集**または**削除**できます。ステップ 13 およびステップ 14 の各指示に従い、引き続き**行を追加**すること、および**列を追加**することもできます。

ステップ 16　2 次元配列の設定が完了したら、[OK] をクリックします。図 9-11 に示されているウィンドウが更新され、新しいデータ ファイルの情報が反映されます。

ステップ 17　次に、[Save] をクリックし、[Close] をクリックして、当該情報を保存し、このファイルを閉じることができます。また、コンフィギュレーション ファイルを表示するには、[Configure] をクリックします。または、[Close] をクリックし、作成した情報を保存する場合は [OK] を必ずクリックします。この情報を保存しない場合、[Close] をクリックし、[Cancel] をクリックします。

テンプレートおよびデータ ファイルの編集

テンプレートまたはデータ ファイルを編集するには、次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　[Template Manager] ツリーで、編集するテンプレートが存在するフォルダまたはサブフォルダをクリックするか、編集するデータ ファイルが存在するテンプレートをクリックします。また、データ ペインの左上隅にある名前がテンプレートの場合、そのテンプレート名をクリックしてテンプレートを編集できます。

テンプレートを編集する場合、図 9-2 に示されているウィンドウが表示されます。データ ファイルを編集する場合、図 9-10 に示されているウィンドウが表示されます。

ステップ 3　[Show Templates] ドロップダウン リストまたは [Show Data Files] ドロップダウン リストを使用することで、テンプレートまたはデータファイルを**名前**順と**説明**順のどちらで表示するか選択できます（どちらの場合もアルファベット順に並べ替えられます）。次に、[Show] ボタンをクリックして、テンプレートまたはデータ ファイルの表示方法をアクティブにします。[Show] ボタンをクリックする前に [matching] フィールドに文字を入力すると、**名前**順または**説明**順に表示されるテンプレートまたはデータ ファイルのリストを最小にすることができます。データ ペインの右上隅にある [Show Templates matching] フィルタまたは [Show Data Files matching] フィルタが非常に便利です。たとえば、[Show Templates] または [Show Data Files] のドロップダウン リストをクリックし、**名前**または**説明**とのマッチングを選択し（マッチングでは、大文字と小文字が区別されます）、その後、[matching] ボックスで、**abc** で始まるテンプレートまたはデータ ファイルの処理を選択できます。この場合、フィールドに **abc*** を入力し、[Show] ボタンをクリックします。これにより、**abc** で始まるテンプレートまたはデータ ファイルのみ表示されます。フィルタの詳細については、「テンプレート ツリーとデータ ペインの表示」（P.9-5）を参照してください。

ステップ 4　編集するテンプレートまたはデータ ファイルのチェックボックスをオンにします。

（注）　データ ファイルの場合、[Configlet] 列があり、この列で [View] をクリックすることで、コンフィギュレーション ファイルを表示できます。

ステップ 5　[Edit] をクリックします。

ステップ 6　テンプレートを編集する場合、図 9-3 に示されているウィンドウが表示されます。次に、テンプレートの作成の項のステップ 5 に進みます。データ ファイルを編集する場合、図 9-10 に示されているウィンドウが表示されます。次に、データ ファイルの作成の項の に進みます。

テンプレートおよびデータ ファイルの削除

テンプレートまたはデータ ファイルを削除するには、次のステップを実行します。

ステップ 1　[Service Design] > [Templates] > [Template Manager] を選択します。

ステップ 2　[Templates] ツリーで、削除するテンプレートが存在するフォルダまたはサブフォルダをクリックするか、削除するデータ ファイルが存在するテンプレートをクリックします。

テンプレートを削除する場合、図 9-2 に示されているウィンドウが表示されます。データ ファイルを削除する場合、図 9-10 に示されているウィンドウが表示されます。

ステップ 3　[Show Templates] ドロップダウン リストまたは [Show Data Files] ドロップダウン リストを使用することで、テンプレートまたはデータファイルを**名前**順と**説明**順のどちらで表示するか選択できます（どちらの場合もアルファベット順に並べ替えられます）。次に、[Show] ボタンをクリックして、テンプレートまたはデータ ファイルの表示方法をアクティブにします。[Show] ボタンをクリックする前に [matching] フィールドに文字を入力すると、**名前**順または**説明**順に表示されるテンプレートまたはデータ ファイルのリストを最小にすることができます。データ ペインの右上隅にある [Show Templates matching] フィルタまたは [Show Data Files matching] フィルタが非常に便利です。たとえば、[Show Templates] または [Show Data Files] のドロップダウン リストをクリックし、**名前**または**説**

明とのマッチングを選択し（マッチングでは、大文字と小文字が区別されます）、その後、[matching] ボックスで、**abc** で始まるテンプレートまたはデータ ファイルの処理を選択できます。この場合、フィールドに **abc*** を入力し、[Show] ボタンをクリックします。これにより、**abc** で始まるテンプレートまたはデータ ファイルのみ表示されます。フィルタの詳細については、「テンプレート ツリーとデータ ペインの表示」（P.9-5）を参照してください。

ステップ 4　削除するテンプレートまたはデータ ファイルのチェックボックスをオンにします。

（注）　データ ファイルの場合、[Configlet] 列があり、この列で [View] をクリックすることで、コンフィギュレーション ファイルを表示できます。

ステップ 5　[Delete] ボタンをクリックします。

削除の確認を求める確認ウィンドウが表示されます。データ ファイルを削除する前に、[In SR Use] 列が [No] に設定されているかチェックして、そのデータ ファイルがサービス要求に関連付けられていないことを確認します。フォルダまたはテンプレートを削除する場合、それらに含まれているデータ ファイルがサービス要求に関連付けられていないことを確認します。[OK] をクリックして削除を実行するか、[Cancel] をクリックして削除をキャンセルします。

削除されたテンプレートまたはデータ ファイルが使用できなくなった、更新済みウィンドウ（図 9-2 または図 9-10 に示されているウィンドウ）が表示されます。

データ ファイルに関連付けられたサービス要求のリスト

図 9-10 に示されている [In SR Use] 列において、[Yes] はデータ ファイルが使用中であることを示し、[No] はデータ ファイルが使用中ではないことを示します。[Yes] が表示されている場合、それをクリックすることができ、関連するすべてのサービス要求のリストが表示されます。[Yes] が表示されている場合、ボタン行で [List All SRs] ボタンが有効になります。[List All SRs] ボタンをクリックすると、図 9-13 に示されているように、選択したデータ ファイルに関連付けられているすべてのサービス要求が表示されます。[In SR Use] 列に [No] が表示されている場合、[List All SRs] ボタンは無効です。

図 9-13 で [Close] ボタンをクリックすると、前のウィンドウが表示されます。

図 9-13　すべての SR の一覧表示

（注）　[Data File Name] 列に一覧表示されているデータ ファイルのみが、このウィンドウを表示したユーザが以前に選択したデータ ファイルです。表示されていない他のデータ ファイルにサービス要求が関連付けられている場合があります。

データ ファイルに関連付けられたポリシーのリスト

図 9-13 に示されている [In Policy Use] 列において、[Yes] はデータ ファイルが使用中であることを示し、[No] はデータ ファイルが使用中ではないことを示します。[Yes] が表示されている場合、それをクリックできます。これにより、関連するすべてのポリシーのリストが表示されます。[Yes] が表示されている場合、ボタン行で [List All Policies] ボタンがイネーブルになります。[List All Policies] ボタンをクリックすると、選択したデータ ファイルに関連付けられているすべてのポリシーが表示されます。[In Policy Use] 列に [No] が表示されている場合、[List All Policies] ボタンはディセーブルです。

新しく作成されたウィンドウで [Close] ボタンをクリックすると、前のウィンドウが表示されます。

（注）　[Data File Name] 列に一覧表示されているデータ ファイルのみが、このウィンドウを表示したユーザが以前に選択したデータ ファイルです。表示されていない他のデータ ファイルにポリシーが関連付けられている場合があります。

ポリシーでのテンプレートの使用

この項では、テンプレートのサポートをイネーブル化してテンプレートおよびデータ ファイルを Prime Provisioning ポリシーと関連付け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。

- 「概要」（P.9-22）
- 「テンプレートおよびデータ ファイルのポリシーへの関連付け」（P.9-22）

概要

Prime Provisioning は、テンプレートおよびデータ ファイルとサービス ポリシーとの関連付けをサポートしています。これにより、プロビジョニング ワークフローのステップが最小化され、また、サービス作成時に不適切なテンプレートおよびデータ ファイルが選択された場合に発生する可能性のあるエラーが減少します。ポリシー エディタ ワークフローで、ポリシー属性が設定された後、新しい [Templates Association] ウィンドウが表示されます。このウィンドウに表示される [Enable Templates] チェックボックスを使用すると、ポリシーに対するテンプレートの関連付けをイネーブルにすること、およびそのポリシーに基づいてサービス要求でテンプレートおよびデータ ファイルを使用できるように指定できます。複数のテンプレートおよびデータ ファイルをポリシーに関連付けることができます。各テンプレートおよびデータ ファイルをデバイス ロールに関連付けることができます。使用できるデバイス ロールは、ポリシー タイプにより決まります。U-PE および PE-AGG デバイス ロールの場合、デバイスに UNI インターフェイスがあるかどうかに基づき、テンプレートおよびデータ ファイルを選択的に決定できます。その後、サービス リクエストの作成時、ポリシー内のテンプレートで指定されたロール タイプにデバイス タイプが一致するか、ポリシーの UNI インターフェイスがある（またはない）ロール タイプにデバイス タイプが一致する場合にだけ、テンプレートが利用可能になります。

テンプレートおよびデータ ファイルのポリシーへの関連付け

この項では、テンプレートおよびデータ ファイルを Prime Provisioning ポリシーに関連付ける方法について説明します。これらの機能は、ポリシーを編集する場合にも適用されます。

ポリシーの属性をポリシーに設定すると、[Template Association] ウィンドウが表示されます。

このウィンドウでは、最終ステップとしてテンプレートおよびデータ ファイルの関連付けを行い、その後、[Finish] ボタンをクリックし、ポリシー設定を保存します。

ポリシーにテンプレート/データ ファイルを関連付けるには、次の手順を実行します。

ステップ 1　[Template Enable] チェックボックスをオンにして、このポリシーに基づいてサービス要求でテンプレートを使用できるようにします。このチェックボックスは、デフォルトでオフになっています。

GUI が更新され、テンプレートおよびデータ ファイルをポリシーに関連付けることができるフィールドが表示されます。

ステップ 2　[Add] ボタンをクリックして、関連付けるテンプレートおよびデータ ファイルを指定するための行を追加します。

新しい行が GUI に表示され、ロール タイプを設定するためのフィールド、テンプレートとデータ ファイルを指定するためのフィールド、およびテンプレートとデータ ファイルをポリシーに基づきサービス要求内で編集できるようにするかどうかを指定するためのフィールドが提供されます。

ステップ 3　[Role Type] 列で、ドロップダウン リストからデバイス ロールを選択します。

ロールの選択肢を次に示します。

- N-PE
- PE-AGG
- U-PE
- CE (MULTI_VRF)
- CE (MANAGED)
- MVRF

（注）　ドロップダウン リストで使用できるデバイス ロールは、ポリシー タイプにより決まります。

ステップ 4　テンプレートおよびデータ ファイルを追加するには、[Template/Data File] 列で [Add] 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。

ステップ 5　[Add] ボタンをクリックして、ポリシーに関連付けるテンプレートおよびデータ ファイルを選択します。

（注）　デバイス ロールが U-PE または PE-AGG として指定されている場合、デバイスに UNI インターフェイスがあるかどうかに基づき、テンプレートを選択的に追加できます。この機能の詳細については、「U-PE および PE-AGG デバイス ロール用のテンプレートの選択的決定」（P.9-25）を参照してください。テンプレートおよびデータ ファイルを追加する実際のステップは、次のステップと同じです。

[Template Datafile Chooser] ウィンドウが表示されます。

このウィンドウは、Prime Provisioning でテンプレートおよび（オプションの）データ ファイルに移動して選択するために使用する標準のテンプレート マネージャ ウィンドウです。

（注）　[Template Datafile Chooser] ウィンドウに関連する次のステップは、ウィンドウの機能について知識があることを前提としています。Template Manager と、Prime Provisioning でテンプレートとデータ ファイルが作成および管理される方法についての追加情報は、「概要」（P.9-1）を参照してください。ここで示される手順は例示用のものです。環境に合わせてステップを変更する必要がある場合がありま

す。たとえば、ポリシーに関連付ける対象として、テンプレート ファイルのみ選択する場合、またはテンプレート ファイルとデータ ファイルの両方を選択する場合があります。これらの両方のシナリオがサポートされています。

ステップ 6　フォルダー ツリーでテンプレートに移動し、クリックして選択します。

テンプレートと、それに関連付けられているデータ ファイルが、GUI の右側に一覧表示されます。

ステップ 7　データ ファイル名の左にあるチェックボックスをオンにし、[Accept] ボタンをクリックします。

（注）　この段階では、必要に応じて、およびテンプレートに対してデータ ファイルが存在するかどうかに基づき、テンプレートのみを選択すること、またはテンプレートとデータ ファイルの両方を選択できます。

[Template Datafile Chooser] ウィンドウが閉じ、選択したテンプレートおよびデータ ファイルがリストされた [Add/Remove Templates] ウィンドウが表示されます。

データ ファイルを選択していない場合、[Datafile] 列は空です。

ステップ 8　テンプレート名の左にあるチェックボックスをオンにして、テンプレートを選択します。

ステップ 9　[Action] で、ドロップダウン リストを使用して [APPEND] または [PREPEND] を選択します。

[Append] は Prime Provisioning に、テンプレートによって生成された CLI を通常の Prime Provisioning（非テンプレート）CLI（コンフィグレット）に追加するように指示します。[Prepend] はこの反対です（テンプレートはコンフィグレットの先頭に追加されます）。

ステップ 10　このテンプレートを、このポリシーに基づいてサービス要求に対して使用するには、[Active] を選択します。

[Active] を選択しないと、テンプレートは使用されません。

ステップ 11　その他のテンプレートおよびデータ ファイルをポリシーに関連付けるには、[Add/Remove Templates] ウィンドウで [Add] をクリックし、該当するステップを繰り返して他のテンプレートおよびデータ ファイルを追加します。

ステップ 12　ウィンドウからテンプレート行を削除するには、テンプレートをチェックし、[Remove] ボタンをクリックしてリストからテンプレートを削除します。

ステップ 13　[Add/Remove Templates] ウィンドウでの選択が完了したら、[OK] をクリックします。

[Template Association] ウィンドウが表示され、ウィンドウ内に 1 つ以上のテンプレートおよびデータ ファイルがアクティブ リンクとして一覧表示されます。複数のテンプレートおよびデータ ファイルを追加した場合、それらは、リンクのカンマ区切りリストに表示されます。

リンクをクリックすると、テンプレートおよびデータ ファイル情報を編集または更新するために、[Add/Remove Templates] ウィンドウに戻ることができます。

ステップ 14　ポリシーに基づきサービス要求でテンプレートおよびデータ ファイルの属性を編集できるようにするには、[Edit] チェックボックスをオンにします。

ステップ 15　所定のロール用のテンプレートおよびデータ ファイルをポリシーに追加するには、[Template Association] ウィンドウで [Add] ボタンをクリックして、上記のステップを繰り返します。

ステップ 16　ポリシーに関連付けられているテンプレートおよびデータ ファイルを削除するには、テンプレートおよびデータ ファイルをチェックして選択します。

次に、[Delete] ボタンをクリックして [Template Association] ウィンドウからそれを削除します。

ステップ 17　1 つ以上のテンプレートおよびデータ ファイルのポリシーへの関連付けが終了したら、[Template Association] ウィンドウで [Finish] ボタンをクリックします。

ポリシーの属性が保存され、ポリシーの作成または変更が完了します。

U-PE および PE-AGG デバイス ロール用のテンプレートの選択的決定

Prime Provisioning には、リング環境などでの U-PE および PE-AGG のデバイスを選択的に判別してテンプレートおよびデータ ファイルを適用する機能があります。サービス ポリシー ワークフローでのテンプレートの関連付け時、U-PE および PE-AGG デバイス ロールでは、テンプレートおよびデータ ファイルを関連付けるための 2 つのオプションを使用できます。これらのオプションを次に示します。

- [Devices with UNI]。このオプションでは、UNI インターフェイスを備えた、指定したロールのデバイスに対して、テンプレートおよびデータ ファイルが設定されます。
- [All other devices]。このオプションでは、UNI インターフェイスを備えたデバイスを含む、指定したロールのすべてのデバイスに対してテンプレートおよびデータ ファイルが設定されます。

使用方法に関する注釈：

- 目的のオプションの横の [Add] リンクをクリックすることで、テンプレートおよびデータ ファイルを選択します。以降のステップは、「テンプレートおよびデータ ファイルのポリシーへの関連付け」（P.9-22）に示されているステップと同じです。
- この機能は、U-PE および PE-AGG 以外のデバイス ロールには適用できません。N-PE ロールは、[Template/Data File] 列に単一の [Add] リンクのみを表示します。
- 下位互換性のために、U-PE デバイスおよび PE-AGG デバイス用の古いポリシーおよび既存のポリシーを編集または表示するとき、[All other Devices] オプションの下に関連するテンプレートおよびデータ ファイルが表示されます。
- 既存のポリシーをコピーする場合、既存のポリシーの [All other Devices] オプションまたは [Devices with UNI] オプションから、関連するテンプレートおよびデータ ファイルを、新しいポリシー内にコピーできます。これは、通常の Prime Provisioning の動作と同じです。
- [All other Devices] オプション、[Devices with UNI] オプション、またはこれらの両方に対して、テンプレート（データ ファイルなし）を関連付けることができます。
- テンプレートの選択的決定は、すべての L2VPN および FlexUNI/EVC ポリシー タイプおよびサービス要求でサポートされています。MPLS VPN の場合、MPLS PE-CE および MPLS PE-NoCE ポリシーおよびサービス要求のみサポートされています。MPLS VPN PE-CE ポリシー タイプの場合、この機能は、PE が NPC に関連付けられている場合も、関連付けられていない場合も適用できます。この機能は、マルチ VRFCE ポリシーおよびサービス要求に対しては使用できません。

次の注釈では、この機能がサービス要求ワークフローでどのようにサポートされるかについて説明します。

- サービス要求作成時、選択テンプレートは、UNI インターフェイスがあるデバイス、または U-PE および PE-AGG デバイス ロール用の UNI と NNI の両方のインターフェイスがあるデバイスに基づき異なります。ポリシー内のテンプレートは、指定したロールで機能する各デバイスにコピーされます。他のロールのデバイスに対して動作の変更はありません。
- テンプレートの選択的決定は、サービス要求変更シナリオに対しては適用できません。したがって、サービス要求が作成された後、デバイスに対し設定されているテンプレートの変更は、ユーザの決定で行うことになります。

サービス要求でのテンプレートの使用

この項では、サービス要求とテンプレートおよびデータ ファイルについて情報を提供します。次の事項について説明します。

概要

この項では、サービス要求でのテンプレートの使用について概要情報を提供します。内容は次のとおりです。

Prime Provisioning GUI でのこれらの機能の実装方法の詳細については、「サービス要求ワークフローでのテンプレートおよびデータ ファイルの使用」（P.9-30）を参照してください。

テンプレートのサービス要求への関連付け

Prime Provisioning のテンプレート メカニズムは、サービス要求によって生成されたデバイス コンフィギュレーションに、別のコンフィギュレーション情報を追加する方法を提供します。このテンプレート メカニズムを使用するには、サービス要求が基づくポリシーを設定して、テンプレートをイネーブルにする必要があります。任意で、サービス要求で使用するテンプレートおよびデータ ファイルをポリシーで指定できます。オペレータが、テンプレートおよびデータ ファイルをデバイス コンフィギュレーションに追加できる適切な RBAC 権限を持っている場合、サービス要求作成時に、これを行うことができます。サービス要求のワークフローでテンプレートおよびデータ ファイルを選択する方法については、「サービス要求ワークフローでのテンプレートの選択」（P.9-30）の項を参照してください。

サービス プロビジョニング時のサブテンプレートの関連付け

すべてのテンプレートを、他のテンプレートで構築ブロックとして使用できます。他のテンプレートを使用するテンプレートをスーパー テンプレートと呼びます。使用されるテンプレートをサブテンプレートと呼びます。テンプレート エディタで新しい属性を使用することで、サブテンプレートをスーパー テンプレートに関連付けることができます。スーパー テンプレートは、変数の値をサブテンプレートに渡すことで、必要なすべてのサブテンプレートをインスタンス化します。インスタンス化の後、サブテンプレートに対して生成されたコンフィグレットがスーパー テンプレート内に配置されます。Prime Provisioning は、デバイス タイプ、ラインカード タイプ、ポート タイプ、ロール タイプ、およびソフトウェア バージョンに応じて、テンプレートを複数のサブテンプレートに分割します。これらのオプション属性は、サブテンプレートの作成時に設定します。サブテンプレートは、次の一致基準に基づき選択されます。

- カード タイプ属性およびポート タイプ属性については完全一致のみ認識されます。これらの属性については、ワイルド カード一致は許可されません。

- デバイス タイプ属性については、完全一致のみ認識されます。
- ソフトウェア バージョン属性については、現在のバージョンと同じソフトウェア バージョンが使用できる場合、それらに対して一致処理が実行されます。使用できない場合、以前の最も高いバージョンに対して一致処理が実行されます。
- 完全一致する属性が見つからない場合、一致処理は、表 9-1 で説明されている基準に進みます。いずれかの一致基準が満たされた場合、およびその場合に限り、スーパー テンプレートの完全一致したサブテンプレートを一覧表示する情報メッセージが表示されます。
- どの属性も一致しなかった場合、デフォルトのサブテンプレートが適用されます。
- デフォルトのサブテンプレートが存在しない場合、すべての属性値がヌルのサブテンプレートが一致対象となります。
- 表に示されているどの行も一致しない場合、Prime Provisioning は、デバイスのデフォルトまたはその他のバージョンのデフォルトとしてマークされているサブテンプレートを探します。このようにマークされたサブテンプレートがない場合、一致するサブテンプレートは検出されません。警告メッセージが表示されます。

表 9-1 に一致基準をまとめます。

表 9-1　サブテンプレートのデフォルトの一致基準

一致の順序	ロール タイプ	デバイス タイプ	ラインカード	ポート タイプ	ソフトウェア バージョン
1	Exact Match	Exact Match	Exact Match	Exact Match	Exact Match
2	Exact Match	Exact Match	Exact Match	Exact Match	前の最も高いバージョン
3	Exact Match	Exact Match	Exact Match	値なし	Exact Match
4	Exact Match	Exact Match	Exact Match	値なし	前の最も高いバージョン
5	Exact Match	Exact Match	値なし	値なし	Exact Match
6	Exact Match	Exact Match	値なし	値なし	前の最も高いバージョン
7	Exact Match	Exact Match	値なし	値なし	値なし
8	Exact Match	値なし	Exact Match	Exact Match	Exact Match
9	Exact Match	値なし	Exact Match	Exact Match	前の最も高いバージョン
10	Exact Match	値なし	Exact Match	値なし	Exact Match
11	Exact Match	値なし	Exact Match	値なし	前の最も高いバージョン
12	Exact Match	値なし	値なし	値なし	Exact Match
13	Exact Match	値なし	値なし	値なし	前の最も高いバージョン
14	Exact Match	Default	値なし	値なし	値なし
15	Exact Match	値なし	値なし	値なし	Default
16	Exact Match	値なし	値なし	値なし	値なし

サブテンプレートに関する使用上のその他の注意事項

- Prime Provisioning はサブテンプレートの深度をチェックしません。サブテンプレートの階層は 1 つのみサポートされます。
- スーパー テンプレートとサブテンプレートの構造が円環になっているかどうかチェックするための検証は実行されません。
- スーパー テンプレートが参照するサブテンプレートをオペレータが削除しようとすると、警告メッセージが生成されます。
- サブテンプレートは変更できます。
- サブテンプレートは、複数のスーパー テンプレートに関連付けることができます。
- 現在のリリースでは、サブテンプレートに対して複数のデータ ファイルは使用できません。複数のデータ ファイルが検出された場合、サービス要求は最初のデータ ファイル（アルファベット順にソートされた有効なデータ ファイルのリスト内の最初のデータ ファイル）を自動的に選択します。

サービス要求作成時のデータ ファイルの作成

オペレータは、サービス要求作成時、データ ファイルを「オンデマンドで」作成できます。テンプレートをサービス ポリシーに関連付ける場合、そのテンプレートのデータ ファイルが存在しないと、変数の値を入力するよう要求するウィザードがオペレータに対し表示されます。サービス要求作成時にオンデマンドでデータ ファイルを作成する場合、サービス要求の変更または再展開時に、任意またはすべての変数を変更できます。

サービス要求ワークフローは、次に示すように、データ ファイルの動的作成をサポートしています。

- サービス要求が基づくポリシーで、テンプレートが編集不可としてマークされている場合、オペレータは、サービス要求作成時にそのテンプレートを編集できません。ただし、テンプレートおよびデータ ファイルが変更できなくても、それらの名前は表示できます。
- テンプレートがポリシーで編集可能としてマークされている場合、オペレータは、サービス要求作成時にテンプレートおよびデータ ファイルを変更できます（適切な RBAC 権限が前提となります）。

テンプレートを編集できる場合、次の点が適用されます。

- テンプレートがサービス ポリシーに関連付けられていて、そのテンプレートに対し 1 つ以上のデータ ファイルが存在する場合、オペレータは、サービス要求作成時に、適切なデータ ファイルを選択できます。
- テンプレートに対しデータ ファイルが 1 つのみ存在する場合、そのデータ ファイルが自動的に選択されます。
- サービス要求作成時に、オペレータは、テンプレート変数の値を入力できます。
- テンプレートに対しデータ ファイルが存在しない場合、オペレータは、サービス要求作成時に、新しいデータ ファイルを任意に作成できます。[Template Association] ウィンドウから [Datafile Chooser] ウィンドウを開くと、[Create Datafile] ボタンが表示されます。このボタンを使用して、新しいデータ ファイルを作成できます。
- オペレータが、データ ファイルを作成するための適切な RBAC 権限を所有している場合に限り、[Create Datafile] ボタンは表示されます。

サービス要求のワークフローでデータ ファイルを設定する方法については、「サービス要求ワークフローでのデータ ファイルの作成」（P.9-31）の項を参照してください。

negate テンプレートを使用したテンプレート コンフィギュレーションのデコミッション

テンプレートおよびデータ ファイルから作成されたコンフィギュレーションを削除するには、negate テンプレートを既存のサービスに適用する必要があります。Prime Provisioning は、サービス要求の中止中に、該当する negate テンプレートを自動的に適用します。Prime Provisioning テンプレート マネージャを使用して negate テンプレートを作成する方法の詳細については、「negate テンプレート」（P.9-9）を参照してください。

ポリシーまたはサービス要求でテンプレートを関連付けると、negate テンプレートも自動的に関連付けられます。サービスのデコミッション時、展開に対し negate テンプレートが使用されます。テンプレートおよびデータ ファイルが関連付けられているサービス リクエストを中止すると、オリジナルのテンプレート名にサフィクス「.Negate」が後続したテンプレート名を検索する方法により、negate テンプレートが動的に自動選択されます。これは、展開時に実行されます。negate テンプレートは、negate テンプレートが関連付けられている先のテンプレートのデバイス属性に基づき動的にインスタンス化されます。

（注）　テンプレートに適用されるオプションの属性（デバイス タイプ、ラインカード タイプ、ポート タイプ、ソフトウェア バージョンなど）が、対応する negate テンプレートに自動的に適用されます。オプションの属性は、negate テンプレートに直接適用できません。

サービスがデコミッションされると、適切な negate テンプレートが展開されます。次に示すように、negate テンプレートのデータ ファイルが展開時に選択されます。

- ネゲート テンプレートに有効なデータ ファイルが存在しない場合は、メイン テンプレートと同じ名前を持つネゲート テンプレートの下にデータ ファイルがないか、データ ファイルがまったくないために、サービス要求の展開中にエラーが発生します。
- negate テンプレートに 1 つのデータ ファイルのみ関連付けられている場合、そのデータ ファイルが自動的に選択されます。negate テンプレートに対し 1 つのデータ ファイルがあり、その negate テンプレートの名前がデータ ファイルの名前に一致しない場合、展開はエラーが原因で失敗し、サービス要求は [INVALID] 状態に移行します。
- 複数のデータ ファイルがある場合、negate テンプレートの名前と一致する名前を持つデータ ファイルのみ選択されます。

次の項目で、各種変更シナリオでのテンプレートの動作について説明します。

- サービス要求に関連付けられているテンプレートを変更すると、negate テンプレートは、新しく選択されたテンプレートの negate テンプレートに自動的に変更されます。この場合、Prime Provisioning は、新しく関連付けられたテンプレートとともに、直前に関連付けられていたネゲート テンプレートも実行します。
- テンプレートまたは negate テンプレートを変更しても、サービス要求は、テンプレートを通じて以前に実行されたコンフィギュレーションの変更をロールバックしません。
- サービス要求を変更しても、テンプレート コマンドは常に展開されます （残りの項目を参照して、追加の説明を確認してください）。
- テンプレートおよびデータ ファイル情報を変更せずにサービス要求を変更した場合、テンプレート コマンドは再展開されません。テンプレートおよびデータ ファイルの変更をトリガーする変更は、古いテンプレートの否定、およびデバイス コンフィグレットへの新しいテンプレート コマンドの追加のみです。
- ForceTemplateDeploy DCPL プロパティが ON のとき、変更対象のテンプレートに関係なく、サービス要求が変更されると、テンプレートは再展開されます。ただし、negate テンプレートは再展開されない場合があります。negate テンプレートは、サービス要求のリンクまたは接続回線が削除さ

れた場合に限り展開されます（これは、削除対象のリンクに関連付けられているテンプレートも削除されることを暗黙的に意味します）。ForceTemplateDeploy DCPL プロパティが OFF の場合、negate テンプレートは、次の条件に基づきインスタンス化されます。

  - サービス要求のリンクまたは接続回線が削除またはデコミッションされる。
  - テンプレートが変更される（たとえば、既存のテンプレートが削除され、新しいテンプレートがリンクに追加される、または既存のテンプレートの削除のみ行われる）。
  - テンプレートに関連付けられているサービス要求のリンクまたはデバイスがリホーミングされる。

- サービス要求でデバイスが変更されると、古いデバイスに対し negate テンプレートが展開され、新しいデバイスに対しテンプレートが展開されます。
- サービス要求のリンクが削除され、新しいリンクが追加されると、削除されたリンクに対し negate テンプレートが展開され、追加されたリンクに対しテンプレートが展開されます。

サービス要求ワークフローでのテンプレートおよびデータ ファイルの使用

この項では、サービス要求ワークフローで実行できる、テンプレート、データ ファイル、および negate テンプレートに関連するタスクについて説明します。次のタスクについて説明します。

- 「サービス要求ワークフローでのテンプレートの選択」（P.9-30）
- 「サービス要求ワークフローでのデータ ファイルの作成」（P.9-31）
- 「追加テンプレートを含むサービス要求のデコミッション」（P.9-32）
- 「[Service Requests] ウィンドウからのテンプレートの表示」（P.9-33）

サービス要求ワークフローでのテンプレートの選択

サービス要求を作成する場合、ワークフローには、サービス要求が基づくポリシーの選択、インターフェイスとその他の属性の設定などが含まれます。ワークフローで表示される特定のウィンドウおよび属性は、L2VPN、VPLS、MPLS、FlexUNI/EVC など、サービス要求のタイプに基づきます。

サービス要求でテンプレートおよびデータ ファイルを関連付けるには、[Service Request Editor] ウィンドウの適切なウィンドウでリンクを選択する必要があります。通常は、デバイスの [Add] リンクをクリックすることで、これを行います。

（注）　サービス要求ワークフロー時には、U-PE デバイスおよび PE-AGG デバイス用のテンプレートを選択的に決定するオプションはありません。U-PE ロールおよび PE-AGG ロールで機能するデバイスに UNI インターフェイスが存在するかどうかに基づき、ポリシーからテンプレートが自動的にコピーされます。この機能の詳細については、「U-PE および PE-AGG デバイス ロール用のテンプレートの選択的決定」（P.9-25）の項を参照してください。

デバイス用の 1 つ以上のテンプレートおよびデータ ファイルを選択するには、次のステップを実行します。

ステップ 1　デバイスの [Template/Datafile] 列で [Add] 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。

ステップ 2　[Add] ボタンをクリックします。

[Add/Remove Templates] ウィンドウが表示されます。

ステップ 3　フォルダ内のテンプレートに移動し、テンプレートを選択します。

テンプレートと、それに関連付けられているデータ ファイルが、GUI の右側に一覧表示されます。

この時点では、既存のデータ ファイルを選択すること、または [Create Data File] ボタンをクリックして、ワークフローで動的にデータ ファイルを作成できます。この項の残りのステップでは、既存のテンプレートおよびデータ ファイルを選択する場合について説明します。データ ファイルを動的に作成する方法の詳細については、「サービス要求ワークフローでのデータ ファイルの作成」（P.9-31）の項を参照してください。

ステップ 4　データ ファイルのチェックボックスをオンにして、それを選択します。

ステップ 5　[Accept] ボタンをクリックして選択を確定します。

テンプレートとデータ ファイルの組み合わせが [Add/Remove Templates] ウィンドウに表示されます。

ステップ 6　その他のテンプレートおよびデータ ファイルをリストに追加するには、[Add] ボタンをクリックし、上記の該当するステップを繰り返します。

ステップ 7　テンプレートおよびデータ ファイルの選択が完了したら、[Add/Remove Templates] ウィンドウで [OK] ボタンをクリックします。

[Template Association] ウィンドウの [Template/Datafile] 列にテンプレートおよびデータ ファイルが表示されます。

デバイスに対し複数のテンプレートおよびデータ ファイルを選択した場合、図に示されているように、カンマで区切られたリストとして表示されます。

ステップ 8　[Finish] ボタンをクリックして、選択したテンプレートおよびデータ ファイルが関連付けられたサービス要求を作成します。

サービス要求に関連付けられたテンプレートが、1 つ以上のサブテンプレートで構成されるスーパー テンプレートの場合は、選択の確認を要求するメッセージが Prime ProvisioningISC に表示されます。

サービスの展開時に、テンプレートおよびデータ ファイルをインスタンス化する方法の詳細については、「テンプレートのサービス要求への関連付け」（P.9-26）の項で提供されている情報を参照してください。

サービス要求ワークフローでのデータ ファイルの作成

サービス要求のリンク属性の設定の最終段階で、[Template Association] ウィンドウが表示されます。[Template Association] ウィンドウには、リンクを構成するデバイス、デバイス ロール、およびデバイスに関連付けられている 1 つ以上のテンプレートとデータ ファイルが一覧表示されます。「サービス要求ワークフローでのテンプレートの選択」（P.9-30）の項の説明に従い、デバイスに関連付ける 1 つ以上のテンプレートおよびデータ ファイルを選択できます。[Template Datafile Chooser] ウィンドウで選択したテンプレートのいずれかに、関連するデータ ファイルがない場合、またはそのテンプレート用の新しいデータ ファイルを作成する場合、サービス要求の設定時にワークフローで動的にこれを実行できます。

テンプレート用の新しいデータ ファイルを動的に設定するには、次のステップを実行します。

ステップ 1　[Template Association] ウィンドウで、デバイスの [Template/Datafile] 列内の [Add] リンクをクリックします

（デバイスに対してテンプレートを以前に選択した場合、テンプレート名の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。

ステップ 2　[Add] ボタンをクリックします。

[Template Datafile Chooser] ウィンドウが表示されます。

ステップ 3　フォルダ内のテンプレートに移動し、テンプレートを選択します。

テンプレートと、それに関連付けられているデータ ファイルが、GUI の右側に一覧表示されます。次の例は、例のディレクトリで AccessList1 テンプレートを使用します。

ステップ 4　ワークフローでデータ ファイルを動的に作成するには、[Create Data File] ボタンをクリックします。

[Data File Editor] ウィンドウが表示されます。

ステップ 5　この時点では、Prime Provisioning でデータ ファイルを作成するための標準ワークフロー内にいます。

[Date File Editor] ウィンドウで、データ ファイルの名前と説明を指定すること、変数値を設定すること、コンフィグレットを表示することなどができます。これらのステップを実行する方法の詳細については、「概要」（P.9-1）を参照してください。

ステップ 6　新しいデータ ファイルの属性の設定が完了したら、[Save] をクリックしてこの情報を保存し、[Close] をクリックしてファイルを閉じます。また、コンフィギュレーション ファイルを表示するには、[Configure] をクリックします。また、作成した情報を保存する場合、[Close] をクリックし、必ず [OK] をクリックします。

この情報を保存しない場合、[Close] をクリックし、[Cancel] をクリックします。

データ ファイルが保存されると、[Template Datafile Chooser] ウィンドウが表示され、そこに新しく作成されたデータ ファイルが一覧表示されます。

追加テンプレートを含むサービス要求のデコミッション

この項では、テンプレートを追加した Prime Provisioning サービス要求をデコミッションする方法について説明します。

（注）　Prime Provisioning でテンプレートを使用する方法の一般情報については、「概要」（P.9-1）を参照してください。

テンプレートのコマンドは、サービスの作成に関連付けられたものとは独立して扱われます。したがって、テンプレート コマンドは、サービス デコミッション時にデバイスから個別に削除する必要があります。先行するテンプレート コマンドを削除するには、個別のテンプレートがデコミッション プロセス時に必要になります。サービス要求をデコミッションしても、元のテンプレート コマンドは自動的に削除されません。個別の negate テンプレートをデコミッション プロセスに追加する必要があり、元のテンプレートを削除する必要があります。元のテンプレートで追加された任意の不要な IOS コマンドを正しく削除するには、必要な NO コマンドが negate テンプレートに含まれている必要があります。

追加テンプレートを含むサービス要求を作成する標準的な方法を次に示します。

1. サービス ポリシーを定義します。
2. テンプレートとデータ ファイル（および negate テンプレートとデータ ファイル）を構築します。
3. 追加テンプレートを含むサービス要求を作成します。これを実行するステップは、このガイドの関連する章で説明されています。
4. テンプレートの追加先にサービス要求を展開します。

関連するテンプレートを含む、展開済みのサービス要求をデコミッションするには、次のステップを実行する必要があります。

1. negate テンプレートとデータ ファイル（存在しない場合）を作成します。これを使用して、元のテンプレートにより組み込まれたコマンドを削除します。ネゲート テンプレートの詳細については、*『Cisco Prime Provisioning 6.3 API Programmer Guide』の第 4 章「Using Templates」*を参照してください。
2. サービス要求をデコミッションします。negate テンプレートが動的に選択されます。

   サービス要求は [Requested] 状態のままですが、[Operation Type of Delete] に変更されます。
3. サービス要求を展開します。これにより、サービス要求がデコミッションされ、negate テンプレートがダウンロードされ、それにより、元のテンプレート コマンドが削除されます。

[Service Requests] ウィンドウからのテンプレートの表示

サービス要求に 1 つ以上のテンプレートが関連付けられている場合、[Service Request Manager] ウィンドウの [Data Files] 列にペーパー クリップ型のアイコンが表示されます。

（注） [Show Services with] フィールドを使用して、特定のデータ ファイルまたはテンプレート ファイルを備えたサービス要求を検索できます。ドロップダウン リストから [Data File Name] または [Template Name] を選択し、[matching] フィールドに検索文字列を入力します。[matching] フィールドでは、大文字と小文字は区別されず、またワイルドカード（*）がサポートされます。[of Type] フィールドを使用して特定のサービス タイプの検索に制限することで、検索をさらに絞り込むことができます。[Template Name] を使用してサービス要求を一覧表示する場合、テンプレート ファイルの場所を示すパス全体を指定します（たとえば、examples\template。examples がフォルダ名で、template がテンプレート名を示します）。

サービス要求に関連付けられているテンプレートのコンフィグレットを表示するには、次のステップを実行します。

ステップ 1　[Service Request Manager] ウィンドウのテンプレートが関連付けられたサービス要求のチェックボックスをオンにします。これは、[Data Files] 列にペーパー クリップ型のアイコンが表示されていることで判別できます。

ステップ 2　[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。

図に示されているように、[Associated data file(s)] 行に、サービス要求に関連付けられている各データ ファイルのリンクが表示されます。

ステップ 3　データ ファイルのリンクをクリックして、テンプレートのコンフィグレットを表示します。

ステップ 4　コンフィグレットを確認した後、[OK] をクリックしてコンフィグレット表示ウィンドウを閉じます。

ステップ 5　[OK] をクリックして [Service Request Details] ウィンドウを閉じます。

ステップ 6　別の方法として、[Service Requests] ウィンドウでペーパー クリップ アイコンをクリックすることで、サービス要求に関連付けられているデータ ファイルにアクセスできます。

[Service Request] ウィンドウのデータ ファイルの詳細が表示されます。

このウィンドウには、サービス要求に関連付けられているデータ ファイルのリストのみ表示されます。

ステップ 7　データ ファイルのリンクをクリックして、テンプレートのコンフィグレットを表示します。

ステップ 8　コンフィグレットを確認した後、[OK] をクリックしてコンフィグレット表示ウィンドウを閉じます。

ステップ 9　[Close] をクリックして [Service Request Datafile Details] ウィンドウを閉じ、[Service Requests] ウィンドウに戻ります。

サンプル テンプレート

テンプレートの例にアクセスするには、[Service Design] > [Templates] > [Template Manager] と選択して、[Template] ペインのフォルダをナビゲートします。最後の階層の情報に到達するまで、作成済みの各フォルダおよびサブフォルダの横の矢印記号を続けてクリックできます。最後に使用可能なレベルはテンプレート名です。

表 9-2 には、一部の使用可能なテンプレートの例が示されています。使用可能な例の詳細なリストについては、Prime Provisioning の GUI を参照してください。

表 9-2　サンプル テンプレートとその説明

フォルダ	テンプレート	説明
DIA-Channelization	10K-CHOC12-STS1-PATH	チャネライズド OC12 を STS-1 パスに分割するためのサンプル テンプレート。
	10K-CT3-CHANNELIZED	チャネライズド T3 ラインカードから T1 を作成するためのサンプル テンプレート。
	10K-CT3-UNCHANNELIZED	チャネライズド T3 からフルレート T3 またはサブレート T3 インターフェイスを作成するためのサンプル テンプレート。
	PA-MC-E3-CHANNELIZED	E3 から E1（チャネル グループ）を作成するためのサンプル テンプレート。
	PA-MC-STM1-AU3-CHANNELIZE	TUG-2 から E1（チャネル グループ）を作成するためのサンプル テンプレート。このテンプレートでは、TUG-2 をさらに作成する AU-3 AUG マッピングが使用されています。
	PA-MC-STM1-AU4-CHANNELIZE	TUG-2 から E1（チャネル グループ）を作成するためのサンプル テンプレート。このテンプレートでは、TUG-3 および TUG-2 を作成する AU-4 AUG マッピングが使用されています。
	PA-MC-T3-CHANNELIZED	T3 から T1（チャネル グループ）を作成するためのサンプル テンプレート。
Examples	AccessList	入れ子になった繰り返しループおよび多次元変数の例を示すテンプレート。
	AccessList1	最も単純なテンプレート変数の代入の例を示します。
	CEWanCOS	if-else ステートメント、繰り返しステートメント、数式、および 1 次元変数の例を示します。

表 9-2　サンプル テンプレートとその説明 （続き）

フォルダ	テンプレート	説明
QoS/L2/ATM	CLP_Egress	qos_group の設定、およびインターフェイスの出力での ATM セル損失率優先度の例を示すサンプル テンプレート。
	CLP_Ingress	インターフェイスの入力で、セル損失率優先度がマークされた ATM セルの MPLS experimental bit を設定するサンプル テンプレート。
QoS/L2/Ethernet	3400_Egress	
QoS/L2/FrameRelay	classification	FrameRelay DLCI 値に基づく帯域幅予約の例を示すサンプル テンプレート。

リポジトリ変数の概要

この項には、次の表が含まれています。

- 表 9-4（P.9-45）、「MPLS リポジトリ変数」
- 表 9-3（P.9-35）、「L2VPN リポジトリ変数」
- 表 9-7（P.9-55）、「VRF リポジトリ変数」
- 表 9-5（P.9-49）、「FlexUNI/EVC リポジトリ変数」
- 表 9-6（P.9-49）、「VPLS リポジトリ変数」

表 9-3 に、Prime Provisioning テンプレートから使用できる MPLS リポジトリ変数の概要を示します。

表 9-3　MPLS リポジトリ変数

リポジトリ変数	ディメンション	説明
Advertised_Routes_To_CE	2	CE のアドレス空間を定義するために PE に配置されるアドバタイズ済みスタティック ルートの 1 つ以上の IP アドレスのリスト。
CARD_TYPE	0	サービスにイーサネット アクセスが実装されているかどうかに基づき、NPE または UNI インターフェイスを示します。
CE_BGP_AS_ID	0	CE の BGP AS ID（CE と PE の間のルーティング プロトコルが BGP の場合）。
CE_BGP_AS_ID_IPV6	0	アドレス ファミリが IPv6 の場合、これは、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロトコルの自律システム（AS）番号を指定します。
CE_DLCI	0	フレーム リレー カプセル化対応の CE の DLCI 値。
CE_EIGRP_AS_ID	0	CE の EIGRP AS ID（CE と PE の間のルーティング プロトコルが EIGRP の場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
CE_Facing_MVRFCE_BGP_AS_ID	0	MVRFCE の BGP AS ID（CE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_DLCI	0	フレーム リレー カプセル化対応の MVRFCE インターフェイスに接続する CE の DLCI 値（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_EIGRP_AS_ID	0	MVRFCE の EIGRP AS ID（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Intf	0	MVRFCE のインターフェイスに接続する CE の名前（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Intf_Address	0	MVRFCE インターフェイスに接続する CE に割り当てる IP アドレス（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Intf_Encap	0	MVRFCE インターフェイスの CE 接続のカプセル化（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Intf_Name	0	MVRFCE インターフェイスに接続する CE の名前（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Intf_Type	0	MVRFCE インターフェイスの CE 接続のインターフェイス タイプ（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Ospf_Process_ID	0	MVRFCE の OSPF プロセス ID（CE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_Tunnel_Src_Addr	0	GRE カプセル化対応の MVRFCE インターフェイスに接続する CE のトンネル ソース アドレス（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_VCD	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する CE の VCD 値（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_VCI	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する CE の VCI 値（MPLS リンクに MVRFCE が含まれる場合）。
CE_Facing_MVRFCE_VLAN_ID	0	イーサネット カプセル化対応の MVRFCE インターフェイスに接続する CE の VLAN ID（MPLS リンクに MVRFCE が含まれる場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
CE_Facing_MVRFCE_VPI	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する CE の VPI 値（MPLS リンクに MVRFCE が含まれる場合）。
CE_Intf_Address	0	CE インターフェイスに割り当てる IP アドレス。
CE_Intf_Encap	0	CE インターフェイスのカプセル化。
CE_Intf_Name	0	CE インターフェイスの名前。
CE_MVRFCE_Bandwidth_Metric_For_Redistribution	0	EIGRP の再配布の帯域幅メトリック（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFC が含まれる場合）。
CE_MVRFCE_BGP_AS_ID	0	CE の BGP AS ID（CE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
CE_MVRFCE_Delay_Metric_For_Redistribution	0	EIGRP の再配布の遅延メトリック（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFC が含まれる場合）。
CE_MVRFCE_EIGRP_AS_ID	0	CE の EIGRP AS ID（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
CE_MVRFCE_Loading_Metric_For_Redistribution	0	EIGRP の再配布のロード メトリック（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFC が含まれる場合）。
CE_MVRFCE_MTU_Metric_For_Redistribution	0	EIGRP の再配布の MTU メトリック（CE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFC が含まれる場合）。
CE_MVRFCE_Ospf_Process_ID	0	CE の OSPF プロセス ID（CE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
CE_Ospf_Process_ID	0	CE の OSPF プロセス ID（CE と PE の間のルーティング プロトコルが OSPF の場合）。
CE_Tunnel_Src_Addr	0	GRE カプセル化対応の CE のトンネル ソース アドレス。
CE_VCD	0	ATM カプセル化対応の CE の VCD 値。
CE_VCI	0	ATM カプセル化対応の CE の VCI 値。
CE_Vlan_ID	0	イーサネット カプセル化対応の CE の VLAN ID。
CE_VPI	0	ATM カプセル化対応の CE の VPI 値。
Export_Map	0	VRF に関連付けられているエクスポート マップの名前。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
Extra_CE_Loopback_Required	0	CE で追加のループバック要求が必要かどうかを示すフラグ。
Import_Map	0	VRF に関連付けられているインポート マップの名前。
Is_Default_Info_Originate	0	PE で BGP に対し **default-information originate** コマンドを使用するかどうか示すフラグ（STATIC が CE と PE の間の実行プロトコルの場合）。
Is_Default_Info_Originate_IPV6	0	PE で BGP に対し default-information originate コマンドを使用するかどうかを示すフラグ（アドレス ファミリが IPv6 で、STATIC が CE と PE の間の実行プロトコルの場合）。
Is_Default_Routes_Sent_To_CE	0	デフォルト ルートをリモート CE に送信するかどうかを示すフラグ。
Join_Grey_Mgmt_Vpn	0	Grey Management VPN に MPLS を追加するかどうかを示すフラグ。
Max_route_threshold	0	VRF にインポートできるルートの最大数のパーセント値。
Max_Routes	0	VRF にインポートできるルートの最大数。
MPLSCeInterfaceMask	0	特定の MPLS VPN リンク用の CE インターフェイスに割り当てる IP アドレスのマスク。
MPLSCeLoopbackAddress	0	特定の MPLS VPN リンク用の追加 CE ループバック アドレスの IP アドレス。
MPLSCLECeFacingEncapsulation	0	その特定の MPLS VPN リンク用の CE に接続するデバイスのインターフェイスのカプセル化。
MPLSCLECeFacingInterfaceName	0	その特定の MPLS VPN リンク用の CE に接続するデバイスのインターフェイスの名前。
MPLSCLEPeFacingEncapsulation	0	その特定の MPLS VPN リンク用の PE に接続するデバイスのインターフェイスのカプセル化。
MPLSCLEPeFacingInterfaceName	0	その特定の MPLS VPN リンク用の PE に接続するデバイスのインターフェイスの名前。
MPLSExportRouteTargets	1	MPLS VPN リンクに関連付けられている特定の VRF に対しエクスポートされるルート ターゲットのリスト。
MPLSImportRouteTargets	1	MPLS VPN リンクに関連付けられている特定の VRF に対しインポートされるルート ターゲットのリスト。
MPLSPeInterfaceMask	0	特定の MPLS VPN リンク用の PE インターフェイスに割り当てる IP アドレスのマスク。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
Multicast_Enabled_IPv6	0	マルチキャスト IPv6 VPN のイネーブル化およびディセーブル化。チェックボックスがオンの場合、マルチキャスト IPv6 VPN コンフィグレットが生成されます。
Multicast_Route_Limit	0	VRF のマルチキャスト ルート制限値。
MVRFCE_CE_Advertised_Routes_To_CE	2	MPLS リンクに MVRFCE が含まれる場合の、CE のアドレス空間を定義するために PE に配置されるアドバタイズ済みスタティック ルートの 1 つ以上の IP アドレスのリスト。
MVRFCE_CE_IP_Unnumbered	0	MVRCE と CE のリンクに番号を付けないようにするかどうか示すフラグ（MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_Is_Default_routes_Sent_To_CE	0	デフォルト ルートをリモート CE に送信するかどうかを示すフラグ（MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_NBR_ALLOW_AS_IN	0	AllowASIn フラグ（CE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_NBR_AS_OVERRIDE	0	ASOverride フラグ（CE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_Ospf_Area_Number	0	OSPF エリア番号（CE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_Ospf_Route_Policy	0	設定する OSPF ルートの再配布ポリシーの名前（MPLS リンクに MVRFCE_CE が含まれる場合）。
MVRFCE_CE_Routes_To_Reach_Other_Sites	2	CE に配置するスタティック ルートを指定する 1 つ以上の IP アドレスのリスト（MPLS リンクに MVRFCE が含まれる場合）。
MVRFCE_CE_Routing_Protocol	0	MVRFCE と CE の間のルーティング プロトコル。
PE_BGP_AS_ID	0	PE の BGP AS ID（CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_Cable_Both_Helper_Address_List	1	ケーブル モデムとホストの両方の UDP ブロードキャストが転送される先の DHCP サーバの IP アドレスのリスト。
PE_Cable_Modem_Helper_Address_list	1	ケーブル モデムの UDP ブロードキャストが転送される先の DHCP サーバの IP アドレスのリスト。
PE_Cable_Modem_Host_Helper_Address_List	1	ホストの UDP ブロードキャストが転送される先の DHCP サーバの IP アドレスのリスト。
PE_Cable_Modem_Secondary_Address_List	1	ケーブル インターフェイスのケーブル モデム セカンダリ アドレスのリスト。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PE_CE_Bandwidth_Metric_For_ Redistribution	0	EIGRP の再配布用の帯域幅メトリック（CE と PE の間のルーティング プロトコルが EIGRP の場合）。
PE_CE_BGP_ADVERTISE_ INTERVAL_IPV6		BGP ルーティング プロトコルのアドバタイズの間隔値（アドレス ファミリが IPv6 の場合）。
PE_CE_BGP_DEFAULT_ORIGINATE_ ROUTE_POLICY_IPV4	0	デフォルトのオリジネート ルート ポリシーの名前（CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_CE_BGP_DEFAULT_ORIGINATE_ ROUTE_POLICY_IPV6	0	デフォルトのオリジネート ルート ポリシーの名前（CE と PE の間のルーティング プロトコルが BGP で、アドレス ファミリが IPV6 の場合）。
PE_CE_BGP_MAX_PREFIX_NUMBE R	0	BGP ルーティング プロトコルの BGPNieghbor MaxPrefix 値。
PE_CE_BGP_MAX_PREFIX_NUMBE R_IPV6	0	BGP ルーティング プロトコルの BGPNieghbor MaxPrefix 値（アドレス ファミリが IPv6 の場合）。
PE_CE_BGP_MAX_PREFIX_RESTAR T	0	BGP ルーティング プロトコルの BGPNieghborMaxprefix 再起動値。
PE_CE_BGP_MAX_PREFIX_RESTAR T_IPV6	0	BGP ルーティング プロトコルの BGPNieghborMaxprefix 再起動値（アドレス ファミリが IPv6 の場合）。
PE_CE_BGP_MAX_PREFIX_THRESH OLD	0	BGP ルーティング プロトコルの BGPNieghborMaxprefix しきい値。
PE_CE_BGP_MAX_PREFIX_THRESH OLD_IPV6	0	BGP ルーティング プロトコルの BGPNieghborMaxprefix しきい値（アドレス ファミリが IPv6 の場合）。
PE_CE_BGP_MAX_PREFIX_WARNIN G_ONLY	0	BGPNieghborMaxprefix warnily_only（イネーブルまたはディセーブル）。
PE_CE_BGP_MAX_PREFIX_WARNIN G_ONLY_IPV6	0	BGPNieghborMaxprefix warnily_only（イネーブルまたはディセーブル）（アドレス ファミリが IPv6 の場合）。
PE_CE_BGP_Neighbor_Route_Map_ Or_Policy_In	0	デバイスで設定する BGP ネイバー ルート マップまたはポリシーの名前。
PE_CE_BGP_Neighbor_Route_Map_ Or_Policy_Out	0	デバイスで設定する BGP ネイバー ルート マップまたはポリシー アウトの名前。
PE_CE_Delay_Metric_For_ Redistribution	0	EIGRP の再配布用の遅延メトリック（CE と PE の間のルーティング プロトコルが EIGRP の場合）。
PE_CE_EIGRP_AUTHENTICATION_K EY_CHAIN_NAME	0	1 つ以上のインターフェイスで 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の名前（CE と PE の間のルーティング プロトコルが EIGRP の場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PE_CE_EIGRP_AUTHENTICATION_KEY_CHAIN_NAME_IPV6	0	アドレス ファミリが IPV6 で、CE と PE の間のルーティング プロトコルが EIGRP の場合、これは、1 つ以上のインターフェイスで 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の名前を指定します。
PE_CE_IP_Unnumbered	0	PE と CE のリンクに番号を付けないようにするかどうか示すフラグ。
PE_CE_IPV6_Routing_Protocol	0	PE と CE の間のルーティング プロトコル（アドレス ファミリが IPv6 の場合）。
PE_CE_Loading_Metric_For_Redistribution	0	EIGRP の再配布用のロード メトリック（CE と PE の間のルーティング プロトコルが EIGRP の場合）。
PE_CE_MTU_Metric_For_Redistribution	0	EIGRP の再配布用の MTU メトリック（CE と PE の間のルーティング プロトコルが EIGRP の場合）。
PE_CE_NBR_Allow_AS_In	0	AllowASIn フラグ（CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_CE_NBR_Allow_AS_In_IPV6	0	AllowASIn フラグ（アドレス ファミリが IPv6 で、CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_CE_NBR_AS_Override	0	ASOverride フラグ（CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_CE_NBR_AS_Override_IPV6	0	ASOverride フラグ（アドレス ファミリが IPv6 で、CE と PE の間のルーティング プロトコルが BGP の場合）。
PE_CE_NBR_Send_Community_IPV6	0	アドレス ファミリが IPv6 の場合、これらの値は Send_Community 属性の「Standard」、「extended」、「Both」を指定します。
PE_CE_Ospf_Area_Number	0	OSPF エリア番号（CE と PE の間のルーティング プロトコルが OSPF の場合）。
PE_CE_Ospf_Match_Internal_External	0	デバイスで設定する OSPF 再配布の一致基準の名前。
PE_CE_OSPF_METRIC_TYPE	0	メトリック タイプ（CE と PE の間のルーティング プロトコルが OSPF の場合）。
PE_CE_OSPF_METRIC_VALUE	0	メトリック値（CE と PE の間のルーティング プロトコルが OSPF の場合）。
PE_CE_Ospf_Route_Policy	0	デバイスで設定する OSPF 再配布のルート ポリシーの名前。
PE_CE_OSPF_ROUTE_POLICY	0	ルート ポリシーの名前（CE と PE の間のルーティング プロトコルが OSPF の場合）。
PE_CE_Reliability_Metric_For_Redistribution	0	EIGRP の再配布用の信頼性メトリック（CE と PE の間のルーティング プロトコルが EIGRP の場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PE_CE_Routing_Protocol	0	PE と CE の間のルーティング プロトコル。
PE_DLCI	0	フレーム リレー カプセル化対応の PE の DLCI 値。
PE_EIGRP_AS_ID	0	PE の EIGRP AS ID（CE と PE の間のルーティング プロトコルが EIGRP の場合）。
PE_Facing_MVRFCE_BGP_AS_ID	0	MVRFCE の BGP AS ID（PE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_DLCI	0	フレーム リレー カプセル化対応の MVRFCE インターフェイスに接続する PE の DLCI 値（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_EIGRP_AS_ID	0	MVRFCE の EIGRP AS ID（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Intf	0	MVRFCE のインターフェイスに接続する PE の名前（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Intf_Address	0	MVRFCE インターフェイスに接続する PE に割り当てる IP アドレス（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Intf_Encap	0	MVRFCE インターフェイスに接続する PE 対応のカプセル化（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Intf_Name	0	MVRFCE インターフェイスに接続する PE の名前（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Intf_Type	0	MVRFCE インターフェイスの PE 接続のインターフェイス タイプ（MPLS リンクに MVRFCE が含まれる場合）。
PE_FACING_MVRFCE_OSPF_Process_ID	0	MVRFCE の OSPF プロセス ID（PE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_Tunnel_Src_Addr	0	GRE カプセル化対応の MVRFCE インターフェイスに接続する PE のトンネル ソース アドレス（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_VCD	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する PE の VCD 値（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_VCI	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する PE の VCI 値（MPLS リンクに MVRFCE が含まれる場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PE_Facing_MVRFCE_VLAN_ID	0	イーサネット カプセル化対応の MVRFCE インターフェイスに接続する PE の VLAN ID（MPLS リンクに MVRFCE が含まれる場合）。
PE_Facing_MVRFCE_VPI	0	ATM カプセル化対応の MVRFCE インターフェイスに接続する PE の VPI 値（MPLS リンクに MVRFCE が含まれる場合）。
PE_Intf_Address	0	PE インターフェイスに割り当てられる IP アドレス。
PE_Intf_Address_IPV6	0	アドレス ファミリが IPv6 の場合、これは、インターフェイスの IP アドレスを指定します。
PE_Intf_Desc	0	PE インターフェイスのインターフェイスの説明。
PE_Intf_Encap	0	PE インターフェイスのカプセル化。
PE_Intf_Name	0	PE インターフェイスの名前。
PE_Intf_Shutdown	0	PE インターフェイスのシャットダウン フラグ。
PE_IS_Cable_Modem_Maintenance_Interface	0	インターフェイスがメンテナンス インターフェイスかどうかを示すフラグ。
PE_MVRFCE_Bandwidth_Metric_For_Redistribution	0	EIGRP の再配布の帯域幅メトリック（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_BGP_AS_ID	0	PE の BGP AS ID（PE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_Delay_Metric_For_Redistribution	0	EIGRP の再配布の遅延メトリック（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_EIGRP_AS_ID	0	PE の EIGRP AS ID（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_IP_Unnumbered	1	PE と MVRFCE のリンクに番号を付けないようにするかどうか示すフラグ（MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_Loading_Metric_For_Redistribution	0	EIGRP の再配布のロード メトリック（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PE_MVRFCE_MTU_Metric_for_redistribution	0	EIGRP の再配布の MTU メトリック（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_NBR_ALLOW_AS_IN	0	AllowASIn フラグ（PE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_NBR_AS_OVERRIDE	0	ASOverride フラグ（PE と MVRFCE の間のルーティング プロトコルが BGP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_Ospf_Area_Number	0	OSPF エリア番号（PE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_OSPF_Process_ID	0	PE の OSPF プロセス ID（PE と MVRCE の間のルーティング プロトコルが OSPF で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_Ospf_Route_Policy	0	設定する OSPF ルートの再配布ポリシーの名前（MPLS リンクに PE_MVRFCE が含まれる場合）。
PE_MVRFCE_Reliability_Metric_For_Redistribution	0	EIGRP の再配布の信頼性メトリック（PE と MVRFCE の間のルーティング プロトコルが EIGRP で、MPLS リンクに MVRFCE が含まれる場合）。
PE_MVRFCE_Routing_Protocol	0	PE と MVRFCE の間のルーティング プロトコル（MPLS リンクに MVRFCE が含まれる場合）。
PE_OSPF_PROCESS_ID	0	PE の OSPF プロセス ID（CE と PE の間のルーティング プロトコルが OSPF の場合）。
PE_Tunnel_Src_Addr	0	GRE カプセル化対応の PE のトンネル ソース アドレス。
PE_VCD	0	ATM カプセル化対応の PE の VCD 値。
PE_VCI	0	ATM カプセル化対応の PE の VCI 値。
PE_Vlan_ID	0	イーサネット カプセル化対応の PE の VLAN ID。
PE_VPI	0	ATM カプセル化対応の PE の VPI 値。
rd	0	VRF のルート識別子値。
RD_FORMAT	0	MPLS リンクで使用する RD 形式を定義します（RD_AS、RD_IPADDR など）。
RD_IPADDRESS	0	MPLS リンクで使用する RD_IPADDRESS 値を定義します（RD 形式が RD_IPADDRESS の場合）。
Redistribute_Connected	0	接続済みのルートを PE の BGP に再配布するかどうかを示すフラグ。

表 9-3　MPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
Redistribute_Connected_IPV6	0	接続済みのルートを PE の BGP に再配布するかどうかを示すフラグ（アドレス ファミリが IPv6 の場合）。
Redistribute_Static	0	スタティック ルートを PE の BGP に再配布するかどうかを示すフラグ。
Redistribute_Static_IPV6	0	スタティック ルートを PE の BGP に再配布するかどうかを示すフラグ（アドレス ファミリが IPv6 の場合）。
Redistributed_Protocol	1	再配布するルーティング プロトコルのリスト。
Rip_Metrics	0	RIP に関連付けられている再配布のメトリック。
Routes_To_Reach_Other_Sites	2	CE に配置するスタティック ルートを指定する 1 つ以上の IP アドレスのリスト）。
vrfName	0	VRF の名前。

表 9-4 に、Prime Provisioning テンプレートから使用できる L2VPN リポジトリ変数の概要を示します。

表 9-4　L2VPN リポジトリ変数

リポジトリ変数	ディメンション	説明
AC_Loopback_Address	0	PE ループバック アドレス（別名、ルータ ID）。
CARD_TYPE	0	サービスにイーサネット アクセスが実装されているかどうかに基づき、NPE または UNI インターフェイスを示します。
CE_DLCI	0	フレーム リレー カプセル化対応の CE の DLCI 値。
CE_Encap	0	CE インターフェイスのカプセル化。
CE_Intf_Desc	0	CE インターフェイスのインターフェイスの説明。
CE_Intf_Main_Name	0	CE インターフェイスのメジャー インターフェイス名。
CE_Intf_Shutdown	0	CE インターフェイスのシャットダウン フラグ。
CE_VCD	0	ATM カプセル化対応の CE の VCD 値。
CE_VCI	0	ATM カプセル化対応の CE の VCI 値。
CE_Vlan_ID	0	イーサネット カプセル化対応の CE の VLAN ID。
CE_VPI	0	ATM カプセル化対応の CE の VPI 値。
L2VPNCLECeFacingEncapsulation	0	UNI のカプセル化。

表 9-4　L2VPN リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
L2VPNCLECeFacingInterfaceName	0	UNI の名前。
L2VPNCLEPeFacingEncapsulation	0	NNI のカプセル化（常に dot1q である必要があります)。
L2VPNCLEPeFacingInterfaceName	1	NNI（アップリンク）の名前（リング トポロジの場合、配列であるため、1 より大きい数を使用できます)。
L2VPNDFBIT_SET	0	ビット セットをフラグメント化しないことを示します（L2TPv3 の場合のみ)。
L2VPNDynamicModeUseDefaults	0	Prime Provisioning デフォルト値を使用したダイナミック セッション設定（L2TPv3 の場合のみ)。
L2VPN_intf_main_name	1	CE または PE ポートのメイン インターフェイス名。
L2VPNIP_PMTU	0	トンネリングされたトラフィックに対しパス MTU のディスカバリをイネーブルにします（L2TPv3 の場合のみ)。
L2VPNIP_TOS	0	トンネリングされたパケットの IP ヘッダー内の TOS バイトの値を設定するか、内部 IP ヘッダーの TOS バイト値を反映させます（L2TPv3 の場合のみ)。
L2VPNIP_TTL	0	IP ヘッダー内の存続可能時間バイトの値を設定します（L2TPv3 の場合のみ)。
L2VPNL2TP_CLASS_NAME	0	デフォルトの L2TP クラス名を上書きする L2TP クラス名（L2TPv3 の場合のみ)。
L2VPNL2TPv3Sequence	0	疑似回線内でのデータ パケットのシーケンス処理がイネーブルにされる方向を指定します（L2TPv3 の場合のみ)。
L2VPNLocalCookieHighValue	0	ピア PE が着信 L2TP パケットのクッキー フィールドに組み込む必要のある値の最終 4 バイトを指定します（L2TPv3 の場合のみ)。
L2VPNLocalCookieLowValue	0	ピア PE が着信 L2TP パケットのクッキー フィールドに組み込む必要のある値の先頭 4 バイトを指定します（L2TPv3 の場合のみ)。
L2VPNLocalCookieSize	0	着信 L2TP パケットのクッキー フィールドのサイズ（0、4、または 8）を指定します（L2TPv3 の場合のみ)。
L2VPNLocalHostName	0	L2VPN エンドツーエンド ワイヤでリモート N-PE とピアの関係にある N-PE のホスト名。
L2VPNLocalLoopback	0	L2VPN エンドツーエンド ワイヤでリモート N-PE とピアの関係にある N-PE のループバック アドレス。
L2VPNLocalSessionId	0	ローカル L2TPv3 セッションの ID を指定します（L2TPv3 の場合のみ)。

表 9-4　L2VPN リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
L2VPNLocalSwitchLoopBack1	1	ローカル スイッチの loopback1（L2TPv3 の場合のみ）。
L2VPNLocalSwitchLoopBack2	1	ローカル スイッチの loopback2（L2TPv3 の場合のみ）。
L2VPNRemoteCookieHighValue	1	この PE が着信 L2RP パケットのクッキー フィールドに組み込む必要のある値の最終 4 バイトを指定します（L2TPv3 の場合のみ）。
L2VPNRemoteCookieLowValue	1	この PE が着信 L2RP パケットのクッキー フィールドに組み込む必要のある値の先頭 4 バイトを指定します（L2TPv3 の場合のみ）。
L2VPNRemoteCookieSize	1	発信 L2TP パケットのクッキー フィールドのサイズ（0、4、または 8）を指定します（L2TPv3 の場合のみ）。
L2VPNRemoteHostName	0	L2VPN エンドツーエンド ワイヤのコンテキストで N-PE とピアの関係にあるリモート N-PE のホスト名。
L2VPNRemoteLoopback	0	L2VPN エンドツーエンド ワイヤのコンテキストで N-PE とピアの関係にあるリモート N-PE のループバック アドレス。
L2VPNRemoteSessionID	1	リモート L2TPv3 セッションの ID を指定します（L2TPv3 の場合のみ）。
L2VPNSessionSetupMode	0	L2TPv3 セッションの設定方法（スタティックまたはダイナミック）を定義します（L2TPv3 の場合のみ）。
L2VPNTransportMode	0	L2TPv3 データの転送方法（フレーム リレーでは、DLCI またはポート。ATM では、VP または VC）を定義します（L2TPv3 の場合のみ）。
L2VPNUniMajorInterfaceName	0	UNI のメイン インターフェイス名。
L2VPNVcId	0	L2TPv3 または AToM トンネルの仮想回線 ID。
PE_DLCI	0	フレーム リレー カプセル化対応の PE の DLCI 値。
PE_Encap	0	PE インターフェイスのカプセル化。
PE_Intf_Desc	0	PE インターフェイスのインターフェイスの説明。
PE_Intf_Main_Name	0	PE インターフェイスのメジャー インターフェイス名。
PE_VCD	0	ATM カプセル化対応の PE の VCD 値。
PE_VCI	0	ATM カプセル化対応の PE の VCI 値。
PE_Vlan_ID	0	イーサネット カプセル化対応の PE の VLAN ID。
PE_VPI	0	ATM カプセル化対応の PE の VPI 値。

表 9-4　L2VPN リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
PseudoWire_Class_Type_Of_Core	0	L2VPN のプロビジョニングで経由するサービス プロバイダーのコア タイプ。
Uni_Aging	0	ポート セキュリティ テーブル内に MAC アドレスを保持できる時間の長さ。
Uni_Cdp_Enable	0	Cisco Discover Protocol（CDP）でレイヤ 2 トンネリングをイネーブルまたはディセーブルにするためのフラグ。
Uni_Cdp_Threshold	0	CDP プロトコルでインターフェイスがシャットダウンされる前に受信する 1 秒あたりのパケットの数。
Uni_Mac_Address	0	ポート セキュリティで許可する MAC アドレスの数。
Uni_Port_Security	0	UNI インターフェイスでセキュリティをイネーブルまたはディセーブルにするためのフラグ。
Uni_Protocol_Tunnelling	0	UNI インターフェイスで、レイヤ 2 のブリッジ プロトコル データ ユニット（BPDU）をイネーブルまたはディセーブルにするためのフラグ。
Uni_Recovery_Interval	0	UNI ポートをリカバリする前に待機する時間。
Uni_Shutdown	0	User Network Interface（UNI; ユーザ ネットワーク インターフェイス）をシャットダウンするかどうかを示すフラグ。
Uni_Speed	0	UNI リンク速度の値。
Uni_Stp_Enable	0	スパニングツリー プロトコル（STP）でレイヤ 2 トンネリングをイネーブルまたはディセーブルにするためのフラグ。
Uni_Stp_Threshold	0	STP でレイヤ 2 トンネリングをイネーブルまたはディセーブルにするためのフラグ。
Uni_Violation_Access	0	ポート セキュリティ違反の検出時に実行されるアクション。
Uni_Vtp_Enable	0	VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）でレイヤ 2 トンネリングをイネーブルまたはディセーブルにするためのフラグ。
Uni_Vtp_Threshold	0	VTP でレイヤ 2 トンネリングをイネーブルまたはディセーブルにするためのフラグ。

表 9-5 に、Prime Provisioning テンプレートから使用できる VRF リポジトリ変数の概要を示します。

表 9-5　VRF リポジトリ変数

リポジトリ変数	ディメンション	説明
Address_Family	0	サービス要求のアドレッシング スキーム。
Cerc_Hub_RT	0	ハブ ルート ターゲットの Customer Edge Routing Community（CERC; カスタマー エッジ ルーティング コミュニティ）。
Cerc_Spoke_RT	0	スポーク ルート ターゲットの CERC。
Export_Map	0	VRF に関連付けられているエクスポート マップの名前。
Export_RT_List	0	VRF からエクスポートする 1 つ以上の Route Target（RT; ルート ターゲット）。
Import_Map	0	VRF に関連付けられているインポート マップの名前。
Import_RT_List	0	VRF にインポートする 1 つ以上の RT。
Max_Routes	0	VRF にインポートできるルートの最大数。
Max_Threshold	0	VRF にインポートできるルートの最大数のパーセント値。
PE	0	プロバイダー エッジ（PE）デバイスの名前。
PE_BGP_AS	0	PE デバイスの BGP 自律 ID。
RD	0	VRF のルート識別子値。
Vrf_Name	0	VRF の名前。

表 9-6 に、Prime Provisioning テンプレートから使用できる FlexUNI/EVC リポジトリ変数の概要を示します。

表 9-6　FlexUNI/EVC リポジトリ変数

リポジトリ変数	ディメンション	説明
ATMIMA_VCI	0	ATM/IMA サービスの仮想回線 ID。1 ～ 65535 の数字。
ATMIMA_VPI	0	ATM/IMA サービスの仮想パス識別子。0 ～ 255 の数字。
ATM_Encapsulation	0	ATM のカプセル化の種類 値は、AAL5 または AAL0 です。
AUG_MAPPING	0	True は SDH フレーミングを使用した場合、管理ユニット グループ マッピングを設定します。
AU_THREE_NUMBER	0	E1 回線の特定の管理ユニット タイプ 3（au 3）を設定するために使用します。1 ～ 3 の数字。

表 9-6　FlexUNI/EVC リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
BACKUP_VC_ID	0	プライマリ疑似回線に対してバックアップが設定されている、AToM のバックアップ仮想回線 ID。これは、2 つの N-PE 間の疑似回線コア タイプ接続に対してのみ適用できます。
CARD_TYPE	0	サービスにイーサネット アクセスが実装されているかどうかに基づき、NPE または UNI インターフェイスを示します。
CEM_CLASS_NAME	0	CEM クラス名。
CEM_GROUP_ID	0	コントローラの下の [CEM Group ID] は、コントローラと同じスロット/サブスロット/ポート情報を持つ CEM インターフェイスを作成します。これが取れる数は、E1 または T1 回線のどちらであるかによって異なります。
CEM_INTERFACE	0	CEM インターフェイスは、コントローラの下で CEM グループを設定した結果として作成されたインターフェイスです。CEM インターフェイスには、その親コントローラと同じスロット/サブ スロット/ポート情報があります。
CHANNELISATION_MODE	0	RAN サービスのチャネライゼーション モードを指定します。
CLOCK_SOURCE_TYPE	0	クロック ソースのタイプ。INTERNAL または LINE にすることができます。
CONFIG_BRIDGE_DOMAIN	0	USE_SVI がイネーブルの場合、値は true です。
CONTROLLER_NAME	0	コントローラの名前を指定します。
CONTROLLER_TYPE	0	CEM TDM サービスでデバイスが使用するコントローラのタイプ。。E1 または T1 ???? にすることができます
CORE_TYPE	0	コア タイプ接続。有効な値は、a）pseudowire、b）VPLS、c）Local connect です。
DEJITTERBUFFER	0	CEM コンフィギュレーション モードで、ネットワーク ジッタに使用されるバッファのサイズ。範囲は 1 ～ 500 ミリ秒です。
EVC_LINK_ID	0	EVC SR のトップ EVC リンク ID を返します。
EVC_NPE_HOSTNAME	0	EVC SR の NPE デバイス ホスト名。
EVC_SR_DESCRIPTION	0	EVC SR の説明。
EVC_SR_JOB_ID	0	EVC SR の SR JOB ID。

表 9-6　FlexUNI/EVC リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
EVC_UNI_DEVICE_ID	0	UNI デバイス ID。リンクごとに一意の MPID 値を設定できます。これは、CFM、IP SLA およびイーサネット OAM のサポートに使用されます。
FLEXUNI_ATM_VCD	0	ATM リンクに対し指定されている ATM VCD/サブインターフェイス値を返します。
FLEXUNI_ATM_VCI	0	ATM リンクに対し指定されている ATM VCI 値を返します。
FLEXUNI_ATM_VPI	0	ATM リンクに対し指定されている ATM VPI 値を返します。
FLEX_UNI_BD_NAME	0	IOS XR に対して使用されるブリッジ ドメイン名を返します。
FLEX_UNI_BG_NAME	0	IOS XR に対して使用されるブリッジ グループ名を返します。
FLEXUNI_ELINE_NAME	0	IOS XR に対して使用される p2p Eline 名を返します。
FLEXUNI_L2_GROUP_NAME	0	IOS XR に対して使用される L2VPN グループ名を返します。
FLEXUNI_PW_CLASS_NAME	0	IOS XR に対して使用される PW クラス要素名を返します。
FLEXUNI_REMOTE_HOSTNAME	0	リモート ピアのホスト名を返します。
FLEXUNI_REMOTE_LOOPBACK	0	リモート ピアのループバック IP アドレスを返します。
FLEXUNI_VLANTranslationCeVlan	0	VLAN 変換に提供された CE VLAN を返します。
FLEXUNI_VLANTranslationNode	0	この接続リンクで VLAN 変換が発生するノードの PE デバイスのロールを返します。
FLEXUNI_VLANTranslationOuterVlan	0	VLAN 変換に提供された外部 VLAN を返します。
FLEXUNI_VLANTranslationType	0	この添付ファイルのリンクに対して選択した VLAN 変換のタイプを返します。
IDLEPATTERN	0	それぞれの損失 CESoPSN データ パケットの置き換えに使用する日付のパターン。範囲は 16 進数の 0x00 ～ 0xFF です。????
IS_FLEX_UNI_LINK	0	EVC リンクが FLEXUNI リンクの場合、値は true です。
LOCAL_CONNECT_NAME	0	接続コマンドを使用する 2 つの Ethernet Flow Point（EFP; イーサネット フロー ポイント）間の接続の名前。FlexUNI/EVC がイネーブルになっている 2 つのリンクがある場合に限り適用できます。
MAC_ACL_NAME	0	MAC ACL 名。
MAC_ACL_RANGE	0	MAC ACL に対し指定される範囲値。

表 9-6　FlexUNI/EVC リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
MATCH_INNER_VLANS	0	入力フレームの内部 VLAN タグに対して一致する必要のある VLAN ID が格納されます。FlexUNI/EVC がイネーブルになっているリンクに対してのみ適用できます。
MATCH_OUTER_VLANS	0	入力フレームの外部 VLAN タグに対して一致する必要のある VLAN ID が格納されます。FlexUNI/EVC がイネーブルになっているリンクに対してのみ適用できます。
No_Cell_Packed	0	ATM サービスで使用されます。パケットにパッキングされるセルの最大数。2 ～ 28 の数字。
PAYLOADSIZE	0	CEM コンフィギュレーション モードで使用されるペイロード サイズ。有効な範囲は 32 ～ 1312 バイトです。
PE_DEVICE_PLATFORM	0	このリンクで使用されている N-PE デバイスのプラットフォーム タイプの情報を返します。
PE_INTERFACE_NAME	0	サービスのリンクの N-PE インターフェイス。これは、直接接続リンクの UNI_INTERFACE_NAME と同じです。
PE_OR_UNI_INTF_DESC	0	UNI インターフェイスの説明。
PUSH_INNER_VLAN_ID	0	別の Dot1q VLAN タグを入力フレームにプッシュします。FlexUNI/EVC が設定されているリンクに対してのみ適用できます。
PUSH_OUTER_VLAN_ID	0	Dot1q VLAN（外部）タグを入力フレームにプッシュします。FlexUNI/EVC が設定されているリンクに対してのみ適用できます。
PW_CLASS_NAME	0	現在のリンクのあらゆる IOS XR デバイスに使用される疑似回線クラスの名前を返します。
PW_TUNNEL_ID	0	N-PE の疑似回線クラスが設定されているトンネル ID（疑似回線コア タイプ選択に対してのみ適用可能）。
RAN_SERVICE_TYPE	0	RAN ervice タイプは SAToP_UNFRAMED または CESoPN_TIMESLOT のいずれかにすることができます。
SERVICE_INSTANCE_ID	0	FlexUNI/EVC がイネーブルのリンクの EFP に対応するサービス インスタンス ID（1 ～ 8000 の数値）。
SERVICE_INSTANCE_NAME	0	FlexUNI/EVC がイネーブルのリンクに対して設定されるサービス インスタンスに付与される EFP の名前。

表 9-6　FlexUNI/EVC リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
SONET_FRAME_TYPE	0	コントローラ フレーミング タイプを設定します。フレーミング タイプは SDH または SONET です。
SR_JOB_ID	0	現在のサービス要求の一意のジョブ ID を返します。
STD_UNI	0	UNI インターフェイスの標準 UNI ステータス。
STORM_CTL_BROADCAST_TRAFFIC	0	ストーム制御のブロードキャスト トラフィック値。
STORM_CTL_MULTICAST_TRAFFIC	0	ストーム制御のマルチキャスト トラフィック値。
STORM_CTL_UNICAST_TRAFFIC	0	ストーム制御のユニキャスト トラフィック値。
STS_MODE_TYPE		sts-1 モード タイプ ???vt-15
STS_ONE_NUMBER		sts-1 番号。1 ～ 3 の数字。
SYSTEM_MTU	0	使用するシステム MTU サイズ。
Sub_Interface	0	ATM 疑似回線 VC サービスのサブ インターフェイス番号。
TIME_SLOT	0	RAN でサービスを設定するタイム スロットの値または範囲を指定します。範囲は T1 コントローラ場合は 1 ～ 24 で、E1 コントローラの場合は 1 ～ 31 です。
TRANSLATE_INNER_VLAN_ID	0	変換対象のフレームのターゲット内部 VLAN ID（VLAN 変換）。FlexUNI/EVC がイネーブルになっているリンクに対してのみ適用できます。これは 1:2/2:2 タイプの変換に対して適用できます。
TRANSLATE_OUTER_VLAN_ID	0	変換対象のフレームのターゲット外部 VLAN ID（VLAN 変換）。FlexUNI/EVC がイネーブルになっているリンクに対してのみ適用できます。これは任意の種類の変換に対し適用できます（1:1/1:2/2:1/2:2）。
TUG_THREE_NUMBER	0	tug-3 番号を指定します。
TUG_TWO_NUMBER	0	tug-2 番号を指定します。
TUNNEL_CDP_DROP_THRESHOLD	0	使用する CDP DROP しきい値。
TUNNEL_STP_DROP_THRESHOLD	0	使用する STP DROP しきい値。
TUNNEL_VTP_DROP_THRESHOLD	0	使用する VTP DROP しきい値。
T_LINE_NUMBER	0	T1 回線番号を指定します。
Timer1	0	マイクロ秒単位の最初 MCPT タイマー値。500 ～ 10000 の数字。
Timer2	0	マイクロ秒単位の 2 つめの MCPT タイマー値。1000 ～ 10000 の数字。

表 9-6　FlexUNI/EVC リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
Timer3	0	マイクロ秒単位の 3 つめの MCPT タイマー値。1500 ～ 10000 の数字。
UNI_AGING	0	UNI のエージング値。
UNI_DEVICE_PLATFORM	0	このリンクで使用されている UNI デバイスのプラットフォーム タイプの情報を返します。
UNI_ENCAPSULATION_TYPE	0	UNI のカプセル化。有効な値は、a）Dot1Q Trunk、b）Dot1Q Tunnel、c）Access です。
UNI_INTERFACE_NAME	0	サービスのリンクの UNI。これは、直接接続リンクの PE_INTERFACE_NAME と同じです。
UNI_PORT_SECURITY	0	UNI のポート セキュリティ ステータス。
UNI_SHUTDOWN	0	UNI のシャットダウン ステータス。
UNI_SPEED	0	UNI の速度値。
UNI_VIOLATION_ACTION	0	使用する違反アクションのタイプ。
USER_DEFINED_ACL_NAME	0	接続回線で使用されるユーザ定義 ACL の名前。
UPE_FACING_INTERFACE_NAME	1	U-PE への NPE の NNI インターフェイスの名前を格納する、1 つまたは 2 つの要素の配列。アクセスがリングを介する場合は 2 つのインターフェイスが存在し、それ以外の場合は 1 つのインターフェイスのみ存在します。
USE_SPLIT_HORIZON	0	スプリット ホライズンがイネーブルの場合、値は true です。
Use_MCPT_Timer	0	ATM サービスで使用する MCPT タイマーを表示します。
VC_ID	0	疑似回線が 2 つの N-PE 間のコア接続タイプである AToM の仮想回線 ID。
VLAN_ID	0	リンク用の PE デバイス上のサービスに対応する VLAN ID。FlexUNI/EVC が設定されているリンクの場合、これは、N-PE でのみ適用できます。一方、MATCH_OUTER_VLANS は、そのリンクのサービスを表します。
VLAN_NAME	0	サービスのリンクに対応する VLAN ID に対し設定される VLAN 名。
VPLS_VPN_ID	0	VPLS コア タイプ接続の VPLS VPN ID。
VPN_ID	0	EVC SR に関連付けられている VPN 名。
VTG_NUMBER	0	仮想トリビュタリ グループ番号を指定します。

表 9-7 に、Prime Provisioning テンプレートから使用できる VPLS リポジトリ変数の概要を示します。

表 9-7　VPLS リポジトリ変数

リポジトリ変数	ディメンション	説明
CARD_TYPE	0	サービスにイーサネット アクセスが実装されているかどうかに基づき、NPE または UNI インターフェイスを示します。
VPLSBridgeDomainId	0	ブリッジ ドメインの ID 値。
VPLSCeEncapsulation	0	特定の VPLS リンクの CE インターフェイスのカプセル化。
VPLSCeInterfaceName	0	特定の VPLS リンクの CE インターフェイスの名前。
VPLSCeMajorInterfaceName	0	特定の VPLS リンクの CE のメジャー インターフェイスの名前。
VPLSCLECeFacingEncapsulation	0	CE に接続する特定デバイスのインターフェイスのカプセル化。
VPLSCLECeFacingInterfaceName	0	CE に接続する特定デバイスのインターフェイス名（リング トポロジの場合、配列のため、1 を超える数値を使用できます）。
VPLSCLEPeFacingEncapsulation	0	PE に接続する特定デバイスのインターフェイスのカプセル化。
VPLSCLEPeFacingInterfaceName	1	PE に接続する特定デバイスのインターフェイス名のリスト（リング トポロジの場合、配列のため、1 を超える数値を使用できます）。
VPLSDisableCDP	0	特定 VPLS リンク用の UNI において CDP をディセーブルにするかどうか指定するフラグ。
VPLSFilterBPDU	0	特定 VPLS リンク用の UNI において BPDU をフィルタリングするかどうか指定するフラグ。
VPLSPeEncapsulation	0	特定の VPLS リンクの PE インターフェイスのカプセル化。
VPLSPeInterfaceDescription	0	特定 VPLS リンクの PE インターフェイスに割り当てる説明。
VPLSPeInterfaceName	0	特定 VPLS リンクの PE インターフェイスの名前。
VPLSPeMajorInterfaceName	0	特定の VPLS リンクの PE のメジャー インターフェイスの名前。
VPLSPeNeighbors	1	特定の VPLS VPN に参加する PE POP のリスト。
VPLSPeVfiName	0	PE POP に存在する特定の VPLS インスタンスに割り当てる VFI 名。
VPLSPeVlanId	0	特定の VPLS リンクの PE に割り当てる VLAN ID。
VPLSPeVpnId	0	特定の VPLS VPN に割り当てる VPN ID。

表 9-7　VPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
VPLSSystemMTU	0	特定の VPLS リンク用の UNI に到着するパケットの最大 MTU 値。
VPLSTunnelCDPEnable	0	CDP パケットを、特定の VPLS リンクのリモート サイトにトンネリングするかどうかを指定するフラグ。
VPLSTunnelCDPThreshold	0	特定の VPLS リンク用の UNI で違反アクションが報告される前に、CDP プロトコルに対し割り当てるしきい値。
VPLSTunnelRecoveryInterval	0	シャットダウン シナリオからリカバリする UNI の間隔。
VPLSTunnelSTPEnable	0	STP パケットを、特定の VPLS リンクのリモート サイトにトンネリングするかどうかを指定するフラグ。
VPLSTunnelSTPThreshold	0	特定の VPLS リンク用の UNI で違反アクションが報告される前に、STP プロトコルに対し割り当てるしきい値。
VPLSTunnelVTPEnable	0	VTP パケットを、特定の VPLS リンクのリモート サイトにトンネリングするかどうかを指定するフラグ。
VPLSTunnelVTPThreshold	0	特定の VPLS リンク用の UNI で違反アクションが報告される前に、VTP プロトコルに対し割り当てるしきい値。
VPLSUniAging	0	特定の VPLS リンク用の UNI で設定されるエージング タイマー。
VPLSUniDuplex	0	特定の VPLS リンク用の UNI に割り当てる半二重。
VPLSUniMajorInterfaceName	0	特定の VPLS リンク用の UNI デバイスのメジャー インターフェイスの名前。
VPLSUniMaxMacAddress	0	特定の VPLS リンク用の UNI で学習できる Mac アドレスの最大数。
VPLSUniPortSecurity	0	特定の VPLS リンク用の UNI のポート セキュリティ オプション。
VPLSUniProtocolTunneling	0	プロトコルを特定の VPLS リンクのリモートサイトにトンネリングするかどうかを指定するフラグ。
VPLSUniSecureMacAddresses	1	特定の VPLS リンク用の UNI で学習できる Mac アドレスの明示リスト。
VPLSUniShutdown	0	特定の VPLS リンク用の UNI のシャットダウン フラグ。
VPLSUniSpeed	0	特定の VPLS リンク用の UNI に割り当てる速度。

表 9-7　VPLS リポジトリ変数 （続き）

リポジトリ変数	ディメンション	説明
VPLSUniViolationAction	0	特定の VPLS リンク用の UNI の違反アクション オプション。
VPLSUseNativeVlan	0	ネイティブ VLAN を特定 VPLS リンク用の UNI で使用するかどうかを指定するフラグ。

テンプレートのインポートとエクスポート

importExportTemplateDB ツールを使用して、Prime Provisioning データベースにテンプレートをインポート、およびこのデータベースからテンプレートをエクスポートできます。

（注）　**negate** テンプレートが存在する場合、negate テンプレートも、テンプレートのインポート時またはエクスポート時に、常に自動的にインポートまたはエクスポートされます。

適切な引数を指定することで、テンプレート データベース全体、またはその一部をインポートまたはエクスポートできます。このツールのパスは、**$PRIMEP_HOME/bin/importExportTemplateDB.sh** です。

次を入力します。

importExportTemplateDB.sh <*admin_user_id*> <*password*> [<*other_arguments*>]

ここで、

<*admin_user_id*> は、**admin** ロールを持つユーザのユーザ ID です。

<*password*> は、**admin** ロールを持つユーザのパスワードです。

<*other_arguments*> には、次の引数をスペースで区切って指定します。

-nooverwrite
データベース内の既存のテンプレートが上書きされないようにするために、この **nooverwrite** 引数の使用を選択する場合、この引数は、<*admin_user_id*> と <*password*> の後の 3 番めの位置に指定する必要があり、また、他のすべての引数の前に指定する必要があります。

（注）　デフォルト（**nooverwrite** は未指定）では、テンプレートは上書きされます。

-exp_db <*dest-dir*>
データベース内のすべてのテンプレートおよびデータ ファイルをエクスポートするには、この引数を使用します。<*dest-dir*> はエクスポート先の宛先ディレクトリです。

-imp_db <*src-dir*>
<*src-dir*> 内のすべてのファイルをデータベースにインポートするには、この引数を使用します。<*src-dir*> はインポート元のソース ディレクトリです。**exp_db** プロセスにより <*src-dir*> 内のファイルが作成されます。

-exp_template_folder <*src-folder-path*> <*dest-dir*>
データベース テンプレート フォルダとそのサブフォルダをエクスポートするには、この引数を使用します。<*src-folder-path*> はエクスポートするテンプレート フォルダのフル パスで、<*dest-dir*> はエクスポートしたファイルを配置するディレクトリです。

-imp_template_folder <*src-dir*> <*dest-folder*>
<*src-dir*> 内のすべてのファイルをデータベースにインポートするには、この引数を使用します。<*src-dir*> はインポートするソース ディレクトリで、<*dest-folder*> は宛先のインポート テンプレート フォルダです。

-imp_template <*srcfile*> <*dest-folder*> <*template-name*>
テンプレートをデータベースにインポートするには、この引数を使用します。<*srcfile*> はインポートするテンプレートのフル パスで、<*dest-folder*> は親フォルダのフル パスで、<*template-name*> はデータベースでのテンプレート名です。

-imp_datafile <*srcfile*> <*dest-template*> <*datafile-name*>
テンプレート データ ファイルをデータベースにインポートするには、この引数を使用します。<*srcfile*> はインポートするデータ ファイルのフル パスで、<dest-template> は親テンプレートのフル パスで、<*datafile-name*> はデータベースでのデータ ファイルの名前です。

-exp_template <*template-pathname*> <*output-file*>
データベース テンプレートをファイルにエクスポートするには、この引数を使用します。<*template-pathname*> はエクスポートするテンプレートのフル パスで、<*output-file*> は出力ファイル名です。

-exp_datafile <*datafile-pathname*> <*output-file*>
テンプレート データ ファイルをファイルにエクスポートするには、この引数を使用します。<*datafile-pathname*> はエクスポートするテンプレート データ ファイルのフル パスで、<*output-file*> は出力ファイル名です。

importExportTemplateDB.sh スクリプトを使用したテンプレート データのインポートに関する既知の問題

importExportTemplateDB.sh スクリプトを使用してインポートされたテンプレート データが、HTTPD または Prime Provisioning 処理が再開された後に、Template Manager GUI にしか表示されません。

回避策の 1 つとして、手動でテンプレートを作成します。これで、前にインポートしたすべてのテンプレートとデータ ファイルが表示されます。この回避策では、HTTPD または Prime Provisioning プロセスを再起動する必要はありません。

これを行う手順は次のとおりです。

ステップ 1　テンプレートおよびデータ ファイルをインポートします。

ステップ 2　Template Manager を調べ、それらが表示されているかどうかを確認します。

ブラウザをリフレッシュしてログイン/ログアウトしても、問題は解決されません。

ステップ 3　Template Manager で簡単なテンプレートを手動で作成します。

保存して、[Close] をクリックすると、[Template Manager] ウィンドウに、すべてのデータ、以前にインポートしたすべてのテンプレート、データ ファイルが表示されるようになります。

よくあるご質問

次の項では、Template Manager の問題の解決に役立つ質問と回答を示します。

文字列を分割する方法を教えてください

Prime Provisioning は、指定された文字列を分割し、指定されたデリミタに基づきサブストリングを返すことのできる、**substringToDelim()** 関数を提供しています。

構文：

substringToDelim (srcString, delimChar, 0/1)
ここで、

0 では、デリミタの前の文字列が返されます。
1 では、デリミタの後の文字列が返されます。

使用方法：**$b=$TMSystem.substringToDelim("10.11.230.145", ".230.145", "0")**

結果：**$b** の値は **10.11** です。**0** の代わりに **1** を指定すると、**$b** の値は **230.145** です。

指定した IP アドレスからアドレス情報を取得する方法を教えてください

Prime Provisioning は、指定した IP アドレスからアドレス、マスク、およびリバース マスクを取得できる関数を提供しています。

使用方法：

$TMSystem.getAddr ("10.33.4.5/30") では、10.33.4.5 が返されます。
$TMSystem.getMask ("10.33.4.5/30") では、255.255.255.252 が返されます。
$TMSystem.getReverseMask ("10.33.4.5/30") では、0.0.0.3 が返されます。
$TMSystem.getNetworkAddr ("10.33.4.5/30") では、10.33.4.4 が返されます。

$TMSystem.GetClassfulNetworkAddr ("10.33.4.5/30") では、10.0.0.0 が返されます。
$TMSystem.CurrentTimeInIOSFormat () では、hh:mm:ss day_of_month month_of_year year が返されます。

指定した IP アドレスからオクテットを取得する方法を教えてください

Prime Provisioning は、呼び出すとオクテットを返すことのできる関数を提供しています。

使用方法：

$TMSystem.getOctet1($ipAddr) では、**ipAddr の最初のオクテットが返されます。**
$TMSystem.getOctet2($ipAddr) では、**ipAddr** の 2 番めのオクテットが返されます。
$TMSystem.getOctet3($ipAddr) では、**ipAddr の 3 番めのオクテットが返されます。**
$TMSystem.getOctet4($ipAddr) では、**ipAddr** の 4 番めのオクテットが返されます。

テンプレートでサブテンプレートを呼び出す方法を教えてください

サブテンプレートは、メイン テンプレートで呼び出すことができます。呼び出し対象のサブテンプレートは、そのデータ ファイルを使用して呼び出す必要があります。変数を、サブテンプレート型として宣言します。サブテンプレートの場所は、データ ファイルで指定します。

使用方法：テンプレート本体で、サブテンプレートを次のように宣言します。

$a.callWithDatafile("data1")

ここで、

変数 **a** は、サブテンプレート型変数として宣言します。

data1 はサブテンプレートのデータ ファイルの名前です。

データ ファイルで、サブテンプレート パスのパスを指定します。

2 つの文字列を連結する方法を教えてください

文字列の連結は簡単です。

たとえば、次のように入力します。

$a=vpnsc と **$b=properties**
を連結します。**${a}${b}** により、これらの 2 つの文字列が連結され、**vpnscproperties** が結果として返されます。
また、**${a}_${b}** では、**vpnsc_properties** が結果として返されます。

文字列を整数に変換する方法、および IP アドレスの最後のオクテットを 1 だけ増加させる方法を教えてください

次のコードを使用することで、IP アドレスの最後のオクテットを増加させることができます。

```
#set($d=$TMSystem.getOctet1($c))
#set($e=$TMSystem.getOctet2($c))
#set($f=$TMSystem.getOctet3($c))
#set($g=$TMSystem.getOctet4($c))
#set($valueOfString = $g)
```

```
#set($valueOfCharsCount = $valueOfString.length() - 1)
#set($valueOfVector = "0123456789")
#set($valueOfBase = 1)
#set($valueOfInt = 0)
#foreach($valueOfCharIterator in $valueOfCharsCount..0)
#set($valueOfChar=$valueOfString.charAt($valueOfCharIterator).toString())
#set($valueOfInt = $valueOfInt +$valueOfVector.indexOf($valueOfChar) * $valueOfBase)
#set($valueOfBase = $valueOfBase * 10)
#end
#set($valueOfInt = $valueOfInt+1)
```

増加値は **$d.$e.$f.$valueOfInt** です。

入れ子にした if ステートメントは使用できますか

if ステートメントは入れ子にできます。**if** ステートメントを入れ子にする場合、字下げを適切に行う必要があります。次のコードは、入れ子にした **if** ステートメント、**elseif** ステートメント、および **if** 節での比較の使用方法を示しています。

```
#if($a=="a") // here: string comparison is made
  --
    #if($b || $d) // here: $b and $d are the Boolean expressions.|| equals OR and && equals AND
       --
       #if(!$c) // here: $c can be integer, string, or Boolean.
                  ---
            #if($p<10)// here: $p is a integer.
            #elseif($p==10)
            #end
      #end
   #end
#end
```

基本的な算術演算を実行する方法を教えてください

Velocity Template Language（VTL）は、テンプレートで使用できる組み込みの算術関数をサポートしています。これらは set ディレクティブで使用します。

使用方法：

```
#set($a = $b + 3)
#set($a = $b - 6)
#set($a = $b * 6)
#set($a = $b / 5)
#set($a = $b % 2)
```

（注）　VTL で算術演算を実行する場合、整数のみ有効です。

2 次元配列からデータを取得する方法、および $velocityCount の使用方法を教えてください

velocity.properties ファイルで指定されている、ループ カウンタ変数参照のデフォルト名は **$velocityCount** です。デフォルトでは、このカウンタは **1** から始まりますが、これを、**$PRIMEP_HOME/resources/webserver/tomcat/shared/lib/velocity-dep-***VelocityVersion***.jar**（現在の *VelocityVersion* は 1.3.1-rc2）にある **velocity.properties** ファイルで **0** または **1** に設定できます。関連する設定を次に示します。

directive.foreach.counter.name=velocityCount
directive.foreach.counter.initial.value=1

get($i) を使用することで、配列からデータを取得できます。

$i は $velocityCount です。

次の例は、**get()** メソッドの使用方法を示しています。

使用方法：
```
#foreach ($Acl in $ACL-List)
        #set ($i = $velocityCount)
    #foreach ($protocol in $Protocol-Lists.get($i))
    #set ($j = $velocityCount)
      access-list $Acl permit $protocol $Source-IP.get($i).get($j)
    #end
    #end
```

ここで、

$ACL-List は 1 次元配列です。
$Protocol-Lists および **$Source-IP** は 2 次元配列です。

ここでは、$velocityCount はデフォルトの **1** に設定されます。必要な場合は、velocity.properties でこれを変更できます。

値の代わりに $a を出力する方法を教えてください

変数 **a** の値が定義されている場合でも、文字 \ を使用することで、値を処理せずに出力できます。

使用方法：

$a が定義されている場合、**\$a** により **$a** が出力されます。**$a** が定義されていない場合、これにより **\$a** が出力されます。

#include() と #parse() の違いについて教えてください

#include("velocity.txt") ディレクティブを使用すると、ファイルをインポートし、そのファイルを定義済みの場所に格納できます。このファイルの内容を、テンプレート エンジンは使用できます。**#include** を使用することで、*.vm ファイルも呼び出すことができます。ファイルの名前は、変数で渡すこともできます。セキュリティ上の理由により、ファイルは **TEMPLATE_ROOT**（vob/ntg/dev/resources/templatesystem）の下位に格納する必要があります。

#parse("velocity.vm") ディレクティブを使用すると、VTL を含むローカル ファイルをインポートできます。Velocity により、VTL が解析され、指定されたテンプレートがレンダリングされます。**#parse** で参照するテンプレートは、**TEMPLATE_ROOT** の下位に格納する必要があります。**#parse** ディレクティブは、1 つの引数のみ受け取ります。VTL テンプレートには、テンプレートを参照する **#parse** ステートメントを含めることができ、参照先のテンプレートにも **#parse** ステートメントを含め

ることができます。
$PRIMEP_HOME/resources/webserver/tomcat/shared/lib/velocity-dep-*VelocityVersion***.jar**（現在の *VelocityVersion* は 1.3.1-rc2）にある **velocity.properties** ファイルでは、**directive.parse.max.depth** プロパティのデフォルト値は 10 に設定されていますが、必要に応じて変更できます。

（注）　**velocity.properties** ファイルに **directive.parse,max.depth** プロパティが存在しない場合、デフォルト値は 10 に設定されます。

例：

TEMPLATE_ROOT 内の **velocity.vm** ファイルには、次の内容が含まれます。

```
welcome to the parse file
The count is $count
#set($count = $count - 1)
#set($cl-list="cl1","cl2","cl3")
#foreach($i in $cl-list)
ipcommunity-list permit $i 30:20
#end
The count is $count
returning from parse
```

テンプレート本体には、次の内容が含まれます。

```
#set($count=8)
#include("velocity.vm")
---------------------------
#parse("velocity.vm")
---------------------------
welcome back to template
The value of count is $count

The following O/P is obtained:
welcome to the parse file
The count is $count
#set($count = $count - 1)
#set($cl-list="cl1","cl2","cl3")
#foreach($i in $cl-list)
ipcommunity-list permit $i 30:20
#end
The count is $count
returning from parse
---------------------------
welcome to the parse file
The count is 8
ipcommunity-list permit cl1 30:20
ipcommunity-list permit cl2 30:20
ipcommunity-list permit cl3 30:20
The count is 7
returning from parse
---------------------------
welcome back to template
The value of count is 7.
```

（注）　前の例では、変数が **#include** ディレクティブではなく、**#parse** ディレクティブで解析されていることが明確に示されています。

マクロとはどのようなもので、どのように使用しますか

macro ディレクティブは、関数とほとんど同じです。マクロには、繰り返し呼び出すことができる、一連のステートメントが含まれます。

例：

```
#macro(community $CL $bgp-list)
   #foreach($bgp in $bgp-list)
      ip $CL standard permit $bgp
   #end
#end

#set($bgp_list ="20:10","30:10","40:10","50:10")
#set($CL = "community-list")

#community($CL $bgp_list)
```

ここでは、マクロ名として **community** を定義しています。このマクロは、**$CL** と **$bgp-list** の 2 つの引数を受け取ります。最終行で、このマクロを呼び出しています。

前のテンプレートの出力を次に示します。

```
ip community-list standard permit 20:10
ip community-list standard permit 30:10
ip community-list standard permit 40:10
ip community-list standard permit 50:10
```

範囲演算子とはどのようなもので、どのように使用しますか

範囲演算子は、**#set** ステートメントおよび **#foreach** ステートメントと組み合わせて使用できます。範囲演算子は、整数が格納されたオブジェクト配列を生成するために使用します。範囲演算子は、次のように、**n..m** という構文を使用します。

例：

```
#set($a=0..2)
#foreach($b in $a)
    $b
#end
#foreach($c in -2..2)
$c
#end
```

特殊文字を含む文字列を分割する方法を教えてください

```
#foreach ($i in $PE_Intf_Name.split('\.')) $i #end
```

ここでは、最初の繰り返しで、**$i** にピリオドの前の文字列が格納され、2 回めの繰り返しで、**$i** にピリオドの後の文字列が格納されます。

リポジトリ変数の使用方法を教えてください

リポジトリ変数は、データ ファイルで選択できます。データ ファイルとともにテンプレートがサービス要求に関連付けられていて、サービス要求が展開されると、リポジトリ変数に値が代入されます。

変数を動的 URL として使用する方法を教えてください

動的 URL として宣言された変数では、次の方法で URL を呼び出すことができます。

callUrl(String S)

例：**$a.callUrl("http://www.cisco.com")**

その他にも例はありますか

次の例を参照してください。

- 「文字列の使用方法」（P.9-65）
- 「マクロの使用方法」（P.9-67）
- 「サブテンプレートの使用方法」（P.9-67）

文字列の使用方法

テンプレートの本体に次が含まれています。

```
## This example illustrates the usage of strings

#set($a="Fast")
#set($b="ethernet")
interface ${a}_${b}

#foreach ($i in $PE_Intf_Name.split('\.'))
$i
#end

#set($c="10.11.230.145")
#set($b=$TMSystem.substringToDelim($c, ".230.145", "0"))
interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address ${b}.20.34 255.255.255.255
no ip directed-broadcast

#set($b=$TMSystem.substringToDelim($c, ".230.145", "1"))
interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
```

```
ip address 20.45.${b} 255.255.255.255
no ip directed-broadcast

#set($c="10.33.4.5/30")
#set($d=$TMSystem.getAddr($c))
The Address of $c is $d
#set($d=$TMSystem.getMask($c))
The mask of $c is $d
#set($d=$TMSystem.getReverseMask($c))
The Reverse mask of $c is $d
#set($d=$TMSystem.getNetworkAddr($c))
The network address of $c is $d

#set($e=$TMSystem.currentTimeInIOSFormat())
The current time in IOS format is : $e

-----------------------------------------------------
getting the octets from the ipaddress
#set($c="10.33.4.5")
#set($e=$TMSystem.getOctet1($c))
The first Octet of $c is $e
#set($e=$TMSystem.getOctet2($c))
The second Octet of $c is $e
#set($e=$TMSystem.getOctet3($c))
The third Octet of $c is $e
#set($e=$TMSystem.getOctet4($c))
The fourth Octet of $c is $e
```

変数は、必要に応じて、文字列型、整数型、またはサブテンプレート型として宣言します。

上のテンプレート本体の出力を次に示します。

```
interface Fast_ethernet

10
11
12
13

interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address 10.11.20.34 255.255.255.255
no ip directed-broadcast

interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address 20.45.230.145 255.255.255.255
no ip directed-broadcast

The Address of 10.33.4.5/30 is 10.33.4.5
The mask of 10.33.4.5/30 is 255.255.255.252
```

The Reverse mask of 10.33.4.5/30 is 0.0.0.3
The network address of 10.33.4.5/30 is 10.33.4.4

The current time in IOS format is: 00:17:01 21 Aug 2006

----
getting the octets from the ipaddress
The first Octet of 10.33.4.5 is 10
The second Octet of 10.33.4.5 is 33
The third Octet of 10.33.4.5 is 4
The fourth Octet of 10.33.4.5 is 5

マクロの使用方法

テンプレートの本体に次が含まれています。

```
## This example illustrates the usage of macro

#macro(community $CL $bgp-list)
#foreach($bgp in $bgp-list)
ip $CL standard permit $bgp
#end
#end

#set($bgp_list = "20:10","30:10","40:10","50:10")
#set($CL = "community-list")

#community($CL $bgp_list)
```

以下が出力されます。

```
ip community-list standard permit 20:10
ip community-list standard permit 30:10
ip community-list standard permit 40:10
ip community-list standard permit 50:10
```

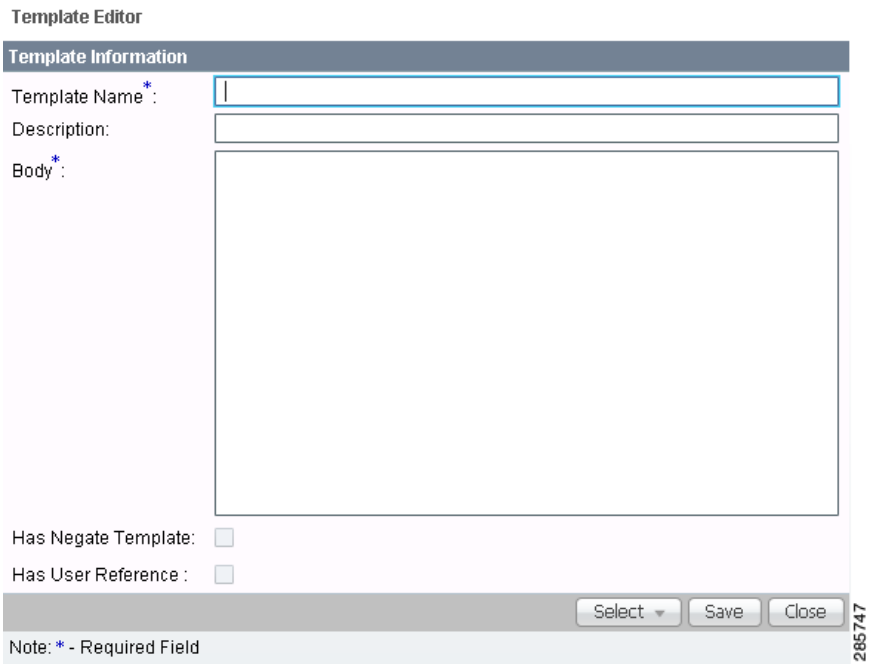
サブテンプレートの使用方法

テンプレートの本文に以下が含まれています。

```
## This example illustrates the usage of the sub-template

$a.callWithDatafile("data1")
```

図 9-14　テンプレート データ ファイル エディタ



変数 **a** は、サブテンプレート型として宣言されています。ここで指定されているデータ ファイル、**data** は、テンプレート **a** のデータ ファイルである必要があり、存在している必要があります。メイン テンプレートのデータ ファイルで、サブテンプレートのパスを指定します。

メイン テンプレートのデータ ファイルで指定するサブテンプレートのパスは、同じディレクトリにすること、または別のディレクトリにすることができます。

CHAPTER 10

モニタリング

この章では、モニタリング アクティビティについて説明します。次の事項について説明します。

ping

ping を使用して、Prime Provisioning は VPN 接続をモニタリングします。つまり、VPN を構成するさまざまなエッジ デバイス間の接続を確認します。

（注） ping 機能は、IOS XR を稼働しているデバイスではサポートされません。

これを実現するために、これらのデバイスの間で一連の ping を実行できます。ping には次の利点があります。

- サービスは独立しているため、MPLS アプリケーションの機能監査に使用できる。
- サービスが機能しているかどうかに関係なく、サービスの機能監査を行わずに確立できる。
- VPN サービス展開よりも前に CPE における IPv4 接続の検証に使用できる。

ただし、ping は次のことを行いません。

- ping は、ICMP トラフィックがブロックされている環境、たとえば、アクセス リストですべての ICMP トラフィックが拒否される Cisco IOS ルータでは機能できない。
- ping は、接続問題があることだけを通知する。そのため、任意のサービス固有の情報を提供しません。接続の問題は、デバイス障害、設定ミスなど、ping では識別できない多くの問題が原因である可能性があります。
- ルータののカスタマー側（または、内部あるいは非セキュア）インターフェイスの背後にある即時のサブネットのみがサポートされます。キャンパス サブネットはサポートできません。

Ping GUI は、MPLS サービス要求で想定されるすべての ping をサポートします。この項では、MPLS サービス要求に ping を実行する例を示します。

（注） Prime Provisioning には役立つ可能性のあるコンポーネントの Prime Diagnostics があります。*『Cisco Prime Provisioning 6.3 User Guide』* を参照してください。

[Inventory] > [Device Tools] > [Ping] を選択します。[Services] ウィンドウが表示されます。

[Type] フィールドに [MPLS] が示されます。手順は次のとおりです。

ステップ 1　ping パラメータを設定する各行の横にあるチェックボックスをオンにします。

ステップ 2　[Configure Ping Parameters] ボタンをクリックして、イネーブルにします。

[MPLS Parameters] ウィンドウが表示されます。

次に入力し、[Start Ping] をクリックします。

- [Ping Type: Do PE to CE Ping]：このオプション ボタンを選択すると、MPLS VPN リンクを形成するすべての PE CE ペアに対して VRF ping が行われます。この ping に対する IP アドレスはリンクのエンドポイント アドレスです。たとえば、MPLS サービス要求に 2 つのリンク PE1<>CE1 と PE2<>CE2 があるとします。この選択の場合、（PE1, CE1）、（PE2, CE2）、（PE1, CE2）、および（PE2, CE1）という 4 つの VRF ping が開始されます。この選択が選ばれると、[Start Ping] をクリックした後に、に直接移動し、結果のページを受け取ります。
- [Ping Type: Do CE to CE Ping]：このオプション ボタンが選択されると、サービス要求にエンドポイントを作成するすべての CE 間で ping が行われます。この選択が選ばれると、[Start Ping] をクリックした後に、ステップ 3 に移動します。
- [Two-way Ping]（デフォルトでは使用不可で選択されていない）：このチェックボックスは、[Do CE to CE Ping] を選択した場合にのみ使用できます。デバイス 1 からデバイス 2 への ping が発生する場合、このチェックボックスがオンにされていると、デバイス 2 からデバイス 1 への ping も発生します。
- [Packet Repeat Count]（デフォルトは 5）：この値は、ping に使用する ICMP パケットの数を示します。
- [Datagram size]（デフォルトは 100）：この値は、ping に使用する ICMP のパケット サイズです。

ステップ 3　[Do CE to CE Ping] に [MPLS CE Selection] ウィンドウが表示されます。

ステップ 4　CE を選択する各行の横にあるチェックボックスをオンにします。

ステップ 5　[Start MPLS CE Ping] をクリックして、イネーブルにします。

[MPLS Ping Test Results] ウィンドウを受け取ります。

ウィンドウ下部のボタンを次に示します。

- [Redo Ping]：このボタンをクリックすると、すべての ping が再開します。使用されるパラメータは前回の要求で指定されたものと同じです。
- [View Job Logs]：このボタンをクリックすると、ping を実行するために作成されたすべての Prime Provisioning のジョブのログを受け取ります。ping アプリケーションは、選択されたサービス要求ごとに 1 つのジョブを作成します。
- [Refresh]：選択的に更新するには、[Auto Refresh] ボタンをオフにして、結果を更新したいときにこのボタンをクリックします。
- [Close]：現在の ping 要求を閉じるには、このボタンをクリックします。[Monitoring] ページに戻ります。

（注）　カラム ヘッダが青色の場合、そのカラム ヘッダをクリックすると、カラムをソートできます。

ステップ 6　[Close] をクリックしてこの ping セッションを終了します。

SLA

サービス レベル契約（SLA）は、顧客にサービス プロバイダーが提供するサービスのレベルを定義します。パフォーマンスは SLA サーバを介してモニタされます。Prime Provisioning は、サービス保証エージェント（SA エージェント）デバイスをサポートする Cisco IOS ルータで、SLA をプロビジョニング、収集、およびモニタすることにより、サービス関連のパフォーマンス基準をモニタします。SLA をプロビジョニングし、各 SLA の統計情報を収集するには、データ収集タスクで最低限のユーザ入力が必要です。

（注）　SLA 機能は、IOS XR を稼働しているデバイスではサポートされません。

SLA 収集タスクは、関連パフォーマンス データを収集、これを永続的に保存、集約し、役に立つレポートを提供します。SLA 収集タスクは、デバイスの SA Agent MIB から収集します。Prime Provisioning は SA Agent MIB を 24 x 7 ベースの SLA パフォーマンスの監視に利用します。MIB を使用して、一般的なプロトコルのネットワーク トラフィックをモニタできます。

- Dynamic Host Configuration Protocol（DHCP）
- ドメイン ネーム システム（DNS）
- ファイル転送プロトコル（FTP）
- Hyper Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）
- Internet Control Message Protocol Echo（ICMP Echo）
- ジッタ（音声ジッタ）
- Transmission Control Protocol Connect（TCP Connect）
- User Datagram Protocol Echo（UDP Echo）。

（注）　SLA は Oracle をデータベースとして選択するかどうかとは関係なく、組み込み Sybase データベースを使用します。

（注）　SLA は、[Create]、[Delete]、[Enable Probes]、[Disable Probes]、[Enable Traps]、および [Disable Traps] の操作を自動的に行うことでタスクを作成し、それによって実際の操作を実行します。　タスクのステータスは、[Inventory] > [Task Manager] > [Logs] にナビゲートすることで表示できます。

この項では、SLA プローブの設定、SLA データの設定、およびこれらの SLA プローブに関する SLA レポートの表示方法を説明します。

「SLA を使用する前のセットアップ」（P.10-4）でセットアップ手順を実装してから、[Inventory] > [Device Tools] > [SLA] を選択します。

次に、[Inventory] > [Device Tools] > [SLA] を選択すると、次のいずれかを選択できるようになります。

- 「プローブ」（P.10-7）はデフォルトの選択肢です。
- 「レポート」（P.10-19）

SLA を使用する前のセットアップ

SLA は SNMP のアクティビティです。SNMP がイネーブルであり、ルータの SNMP 設定がリポジトリの設定と一致することを確認します。

SLA を [From MPLS CPE] または [From MPLS PE or MVRF-CE] を使用して作成する場合、サービスに関連付けられたサービス要求は [Deployed] 状態である*必要があります*。

SNMP の設定

Prime Provisioning を機能させるには、SNMP がカスタマー ネットワークの各 CPE デバイスで設定されている必要があります。Prime Provisioning で、SNMP は次を行うために使用されます。

- インターフェイス MIB からの収集
- SLA データをプロビジョニングと収集

SNMPv1/v2c と SNMPv3 の 2 つのセキュリティ モデルを使用できます。表 10-1 には、セキュリティ モデルとセキュリティ レベルの組み合わせが示されています。

表 10-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	説明
v1/v2c	認証なし / 暗号化なし	Community String	No	コミュニティ ストリングの照合を使用して認証します。
v3	認証なし / 暗号化なし	Username	No	ユーザ名の照合を使用して認証します。
v3	認証 / 暗号化なし	MD5 または SHA	No	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
v3	認証 / 暗号化	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。CBC-DES（DES-56）標準に基づいて認証する以外に、DES 56 ビット暗号化を行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。*セキュリティ モデル*は、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。*セキュリティ レベル*とは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：パケットの内容を符号化して許可されていない送信元から読み取れないようにします。

SNMPv3 オブジェクトには次の特性があります。

- 各ユーザは 1 つのグループに属します。

- グループは、一連のユーザに対してアクセス ポリシーを定義し、このユーザが受信できる通知のリストを決定します。グループは、そのユーザのセキュリティ モデルとセキュリティ レベルも定義します。
- アクセス ポリシーは、どの SNMP オブジェクトが読み取り、書き込み、または作成のためにアクセスできるかを定義します。
- SNMPv3 は、検出ではサポートされません。

Cisco IOS ルータでの SNMPv1/v2c の設定

SNMP がイネーブルかどうかを判別し、Cisco IOS ルータで SNMP コミュニティ ストリングを設定するには、各ルータに対して次のステップを実行します。

	コマンド	説明
ステップ 1	Router> **enable** Router> *<enable_password>*	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ 2	Router# **show snmp**	**show snmp** コマンドの出力を確認して、「SNMP agent not enabled.」というステートメントがあるかどうかを確認します。SNMP がイネーブルではない場合、この手順のステップを完了します。
ステップ 3	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	Router(config)# **snmp-server community** *<userstring>* **RO**	コミュニティ read-only ストリングを設定します。
ステップ 5	Router(config)# **snmp-server community** *<userstring>* **RW**	コミュニティ read-write ストリングを設定します。
ステップ 6	Router(config)# **Ctrl+Z**	特権 EXEC モードに戻ります。
ステップ 7	Router# **copy running startup**	設定の変更内容を不揮発性 RAM（NVRAM）に保存します。

ヒント　ターゲット デバイスごとに Prime Provisioning に定義された SNMP コミュニティ ストリングは、デバイスで設定されているものと同じでなければなりません。

Cisco IOS ルータでの SNMPv3 パラメータの設定

この項では、Cisco IOS ルータで SNMPv3 パラメータを設定する方法について説明します。SNMPv3 は、IOS の暗号化イメージのみでサポートされます。認証/暗号化を行うには、IOS イメージに DES56 が必要です。

ヒント　ターゲット デバイスごとに Prime Provisioning に定義された SNMP ユーザは、デバイスで設定されているものと同じでなければなりません。

既存の SNMP コンフィギュレーションを確認するには、ルータ端末セッションで次のコマンドを使用します。

- **show snmp group**
- **show snmp user**

Cisco IOS ルータで SNMPv3 サーバ グループおよびユーザ パラメータを設定するには、次のステップを実行します。

（注）　最初にグループを作成し、次にユーザを作成する必要があります。

	コマンド	説明
ステップ 1	Router> **enable** Router> *<enable_password>*	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ 2	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **snmp-server group** [*<groupname>* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *<readview>*] [**write** *<writeview>*] [**notify** *<notifyview>*] [**access <***access-list>*]	**snmp-server group** コマンドは、新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定します。各グループは、特定のセキュリティ レベルに属します。 例：**snmp-server group v3auth v3 auth read v1default write v1default**
ステップ 4	Router(config)# **snmp-server user <***username>* [*<groupname>* **remote** *<ip-address>* [**udp-port** *<port>*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *<auth-password>* [**priv des56** *<priv-password>*]] [**access** *<access-list>*]	**snmp-server user** コマンドは、新しいユーザを SNMP グループに設定します。 例：**snmp-server user user1 v3auth v3 auth md5 user1Pass**
ステップ 5	Router(config)# **Ctrl+Z**	特権 EXEC モードに戻ります。
ステップ 6	Router# **copy running startup**	設定の変更内容を不揮発性 RAM（NVRAM）に保存します。

Cisco IOS ルータでの RTR 応答側の手動イネーブル

（注）　ルータで SNMP が設定されている必要があります。

Cisco IOS ルータで RTR 応答側を手動でイネーブルにするには、次の手順を実行します。

	コマンド	説明
ステップ 1	Router> **enable** Router> *<enable_password>*	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ 2	Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **rtr responder**	SA エージェント操作のターゲット ルータの SA 応答側をイネーブルにします。
ステップ 4	Router(config)# **Ctrl+Z**	特権 EXEC モードに戻ります。
ステップ 5	Router# **copy running startup**	設定の変更内容を不揮発性 RAM（NVRAM）に保存します。

プローブ

[Inventory] > [Device Tools] > [SLA] を選択すると、[SLA Probes] ウィンドウが表示されます。

イネーブルになっているデフォルト ボタンは [Create] であり、[Create] ドロップダウン リストから、SLA プローブを作成するために [From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] から選択できます。ただし、既存のプローブの行をクリックして 1 つ以上の既存のプローブを選択した場合、他のボタン、[Details]、[Delete]、[Enable] および [Disable] にアクセスできます。[Enable] および [Disable] の場合、ドロップダウン リストには、SLA の [Probes] と SLA の [Traps] をイネーブルまたはディセーブルにするオプションが含まれています。

ボタンとそれに続いて表示されるドロップダウン リストの説明は、次のとおりです。

- 「共通パラメータの作成」（P.10-7）：この項では、すべてのプローブ作成タイプの SLA 共通パラメータ、[From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] を説明します。
- 「任意の SA エージェント デバイスからの作成」（P.10-10）：この項では、任意の SA エージェント デバイスからのプローブを作成する方法を説明し、共通パラメータを作成した後に開始します。
- 「MPLS CPE からの作成」（P.10-11）：この項では、MPLS CPE からプローブを作成する方法について説明し、共通パラメータを作成した後に開始します。
- 「MPLS PE または MVRF-CE からの作成」（P.10-13）：この項では、MPLS PE または MVRF-CE からプローブを作成する方法について説明し、共通パラメータを作成した後に開始します。
- 「プロトコル」（P.10-15）：各 [Create] パスの共通プローブ情報を提供します。
- 「詳細」（P.10-17）：この項では、特定のプローブに関する詳細を説明します。
- 「削除」（P.10-17）：この項では、プローブを削除する方法について説明します。
- 「プローブのイネーブル化」（P.10-18）：この項では、プローブをイネーブルにして、[Created] から [Active] 状態にステータスを変更する方法を説明します。
- 「トラップのイネーブル化」（P.10-18）：この項では、トラップをイネーブルにする方法について説明します。
- 「プローブのディセーブル化」（P.10-19）：この項では、プローブをディセーブルにして、[Active] から [Disabled] 状態にステータスを変更する方法を説明します。
- 「トラップのディセーブル化」（P.10-19）：トラップをディセーブルにする方法について説明します。

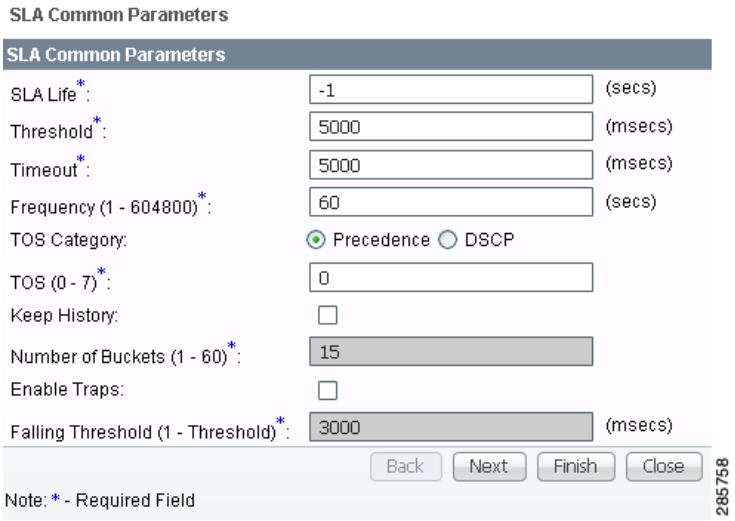
共通パラメータの作成

[Inventory] > [Device Tools] > [SLA] を選択すると、デフォルトは [Probes] ページになり、[Create] ボタンのみがイネーブルになります。[Create] ドロップダウン リストから、[From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] を選択できます。作成中に表示される最初のウィンドウは、すべてここで指定します。その後、選択した特定の作成タイプに進みます。

手順は次のとおりです。

ステップ 1　[Create] を選択すると、図 10-1 に示されているようなウィンドウが表示されます。

図 10-1　SLA Common Parameters



デフォルトを受け入れるか、次のように、共通の SLA パラメータのフィールドの情報を返納し、[Next] をクリックします。

- [SLA Life]（必須）：プローブがアクティブである秒数（最大値は秒単位での 32 ビット整数の最大値です）。値を一般的なデフォルト値である **-1** に設定すると、プローブは永久にアクティブになります。
- [Threshold]（必須）：しきい値制限をミリ秒で定義する整数。このしきい値を超過し、トラップがイネーブルである場合、トラップが送信されます。最大値は 32 ビット整数の最大値です。エージェント（SA エージェント）の動作時間に影響を与えるサービスがこの制限を超えた場合、しきい値超過が SA エージェントによって記録されます。[Threshold] の値が、[Timeout] の値を超えることはできません。デフォルト値は **5000** です。
- [Timeout]（必須）：SA エージェントの操作の完了を待機する時間（ミリ秒単位）。[Timeout] の値は、[Frequency] の値以下であり、[Threshold] の値以上である必要があります。デフォルト値は **5000** です。
- [Frequency]（0 ～ 604800）（必須）：各 SA エージェント操作が開始されるまでの期間（秒単位）。[Frequency] の値は、[Timeout] の値以上である必要があります。デフォルト値は **60** です。
- [TOS Category]（デフォルトは [Precedence]）：[TOS Category] の [Precedence] オプション ボタンを選択した場合、Type of Service（TOS; タイプ オブ サービス）値の 1 のセットを使用できます。[TOS Category] の [DSCP] オプション ボタンを選択すると、TOS 値の異なるセットが得られます。
- [TOS]（必須）：任意の整数。値の範囲と意味は、[TOS Category] のオプション ボタンが [Precedence]（値：0 ～ 7）または [DSCP]（値：0 ～ 63）のどちらに設定されているかによって異なります。
  - [TOS Category] が [Precedence] に設定されている場合、有効な値は **0** ～ **7** です。これらの値は、IP ヘッダーの [ToS] フィールドの 3 つの最上位ビットを表します。デフォルト値は **0** です。[Precedence] 値の意味は、表 10-2 に指定されています。

（注）　タイプ オブ サービスは、SLA プローブの [DNS] および [DHCP] タイプには適用されません。Prime Provisioning はこれらの 2 つのタイプの SLA プローブに設定されたすべての ToS 値を無視します。たとえば、まず ToS 値に 5 を選択し、SLA プローブに [DNS]、[DHCP]、および [ICMP Echo] プロトコルを選択すると、Prime Provisioning は選択した ToS 値を ICMP Echo プローブのみに適用します。

表 10-2　[Precedence] の値の意味

ToS 値	バイナリ値	意味
7	111	ネットワーク制御
6	110	インターネットワーク制御
5	101	CRITIC/ECP
4	100	フラッシュ オーバーライド
3	011	フラッシュ
2	010	即時
1	001	優先順位
0	000	ルーチン

  - [TOS Category] が [DSCP] に設定されている場合、有効な値は **0** から **63** です。これらの値は、IP ヘッダーの [ToS] フィールドの 6 つの最上位ビットを表します。デフォルト値は **0** です。これらの [TOS] 値は、ユーザ指定です。

（注）　Prime Provisioning は、0 ～ 7 の [PRECEDENCE] 値を 3 つの最上位 ToS ビットにマッピングします（値は 5 ビット左に移動します）。同様に、0 ～ 63 の [DSCP] 値は、2 ビット左に移動します。

- [Keep History]（デフォルトはオフ）: [Keep History] チェックボックスがオンの場合、ルータの最近の [History Table] が保持されます。特に、ロー ラウンドトリップ時間（RTT）SLA 測定を維持する SA Agent MIB で保持されます。このように選択することで、保持する未加工の履歴データの [Number of Buckets] を示すこともできます。[Keep History] のチェックボックスをデフォルトのオフのままにしていると、未加工の履歴データは保持されません。[Keep History] は **HTTP** および **Jitter** についてはサポートされません。
- [Number of Buckets]（1 ～ 60）（必須）: [Keep History] チェックボックスがオンの場合、デフォルトは 15 です。範囲は 1 ～ 60 であり、未加工の履歴データに保存される最新の未加工データ エントリの数を示します。指定した [Number of Buckets] を超過すると、最も古いバケットからバケットの削除が開始され、指定された数のみ未加工のデータ エントリが保持されるようになります。
- [Enable Traps]（デフォルト：オフ、つまり [No] に設定）: [Enable Traps] チェックボックスをオンにすると、作成された SLA は 3 つのタイプのトラップを送信するように設定されます。このように選択すると、[Falling Threshold] を示すことができるようにもなります。[Enable Traps] チェックボックスがオフの場合、このタスクで作成される SLA でトラップがディセーブルにされます。
- [Falling Threshold]（1 ～ [Threshold]）（必須）: [Enable Traps] チェックボックスがオンの場合、デフォルト値は、**3000**（ミリ秒単位）です。範囲は、ミリ秒単位で **1** から [Threshold] 値までです。トラップがイネーブルで、遅延が指定されたミリ秒に達している場合、トラップが送信されます。

ステップ 2　次に、「任意の SA エージェント デバイスからの作成」（P.10-10）、「MPLS CPE からの作成」（P.10-11）または「MPLS PE または MVRF-CE からの作成」（P.10-13）に進みます。

任意の SA エージェント デバイスからの作成

「共通パラメータの作成」（P.10-7）での手順を完了したら、次の手順に従います。

（注）　IP 接続が SA Agent デバイス間で使用できる必要があります。

ステップ 1　表示される次のウィンドウは、図 10-2 に示されているようになります。

図 10-2　SLA 送信元デバイス

ステップ 2　[Add] ボタンをクリックすると、図 10-3 に示すようなウィンドウが表示されます。このウィンドウには、少なくとも 1 つのインターフェイスがある、データベースのすべてのデバイスがリストされます。選択するデバイスの各行の横にあるチェックボックスをオンにして、[Select] をクリックします。

図 10-3　[SLA Devices] > [Add]

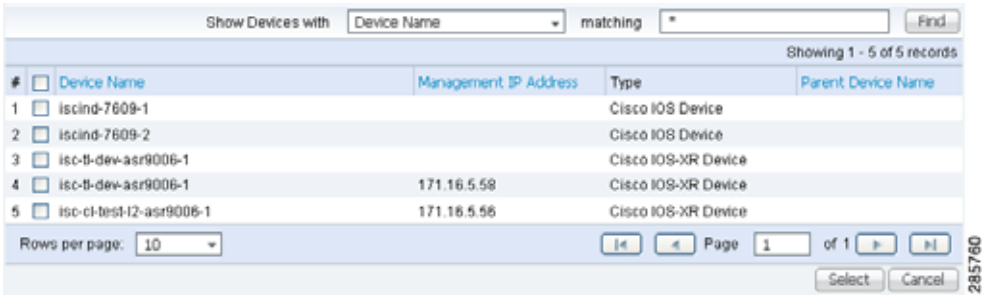


図 10-2 に戻ります。新しく追加された送信元デバイスが表示されます。この送信元デバイスに関する情報は、次のカラムで指定します。

- [Device Name]：このヘッダーをクリックすると、デバイス名がアルファベット順にソートされます。
- [Interface]：[Select] をクリックすると、ウィンドウが表示されます。このウィンドウから、IP アドレスを更新できます。インターフェイスのいずれかのオプション ボタンを選択し、[Select] をクリックすると、図 10-2 に示すように IP アドレスが変わります。
- [Type]：送信元デバイスのタイプを指定します。

ステップ 3　ステップ 2 から を繰り返して複数のデバイスを追加したり、現在選択されている送信元デバイスを削除したりできます。デバイスを削除するには、削除するデバイスの各行の横にあるチェックボックスをオンにして、[Delete] をクリックします。

（注）　送信元デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 4　[Next] をクリックします。

表示される次のウィンドウは、図 10-4 に示されているようになります。

図 10-4　SLA の宛先デバイス

ステップ 5　[Add] ボタンをクリックすると、図 10-3 に示すようなウィンドウが表示されます。選択するデバイスの各行の横にあるチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 6　図 10-4 に戻ります。新しく追加された宛先デバイスが表示されます。この宛先デバイスに関する情報は、次のカラムで指定します。

- [Device Name]：このヘッダーをクリックすると、デバイス名がアルファベット順にソートされます。
- [Interface]：[Select] をクリックすると、ウィンドウが表示されます。このウィンドウから、IP アドレスを更新できます。インターフェイスのいずれかのオプション ボタンを選択し、[Select] をクリックすると、図 10-4 に示すように IP アドレスが変わります。
- [Type]：送信元デバイスのタイプを指定します。

ステップ 7　ステップ 5 からステップ 6 を繰り返してさらにデバイスを追加したり、現在選択されている宛先デバイスを削除したりできます。デバイスを削除するには、削除するデバイスの各行の横にあるチェックボックスをオンにして、[Delete] をクリックします。

（注）　宛先デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 8　[Next] をクリックします。「プロトコル」（P.10-15）に進みます。

MPLS CPE からの作成

「共通パラメータの作成」（P.10-7）での手順を完了したら、次の手順に従います。

ステップ 1　「共通パラメータの作成」（P.10-7）のステップを完了して、次のウィンドウを表示します（図 10-5 を参照）。

図 10-5　SLA CPE パラメータ

ステップ 2　[VPN] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースのすべての **VPN** がリストされます。

ステップ 3　選択する VPN のオプション ボタンをクリックします。次に、[Select] をクリックします。図 10-5 に戻ります。新しく追加された [VPN] および [Customer] の情報が表示され、[CPE] の [Select] ボタンが表示されます。ステップ 2 を繰り返して、VPN を変更できます。

ステップ 4　[CPE] の [Select] ボタンをクリックすると、選択した VPN に関連付けられた CPN がリストされたウィンドウが表示されます。選択する CPE のオプション ボタンをクリックします。次に、[Select] をクリックします。

ステップ 5　図 10-5 に戻ります。新しく追加された [CPE] とその最初のインターフェイスが表示され、[CPE Interface] に [Select] ボタンが表示されます。ステップ 4 を繰り返して CPE を変更できます。

ステップ 6　表示されるデフォルトの [CPE Interface] 情報を変更する場合、[Select] をクリックして、ウィンドウを表示します。

ステップ 7　選択するインターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。図 10-5 に戻ります。新しく追加された [CPE Interface] が表示されます。

ステップ 8　ステップ 6 を繰り返して CPE インターフェイスを変更できます。

ステップ 9　[Connected PE] のオプション ボタンを選択したままにすることで、デフォルトの [Type] を維持することができます。これにより、CPE とその直接接続された PE の間に SLA が作成されます。あるいは、同じ VPN 内で [CPEs] のオプション ボタンを選択できます。[Connected PE] のデフォルトを使用する場合は、ステップ 10 に進みます。[CPEs] オプション ボタンをクリックする場合は、ステップ 14 に進みます。

ステップ 10　[Connected PE Interface] の [Select] をクリックして、ウィンドウを表示します。

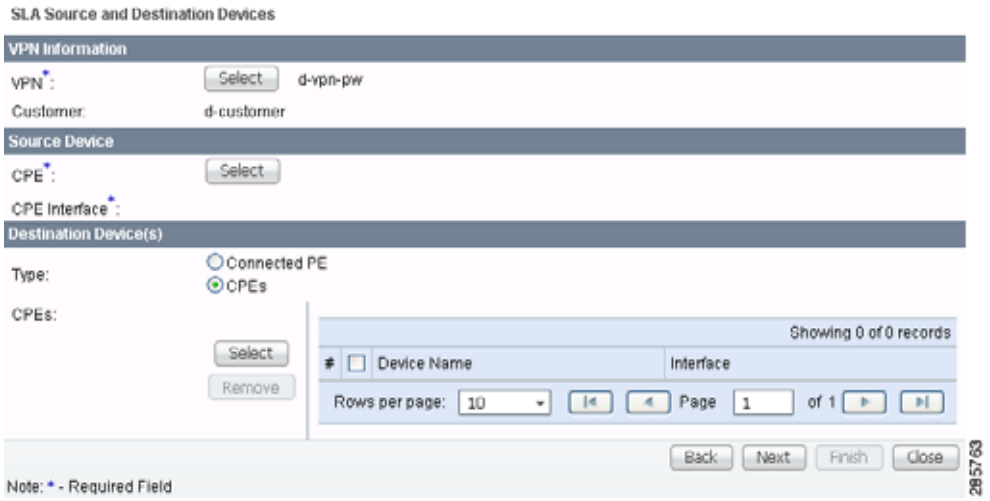
ステップ 11　選択するインターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。

ステップ 12　図 10-5 に戻ります。新しく追加された [Connected PE Interface] が表示されます。ステップ 10 を繰り返して、[Connected PE Interface] を変更できます。

ステップ 13　[Next] をクリックして、「プロトコル」（P.10-15）に進みます。

ステップ 14　[CPEs] をクリックすると、図 10-6、「CPEs」のようなウィンドウが表示されます。

図 10-6　CPEs



ステップ 15　[CPEs] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースの指定 VPN に関連するすべての CPE がリストされます。

ステップ 16　選択する CPE の各行の横にあるチェックボックスをオンにします。次に、[Select] をクリックします。

（注）　[Source Device] として選択されているデバイスを [Destination Device(s)] に追加*しないでください*。

図 10-6 に戻ります。新しく追加された [Device Name] が表示されます。

ステップ 17　[Interface] カラムの [Select] をクリックして、ウィンドウを表示します。

ステップ 18　選択する CPE の行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。

ステップ 19　図 10-6 に戻ります。新しく追加された [CPE Interface] が表示されます。ステップ 17 を繰り返して CPE インターフェイスを変更できます。

ステップ 20　削除するデバイスの各行の横にあるチェックボックスをオンにします。[Remove] ボタンをクリックします。デバイスが削除された状態でウィンドウが表示されます（図 10-6 を参照）。

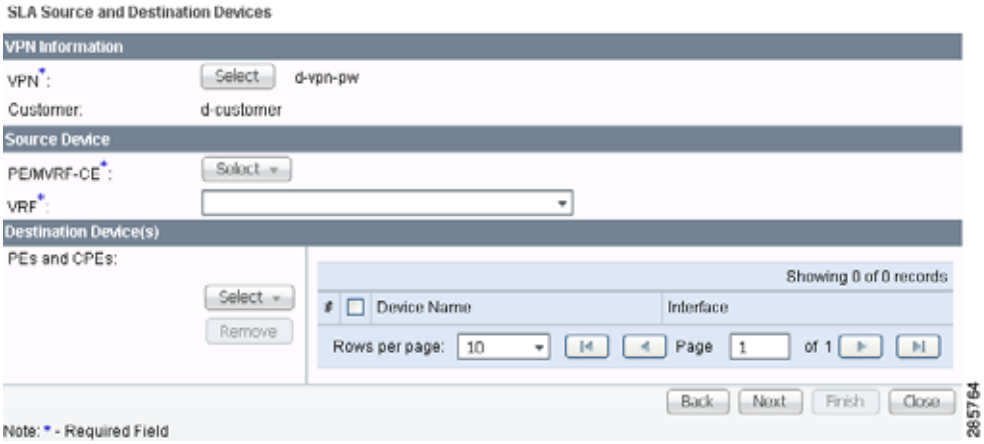
ステップ 21　図 10-6 の表示内容を反映するには、[Next] をクリックして、「プロトコル」（P.10-15）に進みます。

MPLS PE または MVRF-CE からの作成

「共通パラメータの作成」（P.10-7）での手順を完了したら、次の手順に従います。

ステップ 1　「共通パラメータの作成」（P.10-7）の手順を完了すると、図 10-7 の「SLA Source and Destination Devices」に示されているウィンドウが次に表示されます。

図 10-7　SLA Source and Destination Devices



ステップ 2　[VPN] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースのすべての VPN がリストされます。選択する VPN の行の横にあるオプション ボタンをクリックします。

ステップ 3　次に、[Select] をクリックします。

ステップ 4　図 10-7 に戻ります。新しく追加された [VPN] および [Customer] の情報が表示されます。ステップ 2 を繰り返して、[VPN] および [Customer] を変更できます。

ステップ 5　[PE/MVRF-CE] の新しい [Select] ボタンをクリックして、ドロップダウン リストを表示します。このドロップダウン リストから、[PE] または [MVRF-CE] を選択できます。[PE] を選択すると、ウィンドウが表示されます。このウィンドウでは、選択した VPN に関連するすべての PE がリストされます。[MVRF-CE] を選択すると、ウィンドウが表示されます。このウィンドウでは、選択した VPN に関連するすべての MVRF-CE がリストされます。選択する PE または MVRF-CE の行の横にあるオプション ボタンをクリックします。次に、[Select] または [OK] をクリックします。

ステップ 6　図 10-7 に戻ります。新しく追加された [PE] および [MVRF-CE] の情報が表示されます。ステップ 5 を繰り返して、この選択を変更できます。

ステップ 7　ステップ 5 で MVRF-CE 情報を選択すると、[VRF] ドロップダウン リストをクリックできるようになります。

ステップ 8　宛先デバイスの新しい [Select] ボタンをクリック：PE と CPE、およびドロップダウンリストから、[PEs] または [CPEs] を選択します。[PEs] を選択すると、ウィンドウが表示されます。このウィンドウでは、データベースのすべての PE インターフェイスがリストされます。[CPEs] を選択すると、ウィンドウが表示されます。このウィンドウでは、データベースのすべての CPE インターフェイスがリストされます。選択するデバイス インターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。

（注）　[Source Device] として選択されているデバイスを [Destination Device(s)] に追加しないでください。

ステップ 9　図 10-7 に戻り、インターフェイス情報を表示します。[Select] をクリックして、ウィンドウを表示します。このウィンドウでは、別のインターフェイスの横にあるオプション ボタンをクリックできます。[Select] をクリックすると、古いインターフェイスが新しいインターフェイスに置き換えられます。このステップを繰り返して、インターフェイスを変更できます。

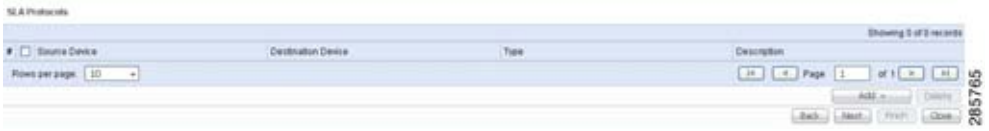
ステップ 10　[Next] をクリックして、「プロトコル」（P.10-15）に進みます。

プロトコル

いずれかの [Create] 機能のすべてのステップ、「共通パラメータの作成」（P.10-7）、「MPLS CPE からの作成」（P.10-11）または「MPLS PE または MVRF-CE からの作成」（P.10-13）を完了したら、この場所を選択します。手順は次のとおりです。

ステップ 1　「共通パラメータの作成」（P.10-7）のステップを完了して、次のウィンドウを表示します（図 10-8 を参照）。

図 10-8　　プロトコル



ステップ 2　[Add] ドロップダウン リストをクリックして、次のものを選択します。

- [ICMP Echo]（宛先デバイスが使用できる場合だけ使用できます）：ステップ 3 に進みます。
- [TCP Connect]（MPLS PE または MVRF-CE からの作成では使用できません。その他のすべての作成方法では、[TCP Connect] は宛先デバイスが使用できる場合だけ使用できます）：ステップ 4 に進みます。
- [UDP Echo]（宛先デバイスが使用できる場合だけ使用できます）：ステップ 5 に進みます。
- [Jitter]（宛先デバイスが使用できる場合だけ使用できます）：ステップ 6 に進みます。
- [FTP]（MPLS PE または MVRF-CE からの作成では使用できません）：ステップ 7 に進みます。
- [DNS]（MPLS PE または MVRF-CE からの作成では使用できません）：ステップ 8 に進みます。
- [HTTP]（MPLS PE または MVRF-CE からの作成では使用できません）：ステップ 9 に進みます。
- [DHCP]（MPLS PE または MVRF-CE からの作成では使用できません）：ステップ 10 に進みます。

ステップ 3　ステップ 2 から [ICMP Echo] を選択した場合、プロトコル [ICMP Echo] ウィンドウが表示されます。

次のように、必須情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Request Size]（0 ～ 16384）（必須）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは **28** です。

ステップ 4　ステップ 2 から [TCP Connect] を選択した場合、プロトコル [TCP Echo] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Destination Port]（1 ～ 65535）（必須）：モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **23** が使用されます。
- [Request Size]（1 ～ 16384）（任意）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは、**1** です。

ステップ 5　ステップ 2 から [UDP Echo] を選択した場合、プロトコル [UDP Echo] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Destination Port]（1 ～ 65535）（必須）：モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **7** が使用されます。
- [Request Size]（4 ～ 8192）（任意）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは **16** です。

ステップ 6　ステップ 2 から [Jitter] を選択した場合、プロトコル [Jitter] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Destination Port]（1 ～ 65535）（必須）：モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **8000** が使用されます。
- [Request Size]（16 ～ 1500）（任意）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは、**32** です。
- [Number of Packets]（1 ～ 1000）（任意）：転送する必要があるパケットの数を表す整数。デフォルト値は、**10** です。
- [Interval]（1 ～ 1000）（任意）：パケット間のパケット間遅延をミリ秒単位で表す整数（**1** ～ **1,000**）。デフォルト値は、**20** です。

ステップ 7　ステップ 2 から [FTP] を選択した場合、プロトコル [FTP] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [User Name]（任意）：空の場合、anonymous が使用されます。
- [Password]（任意）：空の場合、test が使用されます。
- [Host IP Address]（必須）：ファイル転送プロトコル（FTP）の IP アドレスを入力します。
- [File Path]（必須）：FTP サーバの FTP 対象ファイルのパスを入力します。

ステップ 8　ステップ 2 から [DNS] を選択した場合、プロトコル [DNS] ウィンドウが表示されます。

次のように、必須情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Name Server]（必須）：ネーム サーバの IP アドレスを指定する文字列。このアドレスは、ドット付き IP アドレス形式です。
- [Name to be Resolved]（必須）：DNS サーバにより解決される名前または IP アドレスのいずれかである文字列。文字列が名前の場合、長さは 255 文字です。文字列が IP アドレスの場合、ドット付き IP アドレス形式です。
- [Request Size]（0 ～ 16384）（必須）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは、**1** です。

ステップ 9　ステップ 2 から [HTTP] を選択した場合、プロトコル [HTTP] ウィンドウが表示されます。

次のように、オプションおよび必須情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- [Version]（デフォルトは 1.0）：HTTP サーバのバージョンを指定する文字列。これは変更しないでください。Prime Provisioning は、バージョン 1.0 だけをサポートします。
- [URL]（必須）：HTTP プローブが通信する URL、*HTTPServerName*[/*directory*]/*filename* または *HTTPServerAddress*[/*directory*]/*filename*（たとえば、**http://www.cisco.com/index.html** または **http://209.165.201.22/index.html**）を表す文字列。[HTTPServerName] を指定した場合、[Name Server] は必須です。[HTTPServerAddress] を指定した場合、[Name Server] は必須ではありません。
- [Cache]（デフォルトでは選択済み（オン）：チェックボックスがオフの場合、HTTP 要求は、キャッシュされたページをダウンロードしません。チェックボックスがオンの場合、HTTP 要求は、使用できる場合、キャッシュされたページをダウンロードします。そうでない場合、要求は、HTTP サーバに転送されます。
- [Proxy Server]（任意）：プロキシ サーバ情報を表す文字列（最大 255 文字）。デフォルトは、ヌルストリングです。
- [Name Server]（任意、[URL] 設定により異なります）：ネーム サーバの IP アドレスを指定する文字列。このアドレスは、ドット付き IP アドレス形式です。

- [Operation]（デフォルトは [HTTPGet]）：HTTP get 要求を表すデフォルトの [HTTPGet] ではなく、ユーザ定義ペイロードで HTTP 要求を表す [HTTPRaw] が必要な場合、ドロップダウン リストを使用して、選択します。
- [Raw Request]（[Operation] が [HTTPRaw] の場合必須。[Operation] が [HTTPGet] の場合は使用できません）：[Operation] が [HTTPRaw] の場合だけ必要な文字列。これにより、単純な GET 動作以外の他のタイプの HTTP 動作を呼び出すことができます。
- [Request Size]（1 ～ 16384）（必須）：パケットのデータ部分に置かれるオクテット（バイト単位）の数を表す数値。デフォルトは **28** です。

ステップ 10　ステップ 2 から [DHCP] を選択した場合、プロトコル [DHCP] ウィンドウが表示されます。

次のように、必須情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- Destination IP Address（必須）

ステップ 11　図 10-8 に戻ります。提供した [Protocol] 情報に基づいて、情報の追加カラムが表示されます。[Next] をクリックして作業を進める前に、[Add] でプロトコルをさらに追加するか決定します。この場合、ステップ 2 ～ステップ 10 を繰り返します。または、[Delete] で現在選択されている任意のプロトコルを削除します。この場合、[Delete] をクリックして、ステップ 2 ～ステップ 10 を繰り返してプロトコルを削除します。

（注）　宛先デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 12　次に表示されるウィンドウは、定義した [Description]（作成日時）、[Common Parameters]、[Source Devices]、[Destination Devices] および [Protocols] を示す [Probe Creation Task Summary] ウィンドウです。表示内容で変更しない場合、[Finish] をクリックします。変更する場合、[Back] をクリックして変更します。

詳細

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、詳細を表示できます。

ステップ 1　詳細を表示するプローブに対応するチェックボックスをオンにして、既存のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。

ステップ 2　[Details] ボタンをクリックすると、[SLA Probes Details] ウィンドウが表示されます。このウィンドウには、最初に [Create] を実行したときに定義された [Common Attributes] の情報、およびプロトコルで定義された [Protocol Specific Attributes] の情報が含まれます。

ステップ 3　[OK] をクリックして戻ります。さらに [Details] を選択するか、別の機能を実行できます。

削除

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、リストからプローブを削除できます。

ステップ 1　既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Delete] ボタンにアクセスできるようになります。

ステップ 2　[Delete] ボタンをクリックすると、確認ウィンドウが表示されます。

ステップ 3　削除した状態が反映された場合は [OK] をクリックします。反映されていない場合は [Cancel] をクリックします。

（注）　プローブが削除されると、プローブルがプローブ リスト ページから削除されますが、データベースには残ります。

情報が更新された状態のウィンドウが表示されます。

プローブのイネーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、プローブをイネーブルにできます。

ステップ 1　既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Enable] ボタンにアクセスできるようになります。[Enable] ドロップダウン リストから、[Probes] にアクセスできます。

ステップ 2　[Enable] > [Probes] を選択すると、プローブのイネーブルを確認するウィンドウが表示されます。

ステップ 3　プローブがイネーブルにされた場合は [OK] をクリックします。イネーブルにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] にグリーンのチェックマークが付きます。[Status] カラムは、プローブがルータで正常に作成された場合、[Active] に設定されます。

トラップのイネーブル化

[Inventory] > [Device Tools] > [SLA] を選択し、次のステップを実行することで、トラップをイネーブルにできます。

ステップ 1　既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Enable] ボタンにアクセスできるようになります。[Enable] ドロップダウン リストから、[Traps] にアクセスできます。

ステップ 2　[Enable] > [Traps] を選択すると、トラップのイネーブルを確認するウィンドウが表示されます。すべてのトラップには、下限しきい値として 3000 ms が自動的に設定されます。

ステップ 3　トラップがイネーブルにされた場合は [OK] をクリックします。トラップにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] にグリーンのチェックマークが付きます。[Traps Enabled] カラムは、ルータのプローブが正常に変更されると、[yes] に設定されます。

プローブのディセーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、[Disable Probes] を使用して、デバイスのプローブを削除できます。手順は次のとおりです。

ステップ 1　既存のプローブの行のチェックボックスをオンにして、イネーブルにされた 1 つ以上のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。[Disable] ドロップダウン リストから、[Probes] にアクセスできます。

ステップ 2　[Disable] > [Probes] を選択すると、プローブのディセーブルを確認するウィンドウが表示されます。

ステップ 3　プローブがディセーブルにされた場合は [OK] をクリックします。ディセーブルにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] にグリーンのチェックマークが付きます。プローブのステータスは、ルータのプローブが正常に削除されると、[Disabled] になります。

トラップのディセーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、トラップをディセーブルにできます。

ステップ 1　既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。[Disable] ドロップダウン リストから、[Traps] にアクセスできます。

ステップ 2　[Disable] > [Traps] を選択すると、トラップのディセーブルを確認するウィンドウが表示されます。

ステップ 3　トラップをディセーブルにする場合は [OK] をクリックします。ディセーブルにしない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] にグリーンのチェックマークが付きます。ルータのプローブが正常に変更されると、トラップはディセーブルにされます。

レポート

[Inventory] > [Device Tools] > [SLA] を選択すると、図 10-9 に示されているウィンドウが表示されます。

図 10-9　SLA レポート

次のいずれかをクリックして、そのレポートを表示できます。

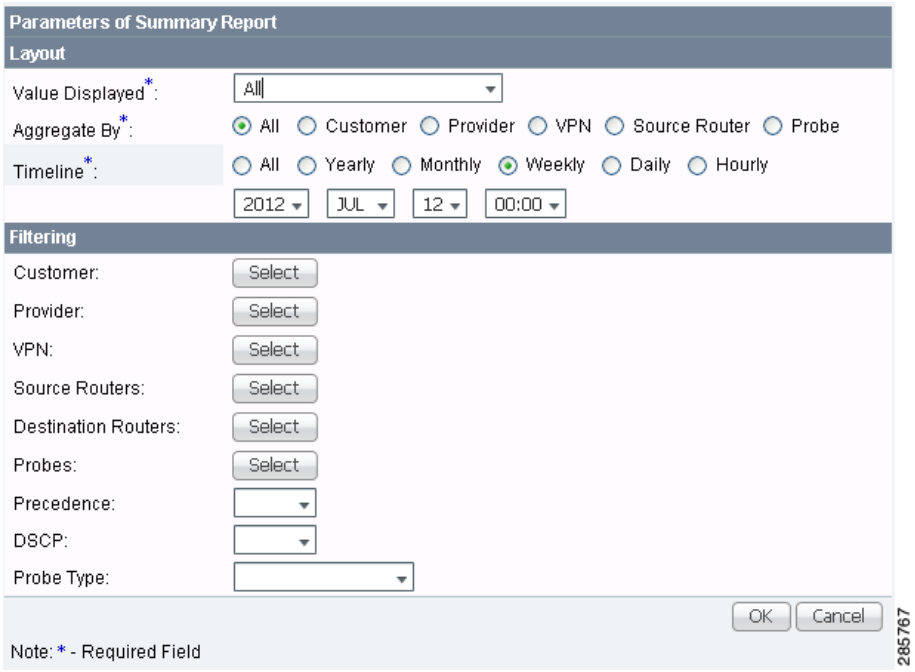
- 「Summary Report」（P.10-20）：このレポートは、HTTP およびジッタ以外のすべての情報（ICMP Echo、TCP Connect、UDP Echo、FTP、DNS および DHCP）を要約します。
- 「HTTP Report」（P.10-23）：HTTP 情報の要約レポートです。
- 「Jitter Report」（P.10-23）：ジッタ情報の要約レポートです。
- 「Summary CoS Report」（P.10-24）：HTTP およびジッタ以外のサービス クラス（CoS）（ICMP Echo、TCP Connect、UDP Echo、FTP、DNS および DHCP）の要約レポートです。
- 「HTTP CoS Report」（P.10-25）：HTTP CoS 情報のレポートです。
- 「Jitter CoS Report」（P.10-25）：ジッタ CoS 情報のレポートです。

Summary Report

図 10-9 から、[Summary Report] を選択して、次のステップを実行します。

ステップ 1　[Summary Report] を選択すると、図 10-10 のようなウィンドウが表示されます。

図 10-10　Parameters of Summary Report



ステップ 2　図 10-10 で、次のように、[Layout] フィールドに入力します。

- [Value Displayed]（必須）（デフォルトは [All]）：ドロップダウン リストをクリックして、次のいずれかを選択します。
  - [All]：すべての値を表示します。
  - [Connections (#)]：接続数を表示します。
  - [Timeouts (#)]：タイムアウト数を表示します。
  - [Connectivity (%)]：接続の割合を表示します。
  - [Threshold Violations (%)]：しきい値超過の割合を表示します。
  - [Max Delay (ms)]：ミリ秒単位の最大遅延を表示します。
  - [Min Delay (ms)]：ミリ秒単位の最小遅延を表示します。
  - [Avg Delay (ms)]：ミリ秒単位の平均遅延を表示します。
- [Aggregate By]（必須）（デフォルトは [All]）：[All]、[Customer]、[Provider]、[VPN]、[Source Router] または [Probe] 別から、データ平均方法のオプション ボタンをクリックします。
- [Timeline]（必須）（デフォルトは [Weekly]、選択した週の最初の日付の午前 0 時から開始）：表示するレポート データ（[All] データ、[Yearly] データ、[Monthly] データ、[Weekly] データ、[Daily] データまたは [Hourly] データ）のオプション ボタンをクリックします。レポートを開始する、年、月、日付、時刻のドロップダウン リストをクリックします。

ステップ 3　図 10-10 で、次のように、[Filtering] フィールドに入力します。

（注） レポートには、フィルタリング フィールドのすべての条件を満たすデータだけが含まれます（すべての条件は、論理積で結合されます）。

- [Customer]（任意）：[Select] ボタンをクリックして、カスタマーの結果リストから、リストをフィルタリングします（選択した場合）。リストされた [Customers] から、この SLA レポートの [Customer] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、選択されたカスタマーが、[Customer] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Provider]（任意）：[Select] ボタンをクリックして、プロバイダーの結果リストから、リストをフィルタリングします（選択した場合）。リストされた [Providers] から、この SLA レポートの [Provider] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、選択されたプロバイダーが、[Provider] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [VPN]（任意）：[Select] ボタンをクリックして、VPN の結果リストから、リストをフィルタリングします（選択した場合）。リストされた [VPNs] から、この SLA レポートの [VPN] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、選択された VPN が、[VPN] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Source Routers]（任意）：[Select] ボタンをクリックして、デバイスの結果リストから、リストをフィルタリングします（選択した場合）。リストされたデバイスから、デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、[Source Routers] に選択されたデバイスが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Destination Routers]（任意）：[Select] ボタンをクリックして、デバイスの結果リストから、リストをフィルタリングします（選択した場合）。リストされたデバイスから、デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、[Destination Routers] に選択されたデバイスが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Probes]（任意）：[Select] ボタンをクリックして、送信元プローブの結果リストから、リストをフィルタリングします（選択した場合）。リストされた送信元プローブから、送信元プローブのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると図 10-10 に戻り、[Probes] に選択された送信元プローブが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Precedence]（デフォルトは [All]）：ドロップダウン リストをクリックして、他の [Precedence] の [TOS] の選択肢、**0** ～ **7** を選択します。これらの値は、IP ヘッダーの [ToS] フィールドの 3 つの最上位ビットを表します。[Precedence] 値の意味は、表 10-2 に指定されています。

（注） Prime Provisioning は、0 ～ 7 の [PRECEDENCE] 値を 3 つの最上位 ToS ビットにマッピングします（値は 5 ビット左に移動します）。

（注） タイプ オブ サービスは、SLA プローブの [DNS] および [DHCP] タイプには適用されません。Prime Provisioning はこれらの 2 つのタイプの SLA プローブに設定されたすべての ToS 値を無視します。たとえば、まず ToS 値に 5 を選択し、SLA プローブに [DNS]、[DHCP]、および [ICMP Echo] プロトコルを選択すると、Prime Provisioning は選択した ToS 値を ICMP Echo プローブのみに適用します。

- [DSCP]（デフォルトは [All]）：ドロップダウン リストをクリックして、他の [DSCP] の [TOS] の選択肢、**0** ～ **63** を選択します。これらの値は、IP ヘッダーの [ToS] フィールドの 6 つの最上位ビットを表します。これらの [TOS] 値は、ユーザ指定です。

（注）　Prime Provisioning は、0 ～ 63 の [DSCP] 値を 6 つの最上位 ToS ビットにマッピングします（値は 2 ビット左に移動します）。

- [Probe Type]（デフォルトは [All]）：ドロップダウン リストをクリックして、プローブのタイプ、[ICMP Echo]、[UDP Echo]、[TCP Connect]、[HTTP]、[DNS]、[Jitter]、[DHCP]、[FTP] から選択します。

（注）　これらのプローブ タイプについては、「プロトコル」（P.10-15）で詳しく説明されています。

ステップ 4　必要な情報が表示されたら、[OK] をクリックします（図 10-10 を参照）。

選択した項目がリストされた要約レポートが表示されます。該当するボタンを使用して、このレポートで [Modify]、[Refresh]、[Print]、[Close] を実行できます。

（注）　[Modify] を選択すると、図 10-10 のようなウィンドウが表示されます。このウィンドウでは、前述のステップで説明されているように、選択項目を変更できます。

HTTP Report

図 10-9 から、[HTTP Report] を選択して、「Summary Report」（P.10-20）と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] のドロップダウン リストの項目が異なります。
- [Destination Routers] 選択はありません。
- プローブ タイプは自動的に [HTTP] になるため、図 10-10 に [Probe Type] ドロップダウン リストはありません。結果は HTTP レポートです。

Jitter Report

図 10-9 から、[Jitter Report] を選択して、「Summary Report」（P.10-20）と同様に処理を進めます。ただし、次のことが異なります。

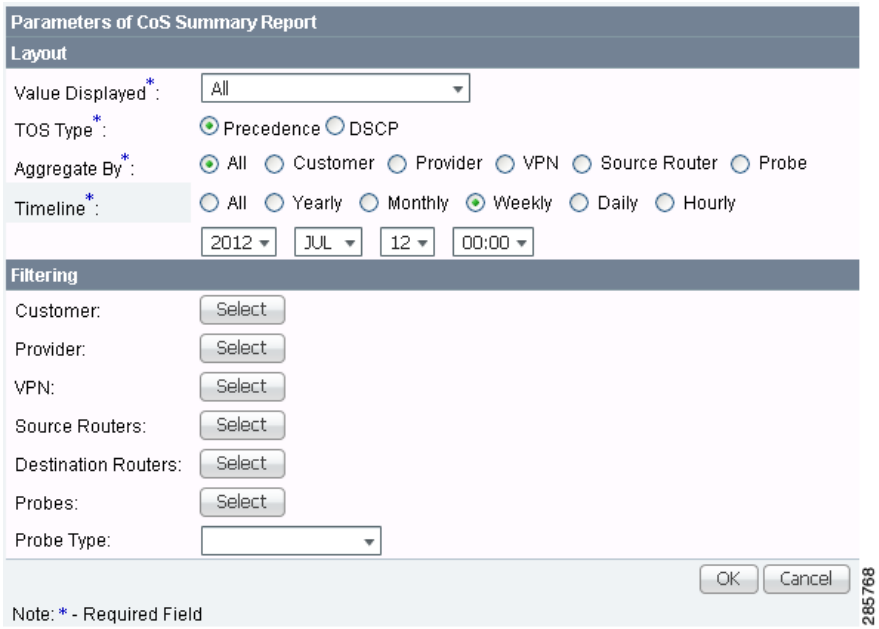
- [Value Displayed] のドロップダウン リストの項目が異なります。
- [Destination Routers] 選択はありません。
- プローブ タイプは自動的に [Jitter] になるため、図 10-10 に [Probe Type] ドロップダウン リストはありません。結果はジッタ レポートです。

Summary CoS Report

図 10-9 から、サービス クラス（CoS）の要約レポート（SLA プローブの TOS 値に基づきます）の [Summary CoS Report] を選択して、次のステップを実行します。

ステップ 1　[Summary CoS Report] を選択します。図 10-11 のようなウィンドウが表示されます。

図 10-11　Parameters of CoS Summary Report



ステップ 2　図 10-11 で、「Summary Report」（P.10-20）のステップ 2 に示すように、[Layout] フィールドに入力します。ただし、次のことが異なります。[Value Displayed] の後、[Aggregate By] の前で、新しい [TOS Type] のオプション ボタン [Precedence]（デフォルト）または [DSCP] を選択します。説明が [Filtering] セクションに示されます（「Summary Report」（P.10-20）のステップ 3 を参照）。

ステップ 3　図 10-11 で、「Summary Report」（P.10-20）のステップ 3 に示すように、[Filtering] フィールドに入力します。ただし、[Precedence] または [DSCP] ドロップダウン リストはありません。この項のステップ 2 で説明されているように、これらは [Layout] フィールドにあります。

ステップ 4　必要な情報が表示されたら、[OK] をクリックします（図 10-11 を参照）。

選択した項目がリストされた CoS 要約レポートが表示されます。該当するボタンを使用して、このレポートで [Modify]、[Refresh]、[Print]、[Close] を実行できます。

（注）　[Modify] を選択すると、図 10-11 のようなウィンドウが表示されます。このウィンドウでは、前述のステップで説明されているように、選択項目を変更できます。

HTTP CoS Report

図 10-9 から、[HTTP Report] を選択して、「Summary CoS Report」（P.10-24）と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] には、[HTTP Report] と同じドロップダウン項目があります。
- [Destination Routers] 選択はありません。
- プローブ タイプは自動的に [HTTP CoS] になるため、図 10-11 に [Probe Type] ドロップダウン リストはありません。結果は CoS HTTP レポートです。この CoS HTTP レポートは、SLA プローブの TOS 値に基づいています。

Jitter CoS Report

図 10-9 から、[Jitter Report] を選択して、「Summary CoS Report」（P.10-24）と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] には、[Jitter Report] と同じドロップダウン項目があります。
- [Destination Routers] 選択はありません。
- プローブ タイプは自動的に [Jitter CoS] になるため、図 10-11 に [Probe Type] ドロップダウン リストはありません。結果は CoS ジッタ レポートです。この CoS ジッタ レポートは、SLA プローブの TOS 値に基づいています。

タスク マネージャ

Prime Provisioning にはタスク マネージャが備わっており、これを使用して、すべてのタイプの現在および期限切れのタスクの両方についての関連情報の表示、新しいタスクの作成とスケジュール設定、指定したタスクの削除、およびアクティブおよび期限切れのタスクの削除を行えます。

ここでは、次の内容について説明します。

- 「タスク」（P.10-25）
- 「タスク ログ」（P.10-29）

タスク

ここでは、次の内容について説明します。

- 「タスク マネージャの起動」（P.10-26）
- 「作成」（P.10-26）
- 「監査」（P.10-27）
- 「詳細」（P.10-28）
- 「スケジューリング」（P.10-28）
- 「ログ」（P.10-28）
- 「削除」（P.10-28）

タスク マネージャの起動

タスク マネージャを起動するには、[Operate] > [Tasks] > [Task Manager] をクリックします。[Tasks list] ページが表示されます。

[Tasks] ウィンドウには、[Task Name]、[Type]、[Targets]、[Schedules] の日時、[User Name]（タスクの作成者）、および [Created on] の日付ごとに、各タスクの情報が表示されます。リストされたタスクを表示、スケジュール設定、または削除するには、対応するチェックボックスをオンにします。

このウィンドウを使用して新しいタスクを作成または監査することもできます。

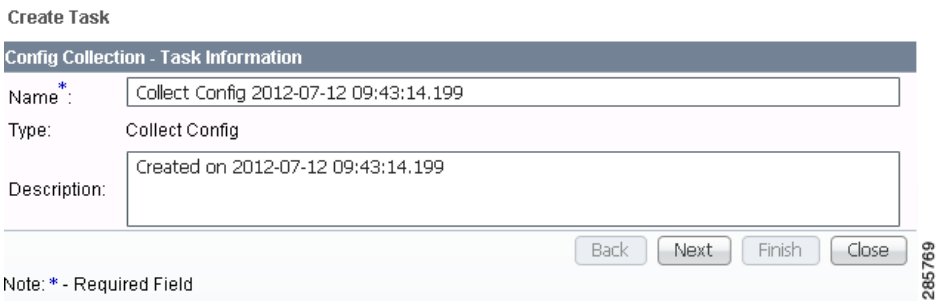
作成

新しいタスクを作成するには、次の手順に従ってください。

ステップ 1　[Task Manager] ウィンドウで、[Create] をクリックします。表示されるドロップダウン リストから、次のいずれかを選択します。選択した項目が、[Type] になります（図 10-12 を参照）。

- [Collect Config]：デバイスからコンフィギュレーションを収集します。
- [Collect Config From Files]：Prime Diagnostics に対してのみ、ファイルからコンフィギュレーションを収集します。
- [Enable Disable VFW Traps]：VFW トラップをイネーブルまたはディセーブルにします。
- [L2VPN (L2TPv3) Functional Audit]：
- [Password Management]：ユーザ パスワードと SNMP コミュニティ ストリングを管理します。
- [SLA Collection]：SLA がイネーブルなデバイスからデータを収集します。
- [Service Deployment]：既存の SR を展開します。
- [TE Full Discovery]：
- [TE Incremental Discovery]：
- [TE Interface Performance]：SNMP を使用するトンネルおよびインターフェイス帯域利用率を計算します。

図 10-12　タスクの作成



ステップ 2　[Name]：タスクの名前を入力します。デフォルト値を受け入れることができます。

ステップ 3　[Type]：ステップ 1 で定義されています。

ステップ 4　[Description]（オプション）：説明を入力します。

ステップ 5　[Task Configuration Method]（デフォルト：[Simplified]）：[Simplified] または [Advanced (via wizard)] を選択します。[Simplified] を選択すると、1 つのウィンドウの多くの選択を行うことができます。[Advanced（via wizard）] を選択すると、多数のウィンドウを移動して選択を行います。

ステップ 6　[Next] をクリックして続行します。

選択するタスクのタイプに従って、[Task Devices]、[Task Service Requests]、または [Configurations File Directory] ページがバリエーションとともに表示されます。

ステップ 7　必要な場合は、[Select/Deselect] をクリックしてデバイスまたはサービス要求を追加します。

（注）　ステップ 7 からステップ 10 は [Collect Config From Files] と [TE Interface Performance] には適用されません。

ステップ 8　結果の選択ウィンドウで、デバイスまたはサービス要求を選択し、[Select] をクリックします。

選択したデバイスまたはサービス要求が表示されます。

ステップ 9　[Groups] は、前の手順で指定するタスクによって、表示される場合と表示されない場合があります。これが表示された場合、ステップ 7 およびステップ 8 と同様に、デバイスのグループを追加できます。これが表示されない場合、またはこのデバイス グループ選択を完了した後、ステップ 10 に進みます。

ステップ 10　[Options] を選択します。

[Retrieve Interfaces] チェックボックスがオンの場合、Prime Provisioning は Simple Network Management Protocol（SNMP）を使用して ifIndex などのデバイス インターフェイス情報を取得します。[Retrieve Interfaces] チェックボックスがオフの場合でも、コンフィギュレーション収集情報は取得されますが、SNMP は使用されません。IP Service Level Agreement（SLA; サービス レベル契約）プローブ以外では、SNMP またはこのオプションは必要ありません。

ステップ 11　[Configuration File Directory] が表示されたら、Prime Provisioning サーバのディレクトリへのパスを [Configuration File Directory] テキスト ボックスに入力して、オフライン コンフィギュレーション ファイルが保存されている Prime Provisioning サーバのディレクトリを示します。

ステップ 12　[Schedule] については、[Now]、[Later]、または [None] をクリックします。[Later] を選択すると、[Later Schedule category] が表示されます。次に、[Edit] ボタンをクリックして、[Task Scheduler] ページを表示する必要があります。

ステップ 13　タスクをスケジューリングする情報を選択して、[OK] をクリックします（デフォルトのスケジュールは [Now] です）。

ステップ 14　続行するには、[Submit] をクリックします。

新しいタスクがタスクのリストに追加されます。

監査

監査情報を取得するには、[Tasks] ページで [Audit] をクリックします。表示されるドロップダウン リストから、次のいずれかを選択します。選択した項目が、[Type] になります。

- [Config Audit]：Prime Provisioning により生成されるコンフィグレットをデバイスのコンフィグレットと比較します。
- [L2VPN (L2TPv3) Functional Audit]：L2TPv3 機能を監査します。
- [MPLS Functional Audit]：MPLS 機能を監査します。
- [TE Functional Audit]：ルータの Label Switch Path（LSP; ラベル スイッチ パス）をリポジトリに格納されている LSP と比較します。

詳細

特定のタスクに関する詳細情報を取得するには、次の手順を実行します。

ステップ 1　[Tasks] ページから、情報の詳細リストを表示する、いずれかのタスクのチェックボックスをオンにします。

ステップ 2　[Details] をクリックします。

ステップ 3　[OK] をクリックして戻ります。

スケジューリング

既存のタスクのスケジューリングを変更するには、次のステップを実行します。

ステップ 1　[Tasks] ページから、スケジューリング方法をリセットする、いずれかのタスクのチェックボックスをオンにします。

ステップ 2　[Schedules] をクリックします。

ステップ 3　このタスクを削除する場合は、ステップ 4 に進みます。スケジューリング方法をリセットする場合は、ステップ 5 に進みます。

ステップ 4　新しいウィンドウで、削除するタスクのチェックボックスをオンにして、[Delete] ボタンをクリックします。次に、ステップ 7 に進みます。

ステップ 5　新しいウィンドウで、[Create] をクリックします。

ステップ 6　新しいスケジューリングの選択を行い、[Save] をクリックして、スケジューリング指示をリセットします。

ステップ 7　すべてのチェックボックスをオフにして、[OK] をクリックして戻ります。

ログ

[Tasks] ページでこの選択を行って、「タスク ログ」（P.10-29）で説明されている事柄を行うこともできます。

削除

1 つ以上のタスクを削除するには、次のステップを実行します。

ステップ 1　[Tasks] ページで、削除するタスクの 1 つ以上のチェックボックスをオンにします。

確認ウィンドウが表示されます。

ステップ 2　削除する場合は、[OK] をクリックします。削除しない場合は、[Cancel] をクリックします。

ステップ 3　更新された [Tasks] ページに戻ります。

タスク ログ

タスク ログを使用して、タスクが正常に完了したかどうか、タスクのステータスを確認できます。また、タスク ログを使用して、失敗したタスクをトラブルシューティングすることもできます。タスク ログを表示するには、次の手順に従います。

ステップ 1　[Operate] > [Tasks] > [Task Logs] をクリックします。

[Task Logs] ウィンドウが表示されます。

このウィンドウには、タスクの [Runtime Task Name]、[Action]、[Start Time]、[End Time]、および [Status] ごとにタスクが表示されます。このウィンドウを使用して、ログを表示または削除できます。

ステップ 2　ログを表示するには、タスクを表す行にあるチェックボックスをオンにして、[View Log] ボタンをクリックします。

[Task Log] ページが表示されます。

表示するログ レベルのタイプを設定できます。[Log Level] を指定し、[Filter] ボタンをクリックして表示する情報を表示します。

ステップ 3　[Return to Logs] をクリックして、表示する別のログを指定します。

レポート

[Inventory] > [Reports] > [Inventory Reports] を選択すると、レポートのツリーがデータ ペインに表示されます。データ ペインで各フォルダの + 記号をクリックすると、提供されたすべてのレポートのリストが表示されます。L2VPN フォルダの SAMPLE 以外のレポートと、MPLS フォルダの SAMPLE 以外のレポートについては、*『Cisco Prime Provisioning 6.3 User Guide』* で説明されています。

特定のレポートをクリックして、レポートの設定方法を定義できます。図 10-13 には、フォルダ **Inventory** の下にあるサンプル ファイルをが示されています。

図 10-13　[Inventory] > [SAMPLE - Template Report - Report] ウィンドウ

この項では、レポート機能と、次の領域でそれを使用する方法について説明します。

- 「レポートの概要」（P.10-30）
- 「レポートへのアクセス」（P.10-30）
- 「レポート GUI の使用」（P.10-30）
- 「レポートの実行」（P.10-31）
- 「カスタム レポートの作成」（P.10-33）

レポートの概要

ネットワーク オペレータは、通常、プロビジョニングされるサービスに関する詳細なレポートが必要となることがあります。たとえば、特定のカスタマーに対して、PE-CE 接続およびそれらの詳細な PE-CE 設定パラメータのリストを表示したり、PE での特定の Layer2 または Layer3 サービス要求を表示したりできます。これらのレポートは、一箇所から Service Request（SR; サービス要求）および VPN 情報を検出できるため、ネットワーク オペレータに役に立ちます。

[Inventory] > [Reports] > [Inventory Reports] を選択すると、タイプごとにレポートがグループ化され、簡単にナビゲーションできるようになります。Prime Provisioning には、ユーザが RBAC 権限を持つ、事前定義された（can された）レポートのみが表示されます。

フィルタリング基準と、レポートに表示される出力を選択できます。レポートは、さまざまな形式で保存できます。

『Cisco Prime Provisioning 6.3 User Guide』 で説明されている事前定義されたレポートのほかに、Prime Provisioning は追加のサンプル レポートを提供します。サンプル レポートは参考用としてのみ提供され、テストおよびサポートは行われません。

Prime Provisioning が GUI にレポートを提供するために使用するデータ構造は XML 形式で定義されます。

レポートへのアクセス

レポートにアクセスするには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI のレポート フレームワークにアクセスするには、[Inventory] > [Reports] > [Inventory Reports] を選択します。

ステップ 2　フォルダをクリックして、使用可能なレポートを表示します。

図 10-13 に示すように、[Reports] ウィンドウが表示されます。

ステップ 3　左側のナビゲーション ツリーのいずれかのフォルダの下にリストされているレポートから、目的のレポートをクリックすると、そのレポートに関連付けられたウィンドウが開きます。

（注）　各レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。ユーザは独自のカスタム レポートを作成するベースとしてこのレポートをサポートされているレポートとともに使用できます。カスタム レポートについては、「カスタム レポートの作成」（P.10-33）を参照してください。

レポート GUI の使用

この項では、レポート GUI を使用するいくつかの一般的なコメントを提供します。この情報はすべてのレポートに適用されます。レポートを呼び出すと、図 10-13 に示されているようなウィンドウが表示されます。

ウィンドウは複数のエリアに分割されています。

- 「レイアウト」（P.10-31）

- 「フィルタ」（P.10-31）
- 「出力フィールド」（P.10-31）
- 「ソート」（P.10-31）

レイアウト

この領域にはレポートのタイトルが表示され、チャート タイプを選択することができます。[Title] フィールドを上書きすることで、独自のレポート タイトルを入力できます。

（注）　表形式の出力のみがサポートされています。

フィルタ

このペインで、レポートの入力または検索条件を定義できます。ここに入力する値は、Prime Provisioning のリポジトリにあるデータ オブジェクト関連付けられた、対応する値と比較されます。値はすべてのフィールドに入力する必要があります。ストリング全体に、アスタリスク（*）をワイルドカードとして使用できます。

フィルタリング可能な各フィールドには、GUI でラベルとテキストの入力フィールドが表示されます。特定のフィールドについては、GUI で [Select] ボタンも表示され、既存のオブジェクトを選択できます（たとえば、[Customer]、[Service Type]、[SR State] など）。使用可能なすべての出力フィールドがウィンドウに表示され、レポートに含めるフィールドを選択できます。すべての出力フィールドはデフォルトで選択されています。

（注）　フィルタ値は、Prime Provisioning 内で表される値と同じ形式にする必要があります。たとえば、Service Request（SR）ID は数値にする必要があります。

出力フィールド

このペインでは、レポートに表示する出力フィールドを選択できます。マウスで出力フィールドの一部またはすべてを選択できます。出力値の連続した範囲を選択するには、Shift キーを使用します。出力値をランダムに選択するには Ctrl キーを使用します。

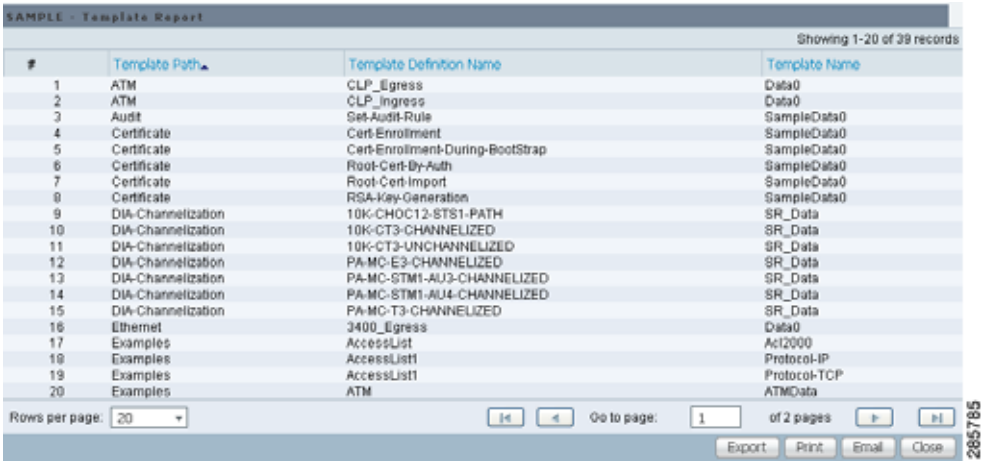
ソート

このペインでは、レポート出力をどのようにソートするかを選択できます。フィールドの場合は、最初のドロップダウン リストを選択して各フィルタ フィールドを選択し、2 番目のドロップダウン リストでレポート フィールドを昇順または降順のどちらで表示するのかを選択します。レポート出力を表示した後に、ソート順序を変更することもできます（図 10-14 を参照）。

レポートの実行

レポートを実行するには、レポート ウィンドウの右下隅の [View] をクリックします。これにより、レポート出力が生成されます。レポート出力の例を図 10-14 に示します。

図 10-14　レポート出力



レポート GUI は表形式の出力をサポートします。出力はレポート ウィンドウで選択した出力から取得された列でリストされます。

各行（またはレコード）は、レポート ウィンドウのフィルタ フィールドを使用して設定した検索基準との一致を示します。

場合によっては、フィールドに返される値は次のいずれかとして表示できます。

- **-1** は、このフィールドに更新された情報がないことを意味します
- **F** は false を意味します
- **T** は true を意味します

三角形アイコンの付いたカラム見出しは、レコードのソート基準になる出力です。カラムの見出しをクリックすることにより、ソートの昇順と降順を切り替えることができます。別の出力値でソートするには、その値のヘッダーをクリックします。

レポート出力のウィンドウから、次のボタンを使用して、エクスポート、印刷、または電子メールを行えます。

- [Export]（「レポートのエクスポート」（P.10-32）を参照）
- [Print]（「レポートの印刷」（P.10-33）を参照）
- [E-mail]（「電子メール レポート」（P.10-33）を参照）

レポートのエクスポート

図 10-14 の [Export] アイコンをクリックして、次の手順を実行します。

ステップ 1　目的の形式に該当するオプション ボタンを選択します。

- [PDF file]：Adobe の Portable Document Format。
- [CSV file]：データをさまざまなアプリケーションに簡単にエクスポートできるカンマ区切り値。

ステップ 2　保存する行を選択して、[OK] をクリックします。

Prime Provisioning は選択した形式でレポートを生成します。

（注）　出力を表示および保存するには、システムに適切なアプリケーションが必要です（たとえば、Acrobat Reader または Excel）。

レポートの印刷

図 10-14 で、[Print] アイコンをクリックします。

このウィンドウを使用して、印刷により適した形式でレポートを表示することができます。目的の行を選択して、[OK] をクリックします。結果が Web ブラウザに表示されます。そこから、レポートを印刷できます。

電子メール レポート

図 10-14 の [E-mail] アイコンをクリックして、次の手順を実行します。

ステップ 1　[To:] フィールド（必須）で、レポートの送信先となる 1 つ以上の電子メール アドレスを指定します。

ステップ 2　[From:] フィールド（任意）に、メッセージ ヘッダに表示される電子メール アドレスを入力します。

これにより、応答メッセージが有効な電子メール アドレスに送信されるようになります。

ステップ 3　[CC:] フィールド（任意）に、このレポートのコピーを受信する受信者の電子メールアドレスを入力します。

ステップ 4　件名フィールドは送信されたレポートのタイトルを示します。

このフィールドを上書きして、レポートの名前を変更できます。これは、電子メール メッセージの [Subject] フィールドに表示されます。

ステップ 5　レポートを送信するときの出力形式（PDF または CSV）のオプション ボタンを選択します。

ステップ 6　送信する行数を選択します。

ステップ 7　必要に応じて、[Message] フィールドに、レポートをアナウンスするにメッセージを入力してから [Send] をクリックします。

カスタム レポートの作成

各フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーション ファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/<*folder_name*>**_report.xml**

ここで、<*folder_name*> *は* **インベントリ**、**L2**、*または* **MPLS** *です。*

使用できる各レポート（サンプル レポートを含む）は、**packageDef name = "**<*folder_name*>**"** 下の <objectDef name> 開始および終了タグ内に含まれる XML コンテンツで定義されます。介入 XML コンテンツによって、レポートのタイトル、すべての許容可能なフィルタ パラメータ、出力、およびデフォルトのソート動作が指定されます。既存のレポートを変更したり、既存のレポートをコピーして新しいレポートのテンプレートとして使用したりできます。

これを実行するには、次のステップを実行します。

ステップ 1　**./prime.sh stopall** コマンドを使用して Prime Provisioning サーバを停止します。

Prime Provisioning の開始および停止の詳細については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』*を参照してください。

ステップ 2　適切な編集ツールを使用して、**$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/**<*folder_name*>**_report.xml**（ここで、<*folder_name*> は **Inventory**、**L2** または **MPLS**）コンフィギュレーション ファイルを開きます。

（注）　ファイルを変更する前に保存してください。

ステップ 3　必要に応じて、既存のレポートを変更するか、レポートをコピーして新しいレポートの基礎として使用します。

ステップ 4　変更した **$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/**<*folder_name*>**_report.xml** ファイルを保存します。

ステップ 5　**./prime.sh startwd** コマンドを使用して、Prime Provisioning を再始動します。

Prime Provisioning の開始および停止の詳細については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』*を参照してください。

Prime Provisioning を再始動した後、**$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/**<*folder_name*>**_report.xml** ファイルに行った変更に基づき、変更内容が反映されます。

L2 および VPLS のレポートの生成

Prime Provisioning のレポート GUI は、L2 や VPLS などの複数の Prime Provisioning モジュールで使用します。レポート GUI の使用、レポートの実行、レポートからの出力の使用、およびカスタマイズされたレポートの作成に関する全般的な説明については、「レポート」（P.10-29）を参照してください。この項の残りの部分では、Prime Provisioning で利用可能な L2 および VPLS のレポートについて説明します。

この項では、L2 および VPLS のレポートの生成について説明します。次の事項について説明します。

- 「L2 および VPLS のレポートへのアクセス」（P.10-34）
- 「L2 および VPLS のレポート」（P.10-35）
- 「L2 および VPLS のカスタム レポートの作成」（P.10-42）

L2 および VPLS のレポートへのアクセス

L2 および VPLS のレポートにアクセスするには、次の手順を実行します。

ステップ 1　Prime Provisioning GUI のレポート フレームワークにアクセスするには、[Inventory] > [Reports] > [Inventory Reports] を選択します。

[Reports] ウィンドウが表示されます。

ステップ 2　[L2] フォルダをクリックして使用可能な L2 および VPLS のレポートを表示します。

ステップ 3　レポートのアイコンをクリックすると、当該レポートの関連ウィンドウが表示されます。

各レポートの詳細については、「L2 および VPLS のレポート」（P.10-35）を参照してください。

L2 および VPLS のレポート

この項では、次の L2 および VPLS のレポートの詳細について説明します。

- 「L2 エンドツーエンド配線レポート」（P.10-35）
- 「L2 PE サービス レポート」（P.10-38）
- 「L2 VPN サービス レポート」（P.10-39）
- 「VPLS 接続回線レポート」（P.10-39）
- 「VPLS PE サービス レポート」（P.10-41）
- 「VPLS VPN レポート」（P.10-41）

（注）　L2 レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。独自のカスタム レポートを作成するベースとして、このレポートを使用できます。詳細については、「L2 および VPLS のカスタム レポートの作成」（P.10-42）を参照してください。

各レポートで提供される情報は次のとおりです。

- レポートの説明または目的。
- レポート ウィンドウの図。
- フィルタ値と説明のリスト。
- 出力値と説明のリスト。

L2 エンドツーエンド配線レポート

L2 エンドツーエンド配線とは、2 本の接続回線を含むポイントツーポイント接続を指します。L2 エンドツーエンド配線レポートは、L2 エンドツーエンド接続上で実行中のサービスを表示します。このレポートを使用すると、接続ごとのすべてのサービスと該当する接続回線の属性を表示できます。

L2 エンドツーエンド配線レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [EndToEndWire ID]：エンドツーエンド配線の ID 番号。
- [Customer Name]：カスタマーの名前。
- [VC ID]：仮想回線の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [Service Type]：サービスのタイプ。値は次のとおりです。
  - ATM
  - ATM_NO_CE
  - FRAME_RELAY

  - FRAME_RELAY_NO_CE
  - L2VPN_ERS
  - L2VPN_ERS_NO_CE
  - L2VPN_EWS
  - L2VPN_EWS_NO_CE
- [SR State]：サービス要求の状態。値は次のとおりです。
  - BROKEN
  - DEPLOYED
  - FAILED_AUDIT
  - FAILED_DEPLOY
  - FUNCTIONAL
  - INVALID
  - LOST
  - PENDING
  - REQUESTED
  - WAIT_DEPLOY
- [AC1-ID]：第 1 接続回線（AC1）の ID 番号。
- [AC2-ID]：第 2 接続回線（AC2）の ID 番号。

出力値：

- [EndToEndWire ID]：エンドツーエンド配線の ID 番号。
- [Customer Name]：カスタマーの名前。
- [VPN]：VPN の名前。
- [VC ID]：仮想回線の ID 番号。
- [SR ID]：サービス要求の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [Service Type]：サービスのタイプ。
- [SR State]：サービス要求の状態。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [AC1-ID]：第 1 接続回線（AC1）の ID 番号。
- [AC1-UNI Device Interface]：第 1 接続回線（AC1）の UNI デバイス インターフェイス。
- [AC1-NPC]：第 1 接続回線（AC1）の名前付き物理回線。
- [AC2-VLAN ID/DLCI/VCD]：第 1 接続回線（AC1）の VLAN ID 番号、Data-Link Connection Identifier（DLCI; データリンク接続識別子）または Virtual Circuit Descriptor（VCD; 仮想回線記述子）。
- [AC1-VPI]：第 1 接続回線（AC1）の仮想パス ID。
- [AC1-VCI]：第 1 接続回線（AC1）の仮想チャネル ID。

- [AC1-Interface Encap Type]：第 1 接続回線（AC1）で使用されるカプセル化のタイプ。
- [AC1-AccessDomain]：第 1 接続回線（AC1）のアクセス ドメイン名。
- [AC1-Customer Facing UNI]：第 1 接続回線（AC1）のカスタマー側の UNI ポート。
- [AC1-Loopback IP Address]：第 1 接続回線（AC1）のループバック アドレス。
- [AC1-STP Shutdown Threshold]：第 1 接続回線（AC1）のスパニングツリー プロトコルのシャットダウンしきい値（パケット数/秒）。
- [AC1-VTP Shutdown Threshold]：第 1 接続回線（AC1）の VLAN トランク プロトコルのシャットダウンしきい値（パケット数/秒）。
- [AC1-CDP Shutdown Threshold]：第 1 接続回線（AC1）の Cisco Discovery Protocol のシャットダウンしきい値（パケット数/秒）。
- [AC1-STP Drop Threshold]：第 1 接続回線（AC1）のスパニングツリー プロトコルのドロップしきい値（パケット数/秒）。
- [AC1-CDP Drop Threshold]：第 1 接続回線（AC1）の Cisco Discovery Protocol のドロップしきい値（パケット数/秒）。
- [AC1-VTP Drop Threshold]：第 1 接続回線（AC1）の VLAN トランク プロトコルのドロップしきい値（パケット数/秒）。
- [AC1-UNI Recovery Interval]：第 1 接続回線（AC1）の UNI ポートの回復間隔（秒）
- [AC1-UNI Speed]：第 1 接続回線（AC1）の UNI ポートの速度。
- [AC1-UNI Shutdown]：第 1 接続回線（AC1）の UNI ポートのシャットダウン ステータス。
- [AC1-UNI PortSecurity]：第 1 接続回線（AC1）の UNI ポートのセキュリティのステータス。
- [AC1-UNI Duplex]：第 1 接続回線（AC1）の UNI ポートのデュプレックス ステータス（[none]、[full]、[half] または [auto]）。
- [AC1-Maximum MAC Address]：第 1 接続回線（AC1）の UNI ポートに許可される最大 MAC アドレス。
- [AC1-UNI Aging]：第 1 接続回線（AC1）の UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。
- [AC2-ID]：第 2 接続回線（AC2）の ID 番号。
- [AC2-UNI Device Interface]：第 2 接続回線（AC2）の UNI デバイス インターフェイス。
- [AC2-NPC]：第 2 接続回線（AC2）の名前付き物理回線。
- [AC2-VLAN ID/DLCI/VCD]：第 2 接続回線（AC2）の VLAN ID、DLCI または VCD。
- [AC2-VPI]：第 1 接続回線（AC2）の仮想パス ID。
- [AC2-VCI]：第 1 接続回線（AC2）の仮想チャネル ID。
- [AC2-Interface Encap Type]：第 2 接続回線（AC2）で使用されるカプセル化のタイプ。
- [AC2-AccessDomain]：第 2 接続回線（AC2）のアクセス ドメイン名。
- [AC2-Customer Facing UNI]：第 2 接続回線（AC2）のカスタマー側の UNI ポート。
- [AC2-Loopback IP Address]：第 2 接続回線（AC2）のループバック アドレス。
- [AC2-STP Shutdown Threshold]：第 2 接続回線（AC2）のスパニングツリー プロトコルのシャットダウンしきい値。
- [AC2-VTP Shutdown Threshold]：第 2 接続回線（AC2）の VLAN トランク プロトコルのシャットダウンしきい値。

- [AC2-CDP Shutdown Threshold]：第 2 接続回線（AC2）の Cisco Discovery Protocol のシャットダウンしきい値。
- [AC2-STP Drop Threshold]：第 2 接続回線（AC2）のスパニングツリー プロトコルのドロップしきい値。
- [AC2-CDP Drop Threshold]：第 2 接続回線（AC2）の Cisco Discovery Protocol のドロップしきい値。
- [AC2-VTP Drop Threshold]：第 2 接続回線（AC2）の VLAN トランク プロトコルのドロップしきい値。
- [AC2-UNI Recovery Interval]：第 2 接続回線（AC2）の UNI ポートの回復間隔。
- [AC2-UNI Speed]：第 2 接続回線（AC2）の UNI ポートの速度。
- [AC2-UNI Shutdown]：第 2 接続回線（AC2）の UNI ポートのシャットダウン ステータス。
- [AC2-UNI PortSecurity]：第 2 接続回線（AC2）の UNI ポートのセキュリティのステータス。
- [AC2-UNI Duplex]：第 2 接続回線（AC2）の UNI ポートのデュプレックス ステータス（[none]、[full]、[half] または [auto]）。
- [AC2-Maximum MAC Address]：第 2 接続回線（AC2）の UNI ポートに許可される最大 MAC アドレス。
- [AC2-UNI Aging]：第 2 接続回線（AC2）の UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。

L2 PE サービス レポート

L2 PE サービス レポートを使用すると、PE を選択したり、PE のロール（たとえば、[N-PE]、[U-PE] または [PE-AGG]）やその場所で実行中の L2 関連のサービスを表示したりできます。

L2 PE サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [PE Role]：PE デバイスのロール（N-PE、U-PE、または PE-AGG）。
- [PE Name]：PE デバイス名。

出力値：

- [PE Role]：PE デバイスのロール（N-PE、U-PE、または PE-AGG）。
- [PE Name]：PE デバイス名。
- [SR ID]：サービス要求の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [SR State]：サービス要求の状態。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [Service Type]：サービスのタイプ。

L2 VPN サービス レポート

L2 VPN レポートを利用すると、VPN を遡って VLAN ID または VC ID あるいはその両方を追跡できるため、カスタマーはすべてのリンクやすべての VPN サービスを繰り返したどる必要がなくなります。VLAN ID または VC ID を指定すると、該当するカスタマーおよび VPN の詳細がレポートに表示されます。

L2 VPN レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [VLAN ID]：VLAN ID 番号。
- [VC ID]：仮想回線の ID 番号。
- [Customer Name]：カスタマーの名前。
- [Access Domain]：アクセス ドメイン名。

出力値：

- [VLAN ID]：VLAN ID 番号。
- [VC ID]：仮想回線の ID 番号。
- [SR Job ID]：サービス要求ジョブの ID 番号。
- [VPN]：VPN の名前。
- [Customer Name]：カスタマーの名前。
- [Service Type]：サービスのタイプ。
- [Access Domain]：アクセス ドメイン名。
- [Provider Name]：プロバイダー名。

VPLS 接続回線レポート

VPLS 接続回線レポートは、指定されたカスタマーの VPN の接続回線の詳細情報を表示します。

VPLS 接続回線レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [SR ID]：サービス要求の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [SR State]：サービス要求の状態。値は次のとおりです。
  - BROKEN
  - DEPLOYED
  - FAILED_AUDIT
  - FAILED_DEPLOY
  - FUNCTIONAL
  - INVALID
  - LOST
  - PENDING
  - REQUESTED
  - WAIT_DEPLOY

- [Customer Name]：カスタマーの名前。
- [VPN]：VPN の名前。
- [Service Type]：サービスのタイプ。値は次のとおりです。
  - VPLS_ERS
  - VPLS_ERS_NO_CE
  - VPLS_EWS
  - VPLS_EWS_NO_CE
- [VLAN ID]：VLAN ID 番号。
- [AccessDomain]：アクセス ドメイン名。

出力値：

- [VPLS Link ID]：VPLS リンクの ID 番号。
- [SR ID]：サービス要求の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [SR State]：サービス要求の状態。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [Customer Name]：カスタマーの名前。
- [VPN]：VPN の名前。
- [Service Type]：サービスのタイプ。
- [VLAN ID]：VLAN ID 番号。
- [Policy Name]：VPLS ポリシー名。
- [VFI Interface]：仮想転送インターフェイス名。
- [Customer Facing UNI]：カスタマー側の UNI ポート。
- [AccessDomain]：アクセス ドメイン名。
- [NPC]：名前付き物理回線。
- [UNI Port]：UNI ポート。
- [UNI Shutdown]：UNI ポートのシャットダウン ステータス。
- [UNI Aging]：UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。
- [UNI Speed]：UNI ポートの速度。
- [UNI Duplex]：UNI ポートのデュプレックス ステータス（[none]、[full]、[half] または [auto]）。
- [Maximum MAC Address]：UNI ポートで許可される最大 MAC アドレス。
- [CDP Shutdown Threshold]：UNI ポートの Cisco Discovery Protocol のシャットダウンしきい値（パケット数/秒）。
- [STP Shutdown Threshold]：UNI ポートのスパニングツリー プロトコルのシャットダウンしきい値（パケット数/秒）。

- [VTP Shutdown Threshold] : UNI ポートの VLAN トランク プロトコルのシャットダウンしきい値（パケット数 / 秒）。
- [CDP Drop Threshold] : UNI ポートの Cisco Discovery Protocol のドロップしきい値（パケット数 / 秒）。
- [VTP Drop Threshold] : UNI ポートの VLAN トランク プロトコルのドロップしきい値（パケット数 / 秒）。
- [STP Drop Threshold] : UNI ポートのスパニングツリー プロトコルのドロップしきい値（パケット数 / 秒）。
- [Recovery Interval] : UNI ポートの回復間隔（秒）。

VPLS PE サービス レポート

VPLS PE サービス レポートを使用すると、PE を選択したり、PE のロール（たとえば、[N-PE]、[U-PE] または [PE-AGG]）やその場所で実行中の VPLS サービスを表示したりできます。

VPLS PE サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [PE Role] : PE デバイスのロール（N-PE、U-PE、または PE-AGG）。
- [PE Name] : PE デバイス名。

出力値：

- [PE Role] : PE デバイスのロール（N-PE、U-PE、または PE-AGG）。
- [PE Name] : PE デバイス名。
- [SR ID] : サービス要求の ID 番号。
- [SR Job ID] : サービス要求ジョブ ID 番号。
- [Service Type] : サービスのタイプ。
- [SR State] : サービス要求の状態。

（注） [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

VPLS VPN レポート

VPLS VPN レポートを利用すると、VPN を遡って VLAN ID または VFI 名あるいはその両方を追跡できるため、カスタマーはすべてのリンクやすべての VPN サービスを繰り返したどる必要がなくなります。VLAN ID または VFI 名を指定すると、該当するカスタマーおよび VPN の詳細がレポートに表示されます。

VPLS VPN レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [VLAN ID] : VLAN ID 番号。
- [Customer Name] : カスタマーの名前。
- [VFI Name] : 仮想転送インターフェイス名。
- [Access Domain] : アクセス ドメイン名。

出力値：

- [VLAN ID]：VLAN ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [VPN]：VPN の名前。
- [Customer Name]：カスタマーの名前。
- [Service Type]：サービスのタイプ。
- [VFI Name]：仮想転送インターフェイス名。
- [Access Domain]：アクセス ドメイン名。
- [Provider Name]：プロバイダー名。

L2 および VPLS のカスタム レポートの作成

L2 フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーション ファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

$ISC_HOME/**resources/nbi/reports/ISC/l2_report.xml**

レポート コンフィギュレーション ファイルを変更して、カスタム レポートを作成する方法の詳細については、「レポート」（P.10-29）を参照してください。

MPLS レポートの生成

Prime Provisioning のレポート GUI は、MPLS などの複数の Prime Provisioning モジュールで使用します。この章の残りの部分では、ISC で使用可能な MPLS レポートについて説明します。

この項では、MPLS のレポートの生成について説明します。次の事項について説明します。

MPLS レポートへのアクセス

MPLS レポートにアクセスするには、次の手順を実行します。

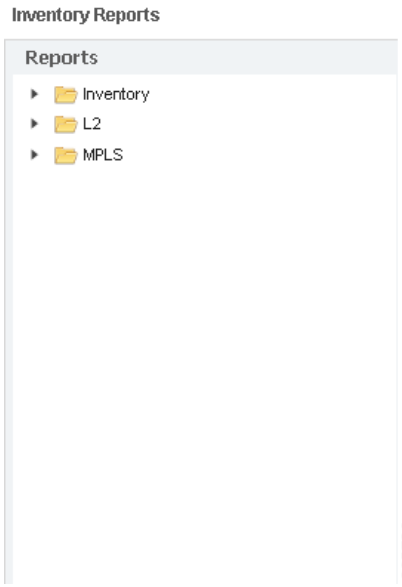
ステップ 1　Prime Provisioning にログインします。

ステップ 2　[Inventory] > [Reports] > [Inventory Reports] に移動します。

ステップ 3　[MPLS] フォルダをクリックして使用可能な MPLS のレポートを表示します。

図 10-15 に示すように、[Reports] ウィンドウが表示されます。

図 10-15　レポート リスト



ステップ 4　左側のナビゲーション ツリーの MPLS の下にリストされているレポートから、目的のレポートをクリックすると、そのレポートに関連付けられたウィンドウが開きます。

（注）　MPLS レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。ユーザは独自のカスタム レポートを作成するベースとしてこのレポートをサポートされているレポートとともに使用できます。カスタム レポートの詳細については、「カスタム レポートの作成」（P.10-47）を参照してください。

レポートの実行

レポートを実行するには、レポート ウィンドウの右下隅の [View] をクリックします。これにより、レポート出力が生成されます。MPLS サービス要求レポート出力の例。

ISC の現在のリリースでは、レポート GUI が表形式での出力をサポートしています。出力はレポート ウィンドウで選択した出力から取得された列でリストされます。

各行（またはレコード）は、レポート ウィンドウのフィルタ フィールドを使用して設定した検索基準との一致を示します。

三角形アイコンの付いたカラム見出しは、レコードのソート基準になる出力です。カラムの見出しをクリックすることにより、ソートの昇順と降順を切り替えることができます。別の出力値でソートするには、その値のヘッダーをクリックします。

MPLS PE サービス レポート

MPLS PE サービス レポートを使用すると、PE を選択したり、PE のロール（たとえば、[N-PE]、[U-PE] または [PE-AGG]）やその場所で実行中の MPLS 関連のサービスを表示したりできます。

MPLS サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます（図 10-16 を参照）。

図 10-16　MPLS PE サービス レポート

フィルタ値

- [PE Role]：PE デバイスのロール（N-PE、U-PE、または PE-AGG）。
- [PE Name]：PE デバイス名。

出力値

- [PE Role]：PE デバイス ロール（N-PE、U-PE または PE-AGG）別にリストされます。
- [PE Name]：PE デバイス名ごとにリストします。
- [Policy Type]：ポリシーのタイプごとにリストします。
- [SR State]：サービス要求状態別にリストされます（「サービス要求状態」（P.8-13）を参照）。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

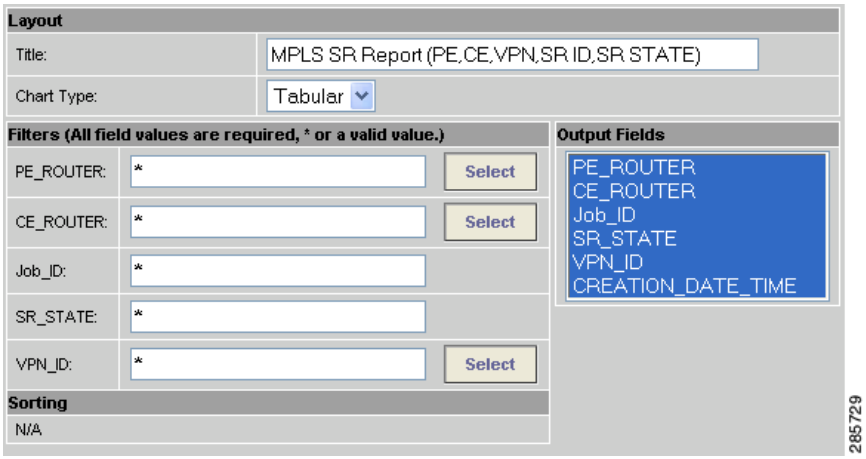
- [SR ID]：サービス要求 ID ごとにリストします。
- [SR Job ID]：サービス要求ジョブ ID ごとにリストします。

MPLS サービス要求レポート

MPLS サービス要求のレポート機能を使用して、[PE]、[CE]、[VPN]、[SR ID]、[SR STATE] に関連するサービス要求をリストできます。

MPLS サービス要求レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます（図 10-17 を参照）。

図 10-17　MPLS サービス要求レポート



フィルタ値

- [PE ROUTER]：一部またはすべて（*）の PE ルータを選択します。
- [CE ROUTER]：一部またはすべて（*）の CE ルータを選択します。
- [Job ID]：サービス要求のジョブ ID。
- [SR STATE]：サービス要求のステータス（「サービス要求状態」（P.8-13）を参照）。
- [VPN ID]：一部またはすべて（*）の VPN を ID によって選択します。

出力フィルタ

- [PE ROUTER]：PE ルータを示します。
- [CE ROUTER]：CE ルータを示します。
- [Job ID]：ジョブ ID ごとにリストします。
- [SR STATE]：サービス要求のステータス（「サービス要求状態」（P.8-13）を参照）。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

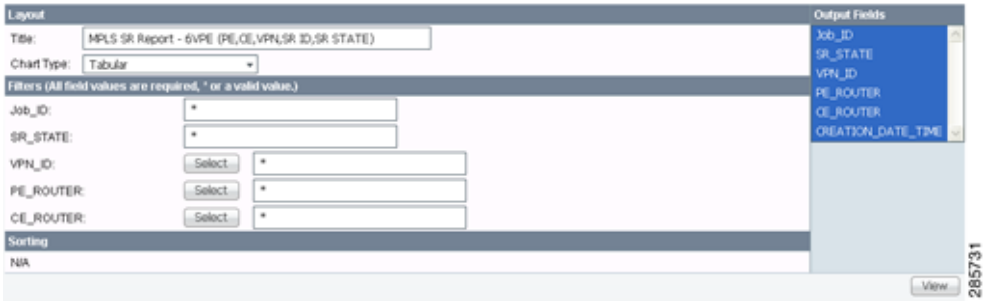
- [VPN ID]：VPN ID ごとにリストします。
- [CREATION DATE TIME]：レポートが作成された日付および時間ごとにリストします。

MPLS サービス要求のレポート：6VPE

MPLS サービス要求のレポート：6VPE レポート機能を使用して、[PE]、[CE]、[VPN]、[SR ID]、[SR STATE] に関連するサービス要求をリストできます。

[MPLS Service Request Report - 6VPE] のアイコンをクリックすると、このレポートのウィンドウが表示されます（図 10-18 を参照）。

図 10-18　MPLS サービス要求のレポート：6VPE



フィルタ値

- [Job ID]：サービス要求のジョブ ID。
- [SR STATE]：サービス要求のステータス（「サービス要求状態」（P.8-13）を参照）。
- [VPN ID]：一部またはすべて（*）の VPN を ID によって選択します。
- [PE ROUTER]：一部またはすべて（*）の PE ルータを選択します。
- [CE ROUTER]：一部またはすべて（*）の CE ルータを選択します。

出力フィルタ

- [Job ID]：ジョブ ID ごとにリストします。
- [SR STATE]：サービス要求のステータス（「サービス要求状態」（P.8-13）を参照）。

（注）　[SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [VPN ID]：VPN ID ごとにリストします。
- [PE ROUTER]：PE ルータを示します。
- [CE ROUTER]：CE ルータを示します。
- [CREATION DATE TIME]：レポートが作成された日付および時間ごとにリストします。

6VPE サポート対象デバイスのレポート

（注）　Prime Provisioning GUI では、このレポートは [Inventory] > [Reports] > [Inventory Reports] の下にあります。

[6VPE Supported Devices Report] アイコンをクリックすると、このレポートのウィンドウが表示されます（図 10-19 を参照）。

図 10-19　6VPE サポート対象デバイスのレポート

フィルタ値

- [Host Name]：ホスト名。
- [Management Address]：管理アドレス。
- [Software Version]：ソフトウェアのバージョン。

出力フィルタ

- [Host Name]：ホスト名。
- [Management Address]：管理アドレス。
- [Software Version]：ソフトウェアのバージョン。

カスタム レポートの作成

MPLS フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーション ファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

$ISC_HOME/resources/nbi/reports/ISC/mpls_report.xml

TEM レポートおよびログの生成

すべての展開および収集タスクはモニタされ、タスクの詳細が記録されます。この情報は、タスク モニタリング ページを使用して表示できます。

この項では、次の内容について説明します。

- 「TE タスク ログ」（P.10-47）
  - 「SR 展開ログ」（P.10-48）
  - 「タスク マネージャから作成されるログ」（P.10-48）
  - 「タスク ログの表示」（P.10-48）
- 「TE パフォーマンス レポート」（P.10-49）。

TE タスク ログ

TE タスク ログは、1 つ以上の TE タスクを実行した結果を表示するときに使用されます。イベントにより、異なるタスク ログが生成されます。

- SR 展開ログ

- 次のような、タスク マネージャから発行されるタスクにより生成されるログ
  - TE ディスカバリ
  - TE 機能監査
  - TE インターフェイス パフォーマンス

SR 展開ログ

サービス要求が展開されると、管理対象または対象外のプライマリ トンネルまたはバックアップ トンネルに関係なく、ログが生成されます。トンネル SR では、展開は、SR のタイプに応じて、複数の段階で発生します。また、同様に、タスク ログが作成されます。

- プライマリ トンネル SR：3 段階の展開に対応する 3 段階のロギング プロセス
- 保護 SR：2 段階の展開に対応する 2 段階のロギング プロセス

展開ログのほか、展開が成功した場合、SR 展開のタイプに関係なく、ConfigAudit ログが作成されます。

タスク マネージャから作成されるログ

TE ディスカバリ タスクのタスク ログを生成および表示する手順については、「タスク ログ」（P.10-29）を参照してください。

TE 機能監査および TE インターフェイス パフォーマンス タスクのタスク ログを生成および表示する手順については、「TE タスクの作成」（P.7-76）を参照してください。

タスク ログの表示

タスク ログは、異なる 2 つの場所からアクセスできます。

- [Tasks] ウィンドウ
- [Service Requests] ウィンドウ

[Tasks] ウィンドウから

TE タスクのタスク ログを表示するには、次のことを実行する必要があります。

1. [Task Logs] ウィンドウにアクセスします。
2. 必要なログを選択して開きます。

タスク ログを表示するには、次のステップを実行します。管理対象のプライマリ トンネルの展開のタスク ログを例として使用します。

ステップ 1　[Operate] > [Task Logs] を選択します。

[Task Logs] ウィンドウが表示されます。

[Task Logs] ウィンドウに次の情報が示されます。

- [Runtime Task Name]：実行時タスクがいつ作成されたかを指定する、属性が自動的に指定されたタスク名。
- [Action]：タスクのタイプ。たとえば、[TE Discovery]、[TE Functional Audit]、または [TE Interface Performance]。
- [Start Time]：実行時タスクが開始したときの日付および時刻。
- [End Time]：実行時タスクが終了した日時。

- [Status]：実行時タスクの事前設定ステータスを示します。

ステップ 2　表示するタスク ログを選択します。

複数の実行がスケジュールされているタスクには、表示するインスタンスが複数ある場合があります。

ステップ 3　[Action] カラムで目的のタスクをクリックします。

対応する [Task Log] ウィンドウが表示されます。このウィンドウの GUI 要素は、[Service Request Manager] ウィンドウにもあります。

記録されたメッセージがテーブルに表示されます。これには、ログ メッセージが作成された時刻、およびログ メッセージに割り当てられた重大度が含まれます。

ロギングのフィルタ設定（デフォルトは [SEVERE]）があります。デフォルトの場合、[SEVERE] のログ メッセージだけが表示されます。目的の詳細レベルに応じて選択できるいくつかの異なるフィルタ設定があります。フィルタ レベルを変更するには、必要なフィルタ レベルを選択し、[Filter] をクリックします。

ログの構造は、実行されたタスクのタイプにより異なります。

ステップ 4　[Return to Logs] をクリックして、ログ ウィンドウを閉じます。

これにより、メインの [Task Logs] ウィンドウに戻ります。

ステップ 5　タスク SR（特定のタスク ログに関連付けられている場合があります）を参照するには、目的のタスク ログを選択して、[Service Requests] ボタンをクリックします。

[Task SRs] ウィンドウが表示されます。

[Service Requests] ウィンドウから

[Service Requests] ウィンドウからログにアクセスするには、次の手順を実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　サービス要求（1 つだけ）を選択します。

ステップ 3　[Status] ボタンをクリックして、[Logs] を選択します。

ステップ 4　表示するログを選択して、[View Log] をクリックします。

[Task Log] ウィンドウが表示されます。

ステップ 5　ドロップダウン メニューからログ レベルを選択して、[Filter] をクリックします。

ログ レベルには、[All]、[Severe]、[Warning]、[Info]、[Config]、[Fine]、[Finer]、および [Finest] があります。

TE パフォーマンス レポート

TE パフォーマンス レポートは、TE インターフェイス パフォーマンス タスクを実行するときに作成されます（「TE インターフェイス パフォーマンス タスクの作成」（P.7-78）を参照）。

このレポートには、選択されたトンネルまたはリンクあるいはその両方の TE インターフェイス パフォーマンス タスクから収集されたトラフィック データが表示されます。TE インターフェイス パフォーマンス タスクは、複数回実行できます。

TE パフォーマンス レポートを表示するには、次のステップを実行します。

ステップ 1　[Inventory] > [Reports] > [Inventory Reports] を選択します。

[TE Performance Report Table] が表示されます。

[TE Performance Report Table] ウィンドウには、次の GUI 要素があります。

- [Report table]：インターフェイス パフォーマンス タスクのリストを示します。
  - [Start Time]：実行時タスクが開始したときの日付および時刻。
  - [End Time]：実行時タスクが終了した日時。
  - [Device Name]：デバイスの名前。
  - [Interface Name]：リンク上のインターフェイスの IP アドレス。
  - [Octets In]：トラフィックの着信オクテットの数。
  - [Octets Out]：トラフィックの発信オクテットの数。
  - [Speed]：インターフェイスの速度。
  - [Util In]：着信トラフィックのインターフェイスの使用率。
  - [Util Out]：発信トラフィックのインターフェイスの使用率。
- [Reconcile Data]：インターフェイス パフォーマンス タスクがインターフェイスで複数回実行された場合は、次の基準に従ってデータを調整するように選択できます。
  - [Peak]：最高のインターフェイス使用率を選択します。
  - [Valley]：最低のインターフェイス使用率を選択します。
  - [Average]：平均のインターフェイス使用率を選択します。
  - [First]：インターフェイス使用率の最初のオカレンスを選択します。

CHAPTER 11

診断の実行

この章では、Cisco Prime Provisioning 6.3 での Diagnostics アプリケーションについて説明します。

概要

この項では、Cisco Prime Provisioning Diagnostics アプリケーションの概要について説明します。

この章の構成は、次のとおりです。

診断の概要

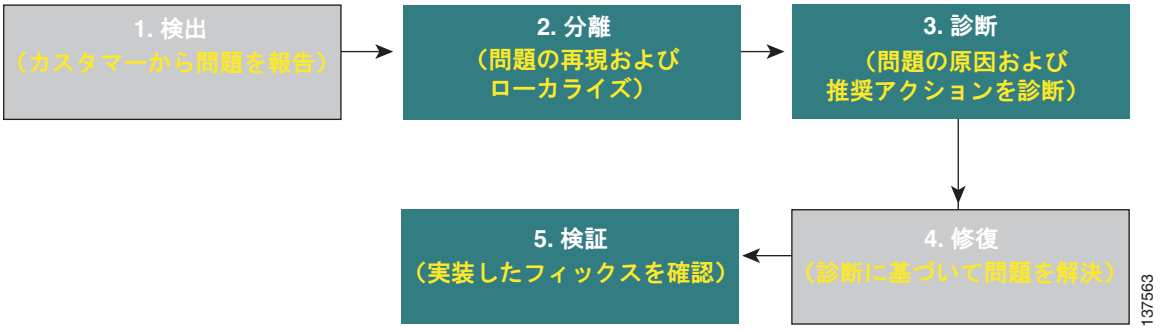
Diagnostics はワークフローに基づいた自動ネットワーク管理アプリケーションで、マルチプロトコル ラベル スイッチング（MPLS）VPN の問題をトラブルシューティングおよび診断します。Diagnostics は、MPLS に関連するネットワーク停止の診断に要する時間を削減するための機能を提供します。多くの場合、時間単位から分単位に短縮されます。診断は、ネットワーク障害シナリオに基づいて、MPLS のアクセス、エッジ、およびコアの各ネットワーク間で実行されます。サービス プロバイダーおよび企業の「自己導入」の、両方の MPLS VPN ネットワークに同様に適用できます。Network Operations Center（NOC; ネットワーク オペレーション センター）は技術者をサポートします。本製品以降は、第 2 次および第 3 次のサポートも受けることができるようになりました。Diagnostics は、オプションで、Prime Provisioning MPLS VPN プロビジョニング コンポーネントと統合できます。MPLS VPN の中核となる問題を診断するには、Label-Switched Path（LSP; ラベルスイッチド パス）ping および LSP traceroute など、MPLS のオペレーションおよびメンテナンス（OAM）機能をサポートする Cisco IOS ソフトウェア リリースおよび IOS XR ソフトウェア リリースが必要です。

障害の発見やトラブルシューティングを効果的に行うため、次の 5 つのステップを踏みます。

1. 検知
2. 分離
3. 診断
4. 修復
5. 確認

Diagnostics は、エンド カスタマーが VPN サービスを使用して問題をレポートするような、反応的な状況をサポートすることを目的として設計されています。これは、基本的に、図 11-1 の「診断」のステップに該当します。ルータ デバイスに加えられた変更を徹底して自ら管理し、それを行うための社内手順を定めているプロバイダーが多いため、「修復」機能はサポートされません。

図 11-1　　反応的な障害ライフサイクル



（注）　ステップ 2、3、および 5 は Diagnostics によって実行されます。ステップ 1 と 4 は手動で実行する必要があります。

Diagnostics では、「分離」、「診断」、および「検証」のステップを重点的に扱います。ネットワークでの障害の分離および診断、障害の発生したデバイスの特定、適切なデバイス ステータスのチェック、および障害発生の考えられる理由を特定するための設定を行うための貴重な機能を提供します。また、Diagnostics は、デバイス設定に加えた変更によって問題が解決されたことを検証するため、テストを再実行する機能も提供します。

この機能は、Prime Provisioning のその他のモジュール（VPN プロビジョニングや Traffic Engineering Management など）に依存せず、単独で使用できます。また、その他の Prime Provisioning モジュールが一部またはすべて使用されている Prime Provisioning インストールでも使用できます。MPLS VPN プロビジョニング機能が使用された場合は、カスタマー データおよび VPN データをトラブルシューティングの開始点として使用し、どのエンドポイント（カスタマー エッジ デバイスなど）間の接続をテストするかを特定できます。

Diagnostics はトラブルシューティングだけでなく、VPN ポストプロビジョニング チェックにも使用できます。VPN を展開した後、手動でまたは Prime Provisioning VPN プロビジョニング機能を使用して接続テストを実行し、VPN が正常にプロビジョニングされているかどうかを検証できます。

（注）　Diagnostics では、基礎となる設定またはルーティングのトラブルシューティング中の変更がサポートされません。Diagnostics の実行中にオペレータまたはルータのコントロール プレーンにより加えられた変更は、いずれも実行される実際のトラブルシューティングには反映されません。このような変更が加えられた場合、Diagnostics で正しい障害シナリオや観察の結果が得られるとは限りません。

前提となる知識

Diagnostics は、MPLS VPN について最低限の知識を持ったユーザによる使用を前提として設計されています。Diagnostics の MPLS VPN 接続性検証テストは、MPLS VPN についてほとんど、またはまったく知らないユーザでも実行できます。また、必要に応じてテスト結果をエクスポートし、MPLS VPN に詳しいエンジニアに解釈してもらうこともできます。ただし、MPLS VPN はもともと複雑であ

るため、RFC 2547 に従って MPLS VPN について習熟し、Diagnostics の利点を最大限に生かすことを推奨します。特に、RFC 2547 アークテクチャ、トポロジ、制御、およびデータ プレーンの知識は、アプリケーションを最大限に利用する方法を理解し、結果を解釈するうえで役立ちます。

Diagnostics は現在、IETF RFC 4379 準拠のラベル スイッチド パス（LSP）ping および LSP traceroute を使用するシスコ デバイスおよびネットワークを診断します。Diagnostics は、Cisco IOS で使用可能な先行のドラフト（ドラフト 3）も継続してサポートしています。ネットワーク内のすべてのデバイスで、一貫した LSP ping および traceroute のドラフトを使用する必要があります。

推奨文献：

- 『MPLS and VPN Architectures』Ivan Pepelnjak、Jim Guichard（Cisco Press）
- 『Troubleshooting Virtual Private Networks』Mark Lewis（Cisco Press）
- LSP ping/trace RFC：http://www.ietf.org/rfc/rfc4379.txt
- RFC 2547：http://www.ietf.org/rfc/rfc2547.txt?number=2547
- RFC 4379：http://www.ietf.org/rfc/rfc4379.txt?number=4379
- MPLS Embedded Management：LSP Ping/Traceroute and AToM VCCV: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gslsppt.html

サポートされているハードウェア、IOS、および IOS XR バージョン

サポートされているプロバイダー（P）およびプロバイダー エッジ（PE）ネットワーク デバイスのタイプおよび関連する Cisco IOS および IOS XR バージョンの詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』*を参照してください。

（注）　その他のデバイス タイプ、IOS、および IOS XR バージョンのサポートが、パッチ リリースで追加される場合があります。最新のパッチ リリースとサポートされているデバイス タイプ、IOS、および IOS VR バージョンの詳細については、Cisco.com を参照してください。

「Prime Provisioning サービスの設定」（P.3-6）で説明されているデバイス タイプ、IOS、および IOS XR バージョンは、MPLS ラベル スイッチド パス（LSP）の ping および traceroute 機能をサポートしています。この機能は、Diagnostics のトラブルシューティングに必要です。すべての P および PE デバイスがサポートされているデバイス タイプ、IOS、および IOS XR バージョンのリストに準拠していれば、Diagnostics はアクセス回線、MPLS VPN、および MPLS コアの問題をトラブルシューティングできます。Diagnostics は、他社製品などのその他のデバイス タイプ、IOS、および IOS XR バージョンにも対応できます。ただし、ネットワーク内にこのリストに準拠していない P または PE デバイスが含まれている場合、完全な診断ができない場合があります。表 11-1 に、可能性のあるシナリオとその結果を示します。

表 11-1　ハードウェア、IOS、および IOS XR のバージョン コンプライアンス

シナリオ	結果
すべての P および PE デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠している。	MPLS VPN 接続性検証テストは、アクセス回線、MPLS VPN、および MPLS コアの問題を正しくトラブルシューティングします。
すべての PE デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠している。1 台または複数の P デバイスが、サポートされているシスコ製ハードウェア、IOS、および IOS XR バージョンに準拠していない（他社製品など）。	MPLS VPN 接続性検証テストは、アクセス回線および MPLS VPN の問題を正しくトラブルシューティングしますが、MPLS コアの問題のトラブルシューティングは完了できない場合があります。

表 11-1　ハードウェア、IOS、および IOS XR のバージョン コンプライアンス （続き）

シナリオ	結果
PE デバイスが、サポートしていない IOS および IOS XR バージョンを実行しているシスコ製ハードウェアであり、MPLS LSP ping および traceroute 機能をサポートしていない。	MPLS VPN 接続性検証テストは、アクセス回線および MPLS VPN の問題を正常にトラブルシューティングできる*可能性はあります*。MPLS VPN 接続性検証テストは、MPLS コアのトラブルシューティングを実行できません。
PE デバイスがシスコ製以外のハードウェアである。	MPLS VPN 接続性検証テストは実行できません。

Diagnostics は、すべてのベンダーの管理対象および管理対象外の CE ルータをサポートしています。CE デバイスについては、デバイス タイプ、IOS、または IOS XR バージョンの要件はありません。

Diagnostics は、MPLS LSP ping および traceroute 機能をサポートしている他のデバイス タイプ、IOS および IOS XR バージョンで動作できます。この機能をサポートしているデバイス タイプ、IOS、および IOS XR のバージョンの詳細については、Cisco Feature Navigator を使用してください。http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp を参照してください。

（注）　PE デバイスが、サポートされていない IOS または IOS XR バージョン（MPLS ping および traceroute 機能を実装していないもの）を実行している場合は、アクセス回線および VPN エッジのトラブルシューティングは実行されますが、MPLS コアのトラブルシューティングはできません。このシナリオでは、コアの障害は PE デバイス上のラベル転送情報ベース（LFIB）不一致としてレポートされます。LFIB 不一致はコア障害の症状ですが、コアはトラブルシューティングできないため、実際のコア障害は診断できません。

IPv6

Internet Assigned Numbers Authority（IANA）が管理する IPv4 アドレス フリー プールが残り少なくなってきています。シスコは、この事態に対応するため、IPv6 アドレス指定を採用しています。

Diagnostics は、IPv4 と IPv6 の両方のアドレスを持つデバイスの、設定および選択をサポートしています。Diagnostics は、接続回線が次のような状態の MPLS VPN サービスをトラブルシューティングできます。

- IPv6 アドレス指定を使用する場合
- デュアルスタックの IPv4/IPv6 アドレス指定を使用する場合

デュアルスタックは、同じインターフェイス上に IPv4 と IPv6 の両方を共存させるための技術です。インターネット上には、永久ではないものの、今後長年にわたって IPv6 と IPv4 ノードが混在します。このため、IPv4 ノードを大規模に展開している企業では、IPv4 から IPv6 への移行を成功させることがとても重要です。たとえば、単一のインターフェイスを、IPv4 アドレスと IPv6 アドレスの両方を持つように設定できます。「デュアルスタック」と呼ばれるあらゆる要素（プロバイダー エッジやカスタマー エッジ ルータなど）は、IPv4 だけでなく、IPv6 アドレス指定およびルーティング プロトコルも実行します。

（注）　Diagnostics は、グローバル ユニキャスト IPv6 アドレスのみをサポートします。グローバル ユニキャスト アドレスの機能は、131.107.1.100 のような IPv4 ユニキャスト アドレスと類似しています。つまり、これらのアドレスは、従来型の、公的にルーティング可能なアドレスであると言えます。グローバル ユニキャスト アドレスには、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID が含まれます。

表 11-2　一般的なユニキャスト アドレス構造

フィールド	ネットワーク プレフィックス	サブネット	インターフェイス ID
Bits	48	16	64

（注）　Diagnostics では、接続回線エンドポイントが IPv6 と IPv6 の場合、IPv4 と IPv4 の場合のいずれにおいてもテストを起動できます。両方のアドレス指定を混在させることはできません。

IPv6 アドレスでテストを開始する場合の詳細については、「Diagnostics 接続テストの概要」（P.11-14）を参照してください。

診断機能

Diagnostics のトラブルシューティングおよび診断は、次の 4 つのドメインをサポートしています。

- アクセス回線：アクセス回線のトラブルシューティングには、ATM、フレーム リレー、およびイーサネットのルーティング プロトコルの基本的なトラブルシューティング、レイヤ 1 およびレイヤ 3 の基本的なトラブルシューティング、およびレイヤ 2 の高度なトラブルシューティングが含まれます。
- MPLS VPN：MPLS VPN のトラブルシューティングは、RFC2547 に基づいて MPLS/MP-BGP VPN をサポートしています。サポートされているトポロジは、ハブ アンド スポーク、セントラル サービス、フル メッシュ、およびイントラネットまたはエクストラネット VPN です。
- MPLS コア：MPLS コアのトラブルシューティングは、データ プレーンおよびコントロール プレーンのトラブルシューティングをサポートしています。この機能は、MPLS 運用管理および保守（OAM）がサポートされている Cisco IOS または Cisco IOS XR バージョンを実行するすべての MPLS コアおよびエッジ デバイス（検出されたすべての MPLS トラフィック エンジニアリング トンネルのトラブルシューティングを含む）用として用意されています。MPLS OAM がサポートされている Cisco IOS、および Cisco IOS XR のバージョンの詳細については、「サポートされているハードウェア、IOS、および IOS XR バージョン」（P.11-3）を参照してください。

（注）　Diagnostics では、コア内のルーティング プロトコル（ただし IGP プロトコルが OSPF の場合はファースト ホップおよび PE-P-PE トポロジでの OSPF 障害を除く）、コア内の IP 接続性、および相互自律システム（AS）または Carrier-Supporting-Carrier（CsC）の一部のバリエーション（特に LSP が存在しない相互 AS オプション B および CsC）はトラブルシューティングされません。

スタートアップ ガイド

この項では、シスコの Prime Provisioning 診断の使用を開始する方法について説明します。

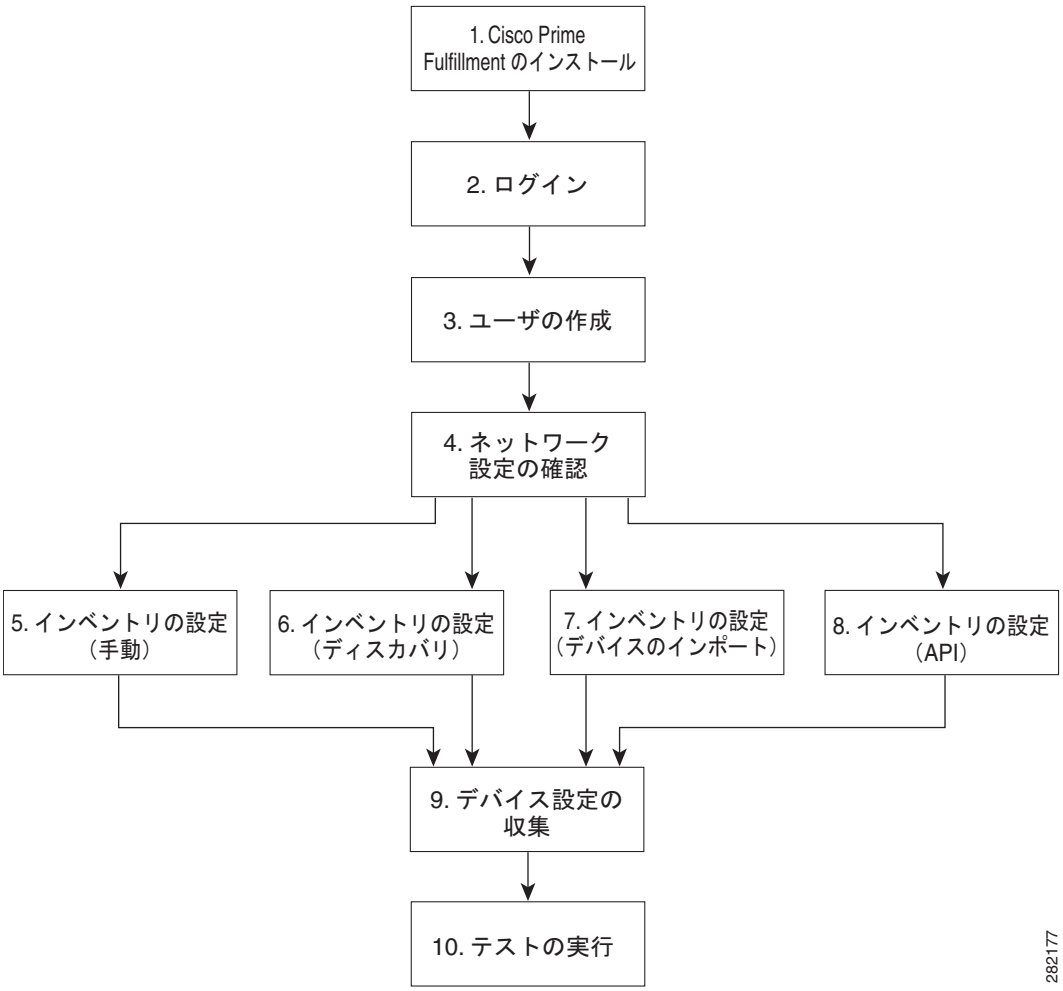
次の事項について説明します。

- 「ユーザ ロール」（P.11-7）

- 「ユーザ ロール」（P.11-7）
- 「ユーザの作成」（P.11-7）
- 「ネットワーク設定」（P.11-7）
- 「インベントリの設定」（P.11-9）

図 11-2 に、Diagnostics の使用を開始する際のワークフローを示します。

図 11-2　Diagnostics の概要



6. ユーザの作成：ユーザを作成し、Diagnostics ユーザ ロールを割り当てます。「ユーザ ロール」（P.11-7）、および「ユーザの作成」（P.11-7）を参照してください。
7. ネットワーク設定の確認：Diagnostics に必要な設定が、すべてのネットワーク デバイスで行われていることを確認します。「ネットワーク設定」（P.11-7）を参照してください。
8. インベントリの設定（手動）：必要な Prime Provisioning インベントリ オブジェクトを手動で作成します。「インベントリの設定」（P.11-9）を参照してください。
9. インベントリの設定（ディスカバリ）：Prime Provisioning ディスカバリを使用して、必要な Prime Provisioning インベントリ オブジェクトを作成します。「インベントリの設定」（P.11-9）を参照してください。

10. インベントリの設定（デバイス インポート）：インベントリ マネージャのデバイス インポート機能を使用して、必要な Prime Provisioning インベントリ オブジェクトを作成します。「インベントリの設定」（P.11-9）を参照してください。
11. インベントリの設定（API）：必要なインベントリ オブジェクトを Prime Provisioning API によって作成します。「インベントリの設定」（P.11-9）を参照してください。
12. デバイス設定の収集：インターフェイス設定を含むデバイス設定を収集し、Prime Provisioning インベントリに追加します。Prime Provisioning インベントリを実際のデバイス設定と定期的に同期するように、スケジュール タスクを設定できます。「デバイス設定の収集」（P.11-12）を参照してください。
13. テストの実行：MPLS VPN 接続性検証テストを設定して実行します。「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。

ユーザ ロール

Prime Provisioning ユーザが使用できる機能は、割り当てられているユーザ ロールによって決まります。ユーザ ロールによって、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うこともできます。

Diagnostics 機能を使用するには、実行する権利が与えられる接続性テストのタイプに応じて、次の定義済み Diagnostics ロールの 1 つ以上が割り当てられている必要があります。

1. MplsDiagnosticsRole：2 つの CE 間で MPLS VPN 接続性テストを実行できます。
2. MplsDiagnosticsPeToAttachedCeTestRole：PE と接続された CE との間で MPLS VPN 接続性テストを実行できます。
3. MplsDiagnosticsCetoPeAcrossCoreTestRole：MPLS コアをまたぐ CE および PE 間で MPLS VPN 接続性テストを実行できます。
4. MplsDiagnosticsPetoPeInVrfTestRole：2 つの PE 間で MPLS VPN 接続性テストを実行できます。
5. MplsDiagnosticsPeToPeCoreTestRole：2 つの PE 間でコア MPLS VPN 接続性テストを実行できます。

（注）　すべての Diagnostics ロールで、デバイスの作成と削除やデバイス設定の収集、MPLS VPN 接続性検証テストの実行を行うことができます。

ユーザの作成

Prime Provisioning ユーザの作成方法については、*『Cisco Prime Provisioning 6.3 Administration Guide』*を参照してください。

ネットワーク設定

この項では、ネットワークのトラブルシューティングを Diagnostics で行うために必要なネットワーク設定を説明します。

MPLS IP 存続可能時間伝搬

MPLS IP 存続可能時間（TTL）伝搬は、シスコ デバイスではデフォルトでイネーブルになっています。Diagnostics では、MPLS IP TTL 伝搬が MPLS コア内でイネーブルになっている必要があります。MPLS IP TTL 伝搬がイネーブルになっていない場合、Diagnostics は MPLS コア内で問題のトラブルシューティングを実行できません。その状態でも、アクセス回線の問題、または MPLS コアのエッジにおける問題のトラブルシューティングは可能です。

Cisco IOS では、IOS コマンドの **no mpls ttl-propagate forward** を使用すると、MPLS コアに転送されるパケットの MPLS IP TTL 伝搬をディセーブルにできます。このコマンドでは、MPLS コアに転送されるパケットの TTL 伝搬が停止されますが、MPLS コア内部から送信されるパケットの TTL 伝搬は許可されます。Diagnostics は、この状況で正しく機能します。

Cisco IOS コマンドの **no mpls ip propagate-ttl** を使用して、または Cisco IOS XR コマンドの **mpls ip-ttl-propagate disable** を使用して TTL 伝搬をディセーブルにしている場合は、すべての TTL 伝搬がディセーブルになるため、Diagnostics は MPLS ネットワークをトラブルシューティングできません。

（注）　トラブルシューティング対象に選択したデバイスと、同じネットワークの一部であるデバイスに対して、タイムスタンプをディセーブルにする必要があります。

MPLS LSP ping/traceroute のリビジョン

Diagnostics は、バージョン 3 の IETF LSP ping ドラフト（draft-ietf-mpls-lsp-ping-03.txt）に基づいて、IOS MPLS LSP ping/traceroute 実装をサポートします。それよりも後のバージョンの IETF LSP ping ドラフトはサポートされません。最新の IOS バージョン（12.4(6)T を含む）および IOS XR は、以降のバージョンの IETF LSP ping ドラフト /RFC 4379 を実装しています。これらの IOS または IOS XR バージョンで Diagnostics を使用するには、バージョン 3 の IETF LSP ping ドラフトを使用するように IOS または IOS XR を設定する必要があります。そのためには、IOS または IOS XR グローバル コンフィギュレーション モードで **mpls oam** コマンドに続けて **echo revision 3** コマンドを入力する必要があります。必要に応じて、コアのすべてのルータが同じバージョンの IEFT LSP ping ドラフトまたは RFC を使用していることを確認します。

ポイントツーポイント アクセス回線リンクでの 31 ビット プレフィックス

IPv4 アドレッシングを使用するアクセス回線リンクに対して、Diagnostics は、31 ビット プレフィックスで設定されたアクセス回線リンクによるトラブルシューティングをサポートします。ただし、各クラスフル ネットワークに対して、Diagnostics は可能性のある 2 つの 31 ビット プレフィックス設定によるトラブルシューティングをサポートしません。その 2 つとは、クラスフル ネットワーク アドレスまたはネットワーク ブロードキャスト アドレスをホスト アドレスとして使用するサブネットです。たとえば、クラス A ネットワーク 10.0.0.0 において、IP アドレス 10.0.0.0 と 10.0.0.1 をホスト アドレスとして使用する 31 ビット プレフィックス サブネット、および IP アドレス 10.255.255.254 と 10.255.255.255 をホスト アドレスとして使用するサブネットはサポートされません。これらの範囲の間にあるすべてのサブネットはサポートされます。

サポートされていない 31 ビット プレフィックス サブネットを使用して Diagnostics テストが設定された場合は、テストは実行されず、サポートされていない 31 ビット プレフィックス設定であることを通知するメッセージが表示されます。このような状況では、このリンクを手動でトラブルシューティングするか、リンクを再設定してサポートされるサブネット設定を使用する必要があります。

インベントリの設定

Diagnostics は、他の Prime Provisioning モジュールにまったく依存することなく使用できます。ただし、使用する前に、Prime Provisioning リポジトリに多数のオブジェクトを入力する必要があります。最低でも、これにはプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトが含まれます。これらの各オブジェクトのロールについて、以下で説明します。

- 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、特定のプロバイダーを表した論理インベントリ オブジェクトです。
- プロバイダー リージョン：プロバイダー リージョンは、1 つのボーダー ゲートウェイ プロトコル（BGP）自律システム内のプロバイダー エッジ ルータ（PE）のグループであると見なされます。プロバイダー リージョンを定義する主な目的は、プロバイダーがヨーロッパ、アジア太平洋などの広い地域で一意の IP アドレス プールを使用できるようにすることです。
- 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。Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義する必要があります。
- PE デバイス：PE デバイスは、特定のプロバイダー リージョンに関連付けられたプロバイダー エッジ（PE）またはプロバイダー（P）ルータを論理的に表したものです。PE デバイスは最初にデバイスとして追加してから、そこに PE デバイス タイプを割り当てる必要があります。

MPLS ネットワークのすべてのプロバイダー エッジ（PE）およびプロバイダー（P）ルータを Prime Provisioning インベントリに追加する必要があります。各プロバイダー エッジ ルータはデバイスとして作成してから、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとする必要があります。各プロバイダー デバイスはデバイスとして作成してから、ロール タイプ P（プロバイダー）を割り当てた PE デバイスとする必要があります。Prime Provisioning インベントリへの顧客宅内装置（CPE）デバイスの追加はオプションです。

（注） デバイスがプロバイダー デバイスおよびプロバイダー エッジ デバイスの両方として動作する場合は、そのデバイスを、ロール タイプ N-PE（ネットワーク方向の PE）を割り当てた PE デバイスとして作成する必要があります。

多くの MPLS VPN ネットワークがルータ リフレクタを使用します。ルータ リフレクタを Prime Provisioning インベントリに追加することを推奨します。ルータ リフレクタはデバイスとして追加してから、ロール タイプが P の PE デバイスとして追加する必要があります。ルータ リフレクタを Prime Provisioning インベントリに追加することにより、Diagnostics は、このデバイスを含む潜在的な障害を識別できます。

（注） その他の Prime Provisioning の機能を使用して MPLS ネットワークを管理している場合は、必要なインベントリ オブジェクトの多くがすでに存在している可能性があります。たとえば、Prime Provisioning MPLS VPN 機能を使用している場合に、必要なプロバイダー、プロバイダー リージョン、およびプロバイダー エッジ デバイスはすでに存在することがあります。その場合は、プロバイダー デバイスのみを追加する必要があります。

必要なインベントリ オブジェクトを作成するための、多数のオプションがあります。これらのオブジェクトは Prime Provisioning GUI により手動で作成することも、Prime Provisioning Discovery 機能、インベントリ マネージャのデバイス インポート機能、あるいは Prime Provisioning API を利用するサードパーティの Operations Support System（OSS）クライアント プログラムを使用して作成することもできます。これらのオプションについては、それぞれ次の項を参照してください。

- 「手動作成」（P.11-10）

- 「Discovery」（P.11-10）
- 「インベントリ マネージャ デバイスのインポート」（P.11-11）
- 「Prime Provisioning API」（P.11-12）
- 「Prime Provisioning API」（P.11-12）

（注）　デバイスの作成時に、デバイス アクセス情報（ログインおよびパスワード）が、物理デバイスに設定されている情報と一致している必要があります。

手動作成

手動作成では、必要な設定を Prime Provisioning グラフィカル ユーザ インターフェイス（GUI）により入力することで、オブジェクトを Prime Provisioning リポジトリに追加できます。オブジェクトの手動作成は、Prime Provisioning リポジトリに追加するオブジェクト数が少ない場合に推奨されます。オブジェクトの手動作成の手順を次に示します。

1. プロバイダーを作成します。
2. プロバイダー リージョンを作成します。
3. デバイスを作成します。
4. インターフェイス設定などのデバイス設定を収集します
5. PE デバイスを作成し、プロバイダー デバイスおよびプロバイダー エッジ デバイスのロールを割り当てます。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。Prime Provisioning サーバおよびデバイス間で使用するトランスポート メカニズムを選択する場合、Cisco CNS Configuration Engine は Diagnostics に必要なコマンドをサポートしないため、MDE と組み合わせて使用できません。Cisco CNS Configuration Engine を Diagnostics と使用しようとすると、Diagnostics はデバイスに接続できないと間違って報告します。

プロバイダー、プロバイダー リージョン、デバイス、および PE デバイス オブジェクトを手動で作成する方法については、「リソースの設定」（P.2-42）を参照してください。

デバイスを手動作成する場合は、対象のデバイスのインターフェイス設定も追加する必要があります。

インターフェイス設定は、デバイス作成時に手動で追加することも、タスク マネージャの Collect Configuration タスクを使用して追加することもできます。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。Collect Configuration タスクを使用することを推奨します。

Discovery

Discovery では、XML ファイルに最低限のデバイスおよびトポロジ情報を設定することにより、ネットワークのデバイスを Prime Provisioning リポジトリに追加できます。次に、Discovery プロセスはこれらのデバイスを照会し、必要なデバイスおよびトポロジ情報を Prime Provisioning リポジトリに入力します。リポジトリに追加するオブジェクト数が多い場合は、Discovery の使用を推奨します。

Prime Provisioning Discovery には、デバイスを検出するための方法として CDP とデバイス / トポロジの 2 つが用意されています。デバイス検出を実行する前に、Discovery に必要な XML コンフィギュレーション ファイルを作成することが必要です。デバイスを検出する方法の詳細については、付録 E「インベントリ - ディスカバリ」を参照してください。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。

（注）　Discovery の完了後に、検出されたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、Diagnostics は検出されたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

インベントリ マネージャ デバイスのインポート

インベントリ マネージャのデバイス インポート機能を使用すると、デバイスの Cisco IOS 実行コンフィギュレーションを含むファイルから Prime Provisioning リポジトリに複数のデバイスをインポートできます。リポジトリに追加するオブジェクト数が多い場合は、インベントリ マネージャのデバイス インポート機能の使用を推奨します。デバイスをインポートする方法の詳細については、付録 E「インベントリ - ディスカバリ」を参照してください。

プロバイダー（P）およびプロバイダー エッジ（PE）デバイスをインポートする前に、必要なプロバイダーおよびプロバイダー リージョン オブジェクトを作成する必要があります。プロバイダーおよびプロバイダー リージョンオブジェクトを手動で作成する方法については、付録 E「インベントリ - ディスカバリ」を参照してください。

デバイスをインポートするときは、Cisco IOS 実行コンフィギュレーションを含むファイルがあるディレクトリを指定する必要があります。ファイル名は指定しないでください。ファイルは、Prime Provisioning サーバからアクセスできるファイル システムのディレクトリに存在する必要があります。

（注）　Provider（P; プロバイダー）デバイスおよびプロバイダー エッジ（PE）デバイスは、いずれも適切な PE ロール タイプが割り当てられた PE デバイス オブジェクトとして Prime Provisioning リポジトリに追加する必要があります。プロバイダー デバイスおよびプロバイダー エッジ デバイスに割り当てる必要のある PE ロール タイプの詳細については、「インベントリの設定」（P.11-9）を参照してください。

（注）　イネーブル シークレット パスワードは、Cisco IOS 実行コンフィギュレーションに追加される前に暗号化されます。その結果、デバイス インポート機能は、Prime Provisioning リポジトリにインポートするデバイスに対してイネーブル シークレット パスワードを設定できません。インポートするデバイスにイネーブル シークレット パスワードが設定されている場合は、Prime Provisioning リポジトリでこれらのデバイスに手動でイネーブル パスワードを設定する必要があります。イネーブル シークレット パスワードとイネーブル パスワードの両方がデバイスに設定されている場合、インベントリ マネージャのデバイス インポート機能は Prime Provisioning リポジトリに追加するデバイスにイネーブル パ

スワードを使用します。このパスワードは正しいイネーブル シークレット パスワードで上書きする必要があります。Prime Provisioning リポジトリのデバイスのイネーブル パスワードは、デバイスのインポート中にも、デバイスのインポート後にも設定できます。

（注）　デバイス インポートの完了後に、インポートされたすべてのデバイスに対してタスク マネージャの Collect Configuration タスクを実行する必要があります。Collect Configuration タスクを実行しないと、Diagnostics はインポートされたデバイスにログインして、トラブルシューティングを実行できません。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

Prime Provisioning API

Prime Provisioning アプリケーション プログラム インターフェイス（API）は、Prime Provisioning システムに接続するために Operations Support System（OSS）クライアント プログラムを使用することができます。Prime Provisioning API は、Prime Provisioning サーバからデータの挿入、取得、更新、および削除を行うためのメカニズムを提供します。API を使用して、必要なプロバイダー、プロバイダー リージョン、デバイスおよび PE デバイス オブジェクトを追加できます。

（注）　Prime Provisioning API は Diagnostics に標準には含まれておらず、別途購入できます。

Prime Provisioning API の使用方法の詳細については、*『Cisco Prime Provisioning 6.3 API Programmer Guide』*および *『Cisco Prime Provisioning API 6.3 Programmer Reference』*を参照してください。

デバイス設定の収集

タスク マネージャの Collect Configuration タスクを使用して、Prime Provisioning リポジトリのデバイスにインターフェイス設定を追加することを推奨します。タスク マネージャの Collect Configuration タスクはネットワークの物理デバイスに接続し、ルータからデバイス情報（インターフェイス設定を含む）を収集して、その情報を Prime Provisioning リポジトリに入力します。

タスク マネージャの Collect Configuration タスクを使用してデバイス インターフェイスの設定を追加する方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

デバイス設定と Prime Provisioning リポジトリの同期

（注）　診断の精度は最新のデバイス情報に依存します。デバイス設定に何らかの変更を加えた後および定期的に、デバイス設定を物理デバイスと再同期することを推奨します。これにより、Prime Provisioning インベントリに保持されているデバイス設定がネットワークの物理デバイスと一致します。

タスク マネージャのスケジュール タスクを使用して、デバイス設定を最新に保つことを推奨します。Collect Configuration と Collect Configuration from File のどちらでも使用できます。タスク マネージャの Collect Configuration スケジュール タスクの作成方法の詳細については、「タスク マネージャ」（P.10-25）を参照してください。MPLS ネットワークの PE および P ルータは、すべてがタスク マネージャのスケジュール タスク Collect Configuration を使用してその設定を収集する必要があります。タスク マネージャの Collect Configuration タスクでは、インターフェイス設定およびその他のデバイス

属性の詳細が収集されます。タスク マネージャの Collect Configuration タスクの実行スケジュール間隔は、ネットワークに対する設定変更の頻度に依存します。タスク マネージャの Collect Configuration タスクを各 P および PE ルータで毎日実行することを推奨します。

Cisco MPLS Diagnostics Expert の使用

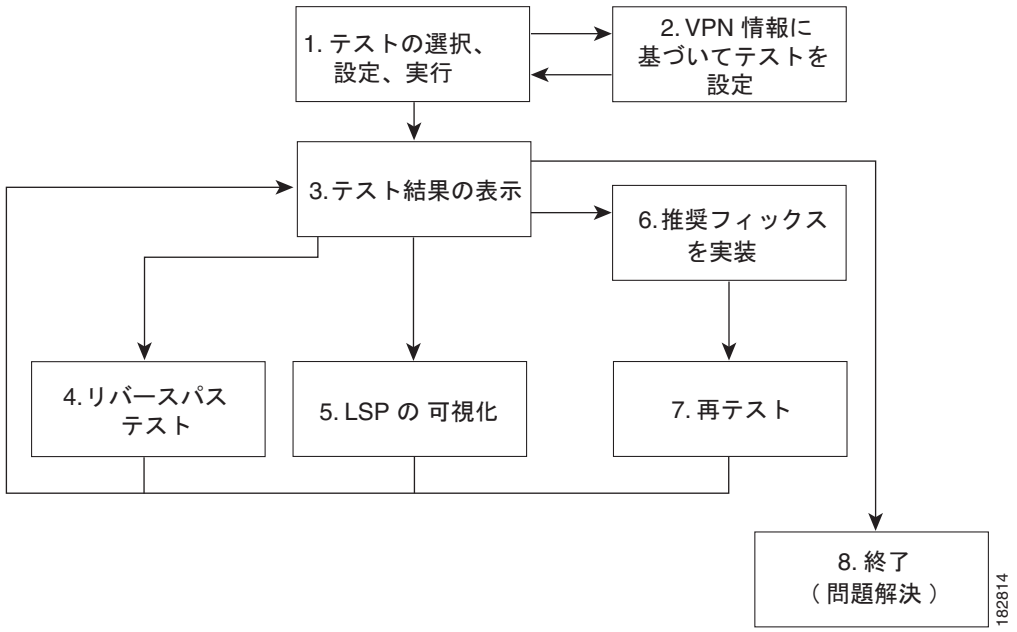
この項では、Diagnostics を使用する方法について説明します。

次の事項について説明します。

- 「Diagnostics 接続テストの概要」（P.11-14）
- 「MPLS VPN 接続性検証テストの実行」（P.11-18）
- 「[Progress] ウィンドウ」（P.11-39）
- 「テスト結果の解釈」（P.11-39）
- 「高度なトラブルシューティング オプション」（P.11-46）
- 「トンネル チェックのオフ：他社製 P ルータを使用したネットワークの場合」（P.11-48）

図 11-3 に、Diagnostics を使用する場合のワークフローを示します。

図 11-3　Diagnostics 使用ワークフロー



1. テストの選択、設定、および実行：MPLS VPN 接続性検証テストを設定して実行します。「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。
2. VPN 情報によるテストの設定：オプションで、VPN 情報を使用して MPLS VPN 接続性検証テストを設定します。これは、Prime Provisioning VPN プロビジョニング機能を使用してネットワーク内に VPN をプロビジョニングした場合にのみ可能です。「カスタマー VRF 情報を使用した設定」（P.11-29）および「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照してください。
3. テスト結果の表示：MPLS VPN 接続性検証テストの結果を、テスト ログを含めて表示します。「テスト結果の解釈」（P.11-39）を参照してください。
4. リバース パス テスト：高度なトラブルシューティングであるリバース パス テストを実行します。「リバース パス テスト」（P.11-46）を参照してください。
5. LSP 可視化：高度なトラブルシューティングである LSP 可視化を実行します。「LSP 可視化」（P.11-46）を参照してください。
6. 推奨フィックスの実装：テスト結果の推奨に従ってフィックスを実装します。
7. 再テスト：MPLS VPN 接続性検証テストを再実行します。通常、実装したフィックスを確認するために実行します。

Diagnostics 接続テストの概要

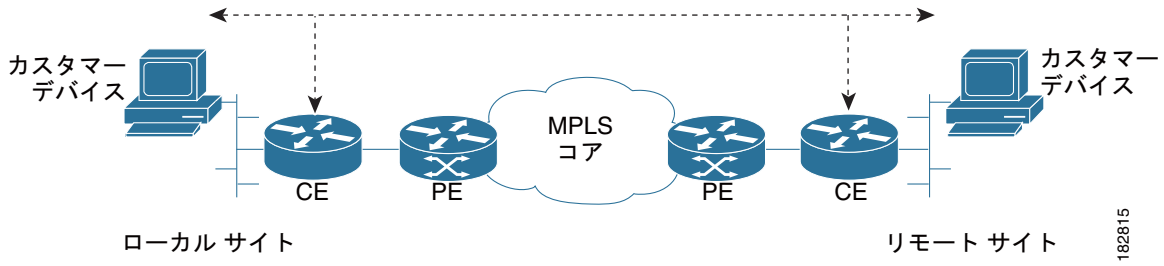
接続性テストは、CE - CE 間ネットワーク全体のサブセクションのトラブルシューティングを目的としています。次の接続性テストが用意されています。

1. L3VPN - CE to CE：2 つの CE 間の MPLS VPN 接続性をチェックします。「L3VPN - CE to CE 接続性テスト」（P.11-14）を参照してください。
2. L3VPN - PE to attached CE：PE と、接続されている CE の間の MPLS VPN 接続性をチェックします。「L3VPN - PE to attached CE 接続性テスト」（P.11-15）を参照してください。
3. L3VPN - CE to PE across Core：MPLS コアをまたがる CE と PE 間の MPLS VPN 接続性をチェックします。「L3VPN - CE to PE across Core 接続性テスト」（P.11-16）を参照してください。
4. L3VPN - PE to PE in VRF：2 つの PE 間の MPLS VPN 接続性をチェックします。「L3VPN - PE to PE in VRF 接続性テスト」（P.11-17）を参照してください。
5. MPLS - PE to PE：2 つの PE 間の MPLS コア接続性をチェックします。「L3VPN - PE to PE 接続テスト」（P.11-17）を参照してください。

L3VPN - CE to CE 接続性テスト

L3VPN - CE to CE テスト（図 11-4）は、2 つの CE 間またはカスタマー デバイス IP アドレスが既知のカスタマー デバイス間の MPLS VPN 接続性をチェックします。

図 11-4　L3VPN - CE to CE 接続性テスト



この場合、Diagnostics はコア、エッジ、および接続回線のトラブルシューティングを実行します。

IPv6 トラブルシューティング

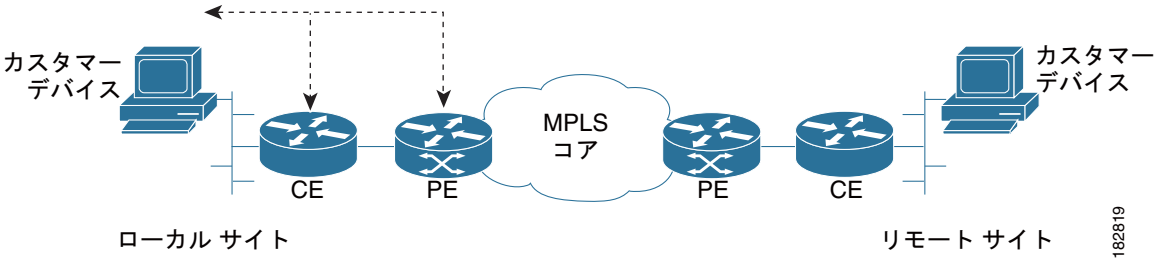
L3VPN - CE to CE テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したローカルおよびリモート PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- ローカルサイトおよびリモートサイトに指定した CE アクセス回線インターフェイス IP アドレスの両方がグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、ローカル サイトおよびリモート サイトの両方またはいずれか一方に指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。

L3VPN - PE to attached CE 接続性テスト

L3VPN - PE to attached CE 接続テスト（図 11-5）は、PE とローカルに接続された CE 間の VPN 接続性テストを実行します。この場合、Diagnostics はエッジおよび接続回線のトラブルシューティングを実行します。

図 11-5　L3VPN - PE to attached CE 接続性テスト



L3VPN - PE to attached CE 接続性テストは、逆の方向には実行できません。

接続の問題は、多くの場合ローカルの接続回線に原因があります。利用できない可能のあるリモートサイトの PE および CE の詳細を必要とせずに、ローカルの接続回線を単独でテストできます。

L3VPN - PE to attached CE 接続性テストによって、VRF 対応 IP SLA プローブで報告されるものと同じ接続回線の接続断を診断できます。この通知には、Diagnostics で対応するアクセス回線の接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

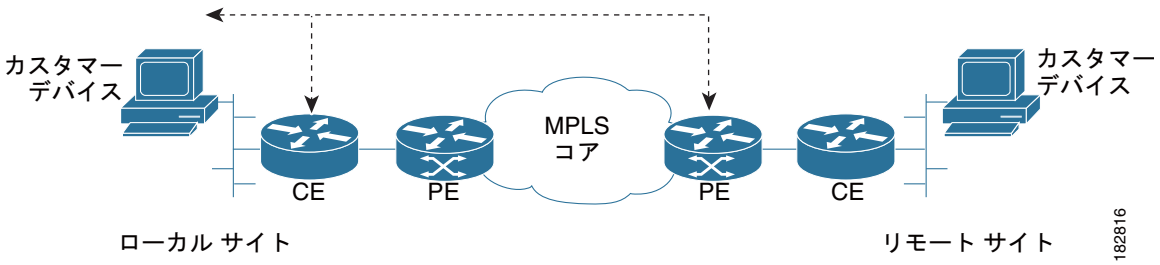
L3VPN - PE to attached CE テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定した PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- 指定した CE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。

L3VPN - CE to PE across Core 接続性テスト

L3VPN - CE to PE across Core 接続性テスト（図 11-6）は、MPLS コアをまたいだ、CE またはカスタマーデバイス（カスタマー デバイス IP アドレスが既知のもの）と PE 間の MPLS VPN 接続性をチェックします。

図 11-6　L3VPN - CE to PE across Core 接続性テスト



この場合、Diagnostics はコア、両方のエッジ、および接続回線のトラブルシューティングを実行します。

IPv6 トラブルシューティング

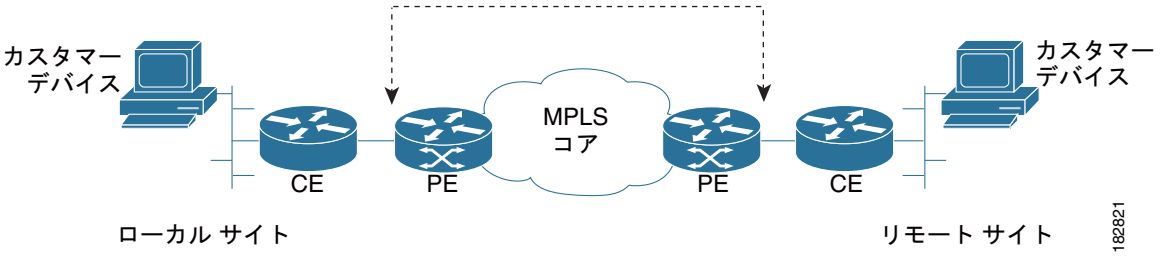
L3VPN - CE to PE across Core テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定した PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスを持っている、またはデータベースでインターフェイスの詳細情報を使用できない場合。
- 指定した CE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- オプションで、指定したカスタマー デバイス IP アドレスがグローバル ユニキャスト IPv6 アドレスの場合。
- 選択または指定された PE アクセス回線インターフェイスにグローバル ユニキャスト IPv6 アドレスがあるか、インターフェイス詳細がデータベースにない場合。

L3VPN - PE to PE in VRF 接続性テスト

VRF 接続性テストの L3VPN - PE to PE（図 11-7）は、2 つの PE 間の MPLS 接続性をチェックします。Diagnostics はコアおよび両側のエッジのトラブルシューティングを実行します。

図 11-7　　L3VPN - PE to PE in VRF 接続性テスト



組織によっては、コアまたはエッジ ネットワークをプロビジョニングしても、すぐには CE を割り当てないことがあります。L3VPN - PE to PE in VRF 接続性テストを使用すると、段階的にネットワークを展開してテストできます。また、このテスト オプションでは高い柔軟性も提供され、CE 情報の準備ができていないときにエッジまたはコア ネットワーク セグメントをテストできます。

さらに、L3VPN - PE to PE in VRF 接続性テストによって、VRF 対応 IP SLA プローブで報告されるものと同じ短距離（PE からリモート PE）VPN 接続断も診断できます。この通知には、Diagnostics で対応するエッジの接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

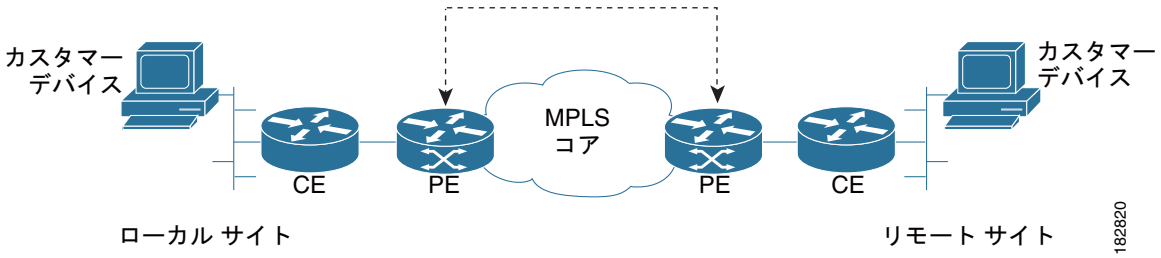
L3VPN - PE to PE in VRF テストでは、次のすべての条件が満たされている場合に、IPv6 セグメントのトラブルシューティングを起動します。

- グローバル ユニキャスト IPv6 アドレスを持つローカル サイト PE アクセス回線インターフェイスまたはリモート サイト PE アクセス回線インターフェイスのいずれかを、インターフェイス選択画面で選択する必要がある場合。
- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したローカル PE アクセス回線インターフェイスがグローバル ユニキャスト IPv6 アドレスしか持っていない場合。
- インターフェイス選択画面でグローバル ユニキャスト IPv6 アドレスが入力された行を選択した、または指定したリモート PE アクセス回線インターフェイス IP アドレスがグローバル ユニキャスト IPv6 アドレスしか持っていない場合。

L3VPN - PE to PE 接続テスト

L3VPN - PE to PE コア接続性テスト（図 11-8）は、2 つの PE 間の MPLS 接続性をチェックします。

図 11-8　　L3VPN - PE to PE コア接続性テスト



L3VPN - PE to PE コア テストは、CE インターフェイスへのアクセスがブロックされている場合（たとえばアクセス リストの使用によるもの）または組織内の異なるグループが、それぞれ別のネットワーク セグメントについて責任を負っている場合を対象にしています。たとえば、Core グループの P に問題があるが、完全な CE-CE または PE-PE テストを実行するためのエンド カスタマーのコンテキストがない場合が該当します。

L3VPN - PE to PE コア テストによって、MPLS 対応 PE 間の接続性をテストする IP SLA ヘルス モニタ プローブで報告されるものと同じコア接続断を診断できます。この通知には、Diagnostics で対応するコアの接続性テストを設定するために必要な、すべての情報が含まれています。

IPv6 トラブルシューティング

コア内の L3VPN - PE to PE テストの場合、このテスト タイプは IPv4 アドレスのみを使用するため、IPv6 トラブルシューティングは開始できません。

MPLS VPN 接続性検証テストの実行

この項では、MPLS VPN 接続性検証テストの実行方法について説明します。ここでは、次の項目について説明します。

- 「[MPLS Diagnostics Expert Feature Selection] ウィンドウを開く」（P.11-18）
- 「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）
- 「L3VPN - PE to attached CE テストの選択、設定および実行」（P.11-32）
- 「L3VPN - CE to PE across Core テストの選択、設定、および実行」（P.11-33）
- 「L3VPN - PE to PE テストの選択、設定および実行」（P.11-34）
- 「MPLS - PE to PE テストの選択、設定および実行」（P.11-35）

（注）　IOS XR バージョン 3.8.0 以降のデバイスで実行される各コマンドでは、出力の最初の行に、Diagnostics が処理できなかったデバイスの現在のタイムスタンプが表示されます。XR デバイスのタイムスタンプを無効にするには、テストを起動する前に、*timestamp disable* コマンドを使用する必要があります。

[MPLS Diagnostics Expert Feature Selection] ウィンドウを開く

（注）　同じクライアント マシンで並行して複数の MPLS VPN 接続性検証テストを実行する場合は、各テストを異なる HTTP セッションで実行する必要があります。そのためには、コマンドライン、またはデスクトップのブラウザのアイコン、または [Start] メニューから起動した個別のブラウザで各テストを実行します。同じブラウザ ウィンドウの別のタブ、または既存のブラウザ ウィンドウから起動したブラウザ ウィンドウで、複数のテストを並行して実行しないでください。

ステップ 1　Prime Provisioning にログインします。ログイン方法の詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください（「**Installing and Logging Into Prime Provisioning**」>「**Logging In for the First Time**」）。

Prime Provisioning のホーム ウィンドウが表示されます。

ステップ 2　[Diagnostics] タブをクリックします。

[MPLS Diagnostics Expert Feature Selection] ウィンドウが表示され、使用できる MPLS VPN 接続性検証テスト タイプが示されます。

（注）　また、少なくとも 1 つの Diagnostics ユーザ ロールが割り当てられていることを確認する必要があります。「ユーザ ロール」（P.11-7）を参照してください。

（注）　使用できるテスト タイプは、割り当てられているユーザ ロールによって決まります。ユーザ ロールは、テスト タイプごとに定義する必要があります。テスト タイプにアクセスできない場合、そのテスト タイプは [MPLS Diagnostics Expert Feature Selection] ウィンドウに表示されません。詳細については、「ユーザ ロール」（P.11-7）を参照してください。

L3VPN - CE to CE テストの選択、設定および実行

この項では、L3VPN - CE to CE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

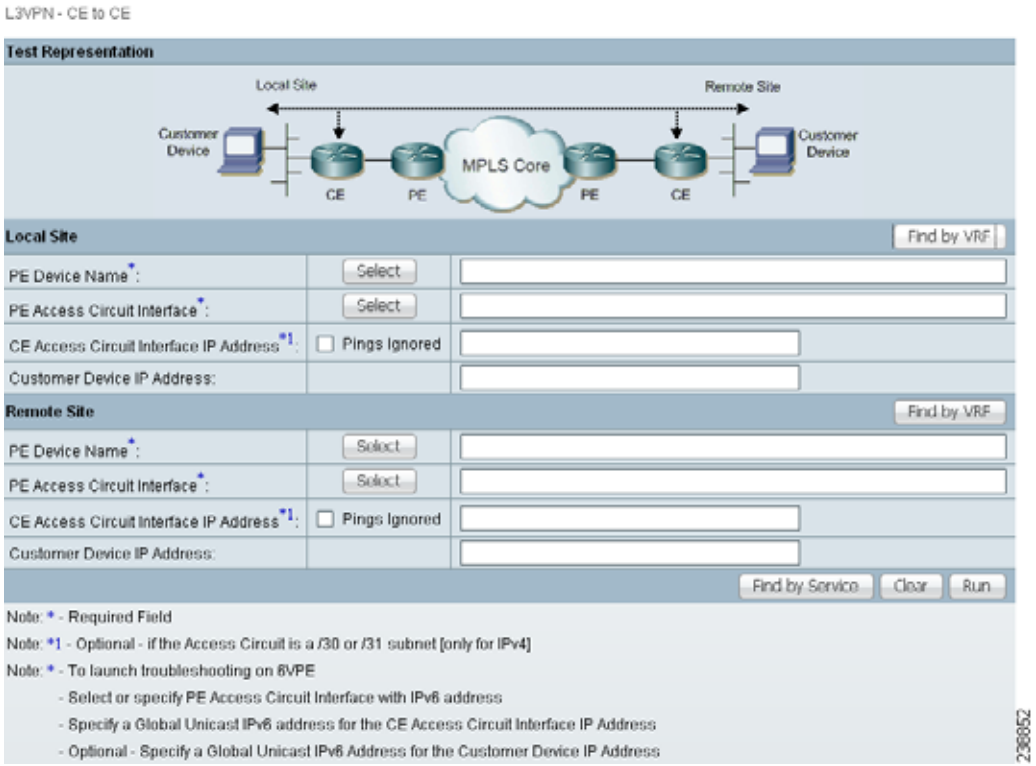
ステップ 1　[Diagnostics] メニューから、[L3VPN - CE to CE] テスト タイプを選択します。

ステップ 2　[L3VPN - CE to CE] 接続性検証テスト タイプをクリックします。

L3VPN - CE to CE 接続性検証テスト タイプの詳細については、「L3VPN - CE to CE 接続性テスト」（P.11-14）を参照してください。[L3VPN - CE to CE] ウィンドウが表示され、L3VPN - CE to CE テスト タイプに対応する入力ウィンドウが表示されます。

ヒント　使用できるテスト タイプごとに独自の入力ウィンドウがあり、異なるパラメータのセットを必要とします。たとえば、L3VPN - CE to CE テストにはローカル サイトとリモート サイトの両方の情報が必要で、L3VPN - PE to attached CE テストのテスト設定ウィンドウではローカル サイトの詳細だけが要求されます。

図 11-9　L3VPN - CE to CE テスト タイプ



[L3VPN - CE to CE] ウィンドウを使用して、実行する接続性テストを設定できます。

このウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

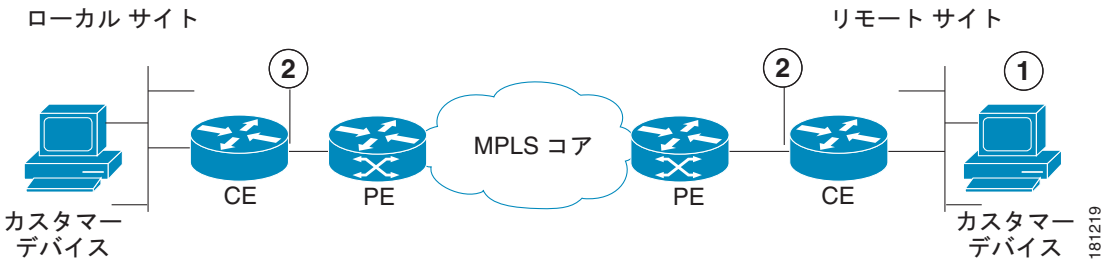
ネットワーク図は、テストを設定するために入力する必要がある情報のコンテキストを提供する静的なイメージです。

MPLS VPN 接続性検証は、VPN 内にある 2 つのサイト間の接続性をテストします。テストを通じて、これらのサイトはローカル サイトおよびリモート サイトと呼ばれます。接続性の問題は、特定のサイトの視点から報告または検出されることが予想されます。通常は、この特定のサイトをローカル サイトとして使用し、このサイトからテストを実行します。ただし、これは必須ではありません。接続性は両方向でテストできるため、どちらのサイトもローカル サイトまたはリモート サイトとして使用できます。

L3 VPN 接続性テストの範囲（図 11-10 を参照）は、サイトごとに変更できます。サイトごとに、そのサイト内にあるカスタマー デバイスへの接続性（図 11-10 の *1*）、または CE アクセス回線インターフェイスへの接続性（図 11-10 の *2*）をテストできます。テスト範囲は、指定した設定によって決まります。

カスタマー デバイスの IP アドレスが既知の場合は、そのデバイスへの接続性検証テストを実行することを推奨します。カスタマー デバイスの IP アドレスが未知の場合は、サイトの CE までの接続性検証テストを実行できます。

図 11-10　テスト範囲



1. カスタマー デバイス。
2. CE アクセス回線インターフェイス。

カスタマー サイトのサブネットワーク内にあるデバイスへの接続性をテストするには、[Customer Device IP Address] フィールドにデバイスの IP アドレスを入力します。デフォルトでは、サイトの必須フィールドだけを指定した場合、CE アクセス回線インターフェイスへのテストが実行されます。

（注）　必須フィールドは、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウに、青いアスタリスクで示されています。すべての必須フィールドに有効な情報が入力されるまでは、次に進めません。

（注）　/30 または /31 アドレッシングが使用されている場合は、[CE Access Circuit Interface IP Address] フィールドは Diagnostics により自動的に入力されます。

Cisco IOS および Cisco IOS XR アクセス コントロール リスト（ACL）により、さまざまな基準に基づいて選択したトラフィックがブロックされるようにできます。カスタマー デバイスまたは CE インターフェイスへの MPLS VPN 接続性検証テストを実行したときに、CE 上で設定されている ACL が原因で、矛盾した結果が報告される場合があります。可能な場合、MPLS VPN 接続性検証テストは、CE デバイス上で設定されている ACL によってトラフィックがブロックされたことを報告します。ただし ACL の設定によっては、CE デバイス上で設定されている ACL によってトラフィックがブロックされたことを識別できない場合があります。場合によっては、MPLS VPN 接続性検証テストでアクセス回線の障害または不明な障害が報告されることがあります。トラフィックが CE でブロックされている疑いがある場合は、そのサイトの [Pings Ignored] チェックボックスをオンにしてください。このようにすると、Diagnostics はトラブルシューティング時にブロッキング アクセス ACL を考慮し、見つかった問題についてより正確な診断が返されます。

（注）　サイトの [Pings Ignored] チェックボックスをオンにした場合は、CE IP アドレスとオプションで [Customer Device IP Address] フィールドを使用して、PE デバイスでトラブルシューティングおよび設定チェックが実行されます。

ステップ 3　必要に応じて [L3VPN - CE to CE] ウィンドウのフィールドを設定します。

表 11-3 には、[L3VPN - CE to CE] ウィンドウのフィールド説明が表示されています。

（注）　表示されるフィールドは、選択したテスト タイプによって異なります。たとえば、CE to CE テストにはローカル サイトとリモート サイトの両方の情報が必要で、PE to attached CE テストのテスト設定ウィンドウではローカル サイトの詳細だけが要求されます。

（注）　テストを設定する別の方法として、カスタマー VPN 情報を使用する方法があります。詳細については、「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照してください。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明

フィールド	有効なテストタイプ	説明
Find by VRF	All	[Find by VRF] ボタンをクリックして、VRF 検索を使用して特定される PE ホスト名または PE インターフェイスの詳細を使用するテストを設定します。（「カスタマー VRF 情報を使用した設定」（P.11-29）を参照）。
PE Device Name	All	[PE Device Name] フィールドにサイトの PE デバイス名を入力するか、[Select] ボタンをクリックしてサイトの PE デバイス名を選択します。 （注）　[Select] ボタンをクリックすると、[Select PE Device] ウィンドウが開きます。（「PE デバイスの選択」（P.11-25）を参照してください）。 デバイス名は、デバイスの完全修飾ホスト名およびドメイン名です。たとえば、router1.cisco.com とします。ただし、ドメイン名はオプションであるため、多くの場合デバイス名はデバイスのホスト名です。たとえば、router1 とします。 指定するデバイス名は、ロール タイプが N-PE の PE デバイスのデバイス名と一致する必要があります。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明 （続き）

フィールド	有効なテスト タイプ	説明
LSP Endpoint Loopback IP Address	L3VPN - PE to PE コアのみ	BGP ネクスト ホップがピア PE の BGP ルータ ID と異なる場合は、BGP ネクスト ホップを入力します。ループバック IP アドレスを入力するか、IP アドレスに解決されるループバック名を入力できます。 コアをテストするときは、ローカル PE からリモート PE に MPLS OAM ping およびトレースが実行されます。この ping の宛先によって、ローカル PE のルーティング情報に基づいて LSP が選択されます。 カスタマー トラフィックは、カスタマー ルートの BGP ネクスト ホップ アドレスを宛先として使用し、LSP を選択します。Diagnostics がテストする IP プレフィックスがカスタマー トラフィックで使用される BGP ネクスト ホップ アドレスと一致していることを確認してください。これによって、Diagnostics はカスタマー トラフィックが経由する LSP と同じ LSP をテストするようになります。 L3VPN - PE to PE コア テストの場合、Diagnostics はカスタマー ルート情報を持っていません。そのため、Diagnostics は BGP ネクスト ホップを識別できず、ping の宛先の選択はネクスト ホップではなくリモート PE の BGP ルータ ID に基づきます。 ネットワーク設定によっては、このルータ ID がカスタマー トラフィックで使用されるネクスト ホップと一致せず、不正な LSP がテストされる（または、どの LSP もテストされない）ことがあります。 これは、次のような場合に発生します。 • BGP ルータ ID が、LSP が割り当てられていないループバックのアドレスである。 • BGP ルータ ID がループバックのアドレスでない。 • カスタマーが複数の定義済み LSP を持っており、カスタマー トラフィックはルータ ID により与えられた LSP 以外の LSP を使用している。 • カスタマーが複数の定義済み LSP を持っており、カスタマー トラフィックがルートマップに基づいて LSP を切り替える。 上記の場合は、正しい BGP ネクスト ホップを指定する必要があります。 （注）　LSP エンドポイント ループバック IP アドレスを指定することで、Diagnostics は MPLS コアにある複数の LSP でコアの障害をテストおよび検出できるようになります。 詳細については、「MPLS - PE to PE テストへの LSP エンドポイント ループバック IP アドレスの設定」（P.11-36）を参照してください。
PE Access Circuit Interface	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core L3VPN - PE to PE in VRF	[PE Access Circuit Interface] フィールドに PE アクセス回線インターフェイスのインターフェイス名を入力するか、[Select] ボタンをクリックして PE アクセス回線インターフェイスを選択します。 （注）　[Select] ボタンをクリックすると [Select Device Interface] ウィンドウが開きます（「PE アクセス回線インターフェイスの選択」（P.11-25）を参照）。 PE アクセス回線インターフェイスを選択するには、有効な PE デバイス名を指定しておく必要があります。指定されたインターフェイスは、サイトの CE に接続されているアクセス回線インターフェイスになっている必要があります。指定されたインターフェイス名は、デバイスのインターフェイスと一致する必要がありますが、必ずしも Prime Provisioning デバイス インベントリに存在する必要はありません。

表 11-3　[L3VPN - CE to CE Diagnostics - Test Setupp] ウィンドウのフィールドの説明 （続き）

フィールド	有効なテスト タイプ	説明
CE Access Circuit Interface IP Address	L3VPN - CE to CE L3VPN PE to attached CE L3VPN - CE to PE across Core	ローカル サイトの CE アクセス回線インターフェイスの IP アドレスを入力します。これは、指定された PE に接続されているアクセス回線インターフェイスにする必要があります。 IPv4 アドレッシングと /30 サブネット マスク（255.255.255.252）または /31 サブネット マスク（255.255.255.254）を使用して設定された PE アクセス回線インターフェイスが選択された場合、その /30 または /31 サブネットで残っているホスト アドレスが [CE Access Circuit Interface IP Address] フィールドに自動的に入力されます。/31 マスク（255.255.255.254）サブネット マスクで設定されている PE アクセス回線インターフェイスを手動で入力した場合、CE アクセス回線インターフェイス IP アドレスの取得は、テストの開始後でないと試行されません。この場合、[CE Access Circuit Interface IP Address] フィールドは [OK] ボタンをクリックするまで自動入力されません。 PE アクセス回線インターフェイスが IP アンナンバードを使用している場合、または CE アクセス回線インターフェイスが別のサブネットにある場合、正しい CE アクセス回線インターフェイス IP アドレスを取得できません。 このテストは、管理対象および管理対象外のシスコ製 CE デバイスおよび他社製 CE デバイスをサポートしています。
Pings Ignored	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core	このチェックボックスをオンにして、プロバイダー コア ネットワークから発信された ping およびトレース ルート パケットを無視する ACL が CE で設定されていることを指定します。
Customer Device IP Address	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core	ローカル サイト カスタマー ネットワーク上のカスタマー デバイス IP アドレスを入力します。カスタマー デバイスの IP アドレスを入力すると、このデバイスへの接続性テストが実行されます。
Find by Service	All	[Populate using VPN/VRF] ウィンドウを開くには、[Find by Service] ボタンをクリックします。[Populate using VPN/VRF] ウィンドウでは、カスタマー VPN/VRF 情報を使用してテストを設定できます（「カスタマー VPN/VRF 情報を使用した設定」（P.11-31）を参照）。
[OK] ボタン	All	[OK] をクリックして、テストを実行します。
[Clear] ボタン	All	[Clear] をクリックして、ウィンドウのすべてのフィールドをリセットします。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

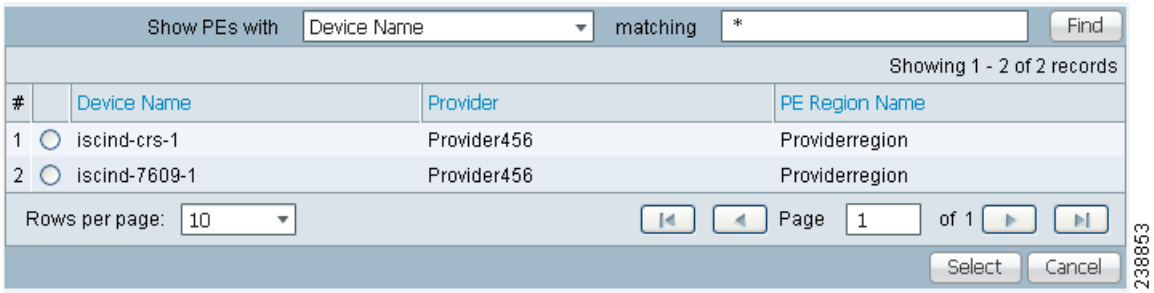
[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

PE デバイスの選択

（ローカルまたはリモートの [PE Device Name] の）[Select] ボタンをクリックすると、[Select PE Device] ウィンドウ（図 11-11 を参照）が開き、ローカルまたはリモート サイト PE を選択できます。[Select PE Device] ウィンドウには、インベントリで使用できるすべての PE デバイスを含むテーブルが表示されます。

（注）　Diagnostics デバイス セレクタのデフォルト値を設定できます。図 11-11 を参照してください。設定可能な値は、[Device Name]、[Provider]、および [PE Region Name] です。

図 11-11　[Select PE Device] ウィンドウ



（注）　PE 表に表示されるすべての PE 属性について、ワイルドカードを使用した文字列検索を実行できます。Prime Provisioning インベントリからローカルまたはリモート サイトの PE を選択すると、ローカルまたはリモートの [PE Device Name] フィールドに入力されたすべての値が上書きされます（図 11-9 を参照）。この検索機能は、大量の PE がある大規模なネットワークで便利です。

PE アクセス回線インターフェイスの選択

（ローカルまたはリモートの [PE Access Circuit Interface] の）[Select] ボタンをクリックすると、[Select Device Interface] ウィンドウ（図 11-12 を参照）が開き、インターフェイス名を選択できます。[Select Device Interface] ウィンドウには、選択されたローカルまたはリモート PE デバイスのすべてのインターフェイスを含むテーブルが表示されます。

図 11-12　[Select Device Interface] ウィンドウ

表に表示されるすべての属性について、ワイルドカードを使用した文字列検索を実行できます。Prime Provisioning インベントリからローカルまたはリモートの PE アクセス回線インターフェイスを選択すると、ローカルまたはリモートの [PE Access Circuit Interface] フィールドに入力されたすべての値が上書きされます（図 11-9 を参照）。

表 11-4 に、[Select Device Interface] ウィンドウのフィールドの説明を示します。

ワンポイントアドバイス

[Show Device Interfaces with] ドロップダウン ボックスと [matching] フィールドを使用して、最初に適切な検索パターンを入力します（図 11-12 を参照）。これによって、大規模なネットワークで発生する、大きくて時間がかかる余分な検索をせずに済みます。表 11-4 に、[Select Device Interface] ウィンドウのフィールドの説明を示します。

表 11-4　[Select Device Interface] ウィンドウのフィールドの説明

フィールド	説明
Show Device Interfaces with	[Show Devices with] ドロップダウン ボックスを使用して、検索結果を調整できます。ドロップダウン メニューから [Interface Name]、[IPV4 Address]、[IPV6 Address]、[VRF Name]、または [Interface Description] を選択して、検索結果を調整するカテゴリを選択します。
matching（オプション フィールド）	[Show Devices with] ドロップダウン ボックスで選択したカテゴリ内の検索を調整するための情報を、[matching] フィールドに入力します。部分文字列としてテキストを入力します。ワイルドカードもサポートされます。
LDP Termination Only	[LDP Termination Only] チェックボックスは、LDP 終端ループバック インターフェイスの選択が必要な場合に、LDP 終端ループバック インターフェイスをフィルタリングするために使用します。このチェックボックスは、オフのままにします。
Find	[Find] をクリックして、[Select Device Interface] ウィンドウで設定した情報を使用して検索を実行します。

表 11-4　[Select Device Interface] ウィンドウのフィールドの説明 （続き）

フィールド	説明
Interface Name	検索の実行後、見つかったインターフェイスのリストが表示されます。[Interface Name] カラムのヘッダーをクリックすると、インターフェイス名のリストがソートされます。
IPV4/IPV6 Address	検索の実行後、見つかった IPV4/IPV6 アドレスのリストが表示されます。[IPV4/IPV6 Address] カラムのヘッダーをクリックすると、IPV4/IPV6 アドレスのリストがソートされます。 IPV6 アドレスを選択するには、既存のリストから選択するか、手動で入力します。
VRF Name	検索の実行後、見つかった VRF 名のリストが表示されます。[VRF Name] カラムのヘッダーをクリックすると、VRF 名のリストがソートされます。
Interface Description	検索の実行後、見つかったインターフェイスの説明のリストが表示されます。[Interface Description] カラムのヘッダーをクリックすると、インターフェイスの説明のリストがソートされます。
Row per page	表に表示される行の行数が表示されます。テーブルの行を選択するには、対応するオプション ボタンをクリックします。
Select	[Select] をクリックして、テーブルでの選択を確認します。テーブルで選択した値が [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics] ウィンドウが表示されます。
Cancel	[Cancel] をクリックすると、[Select Device for VRF Search] ウィンドウが閉じます。

ヒント　[Interface Description] を使用して、カスタマー接続の詳細を記述することを推奨します。Diagnostics では、[Interface Description] の検索ができます（カスタマー回線 ID など）。詳細については、「L3VPN - CE to PE across Core テストの選択、設定、および実行」（P.11-33）および「L3VPN - PE to PE テストの選択、設定および実行」（P.11-34）を参照してください。

IOS マルチリンク アクセス回線インターフェイス間のテスト

Diagnostics では、Cisco IOS マルチリンク アクセス回線インターフェイスをまたがるトラブルシューティングがサポートされます。トラブルシューティングは、マルチリンク バンドル インターフェイスでのみ実行されます。個別のバンドル リンクのトラブルシューティング、またはマルチリンク固有のトラブルシューティングは実行されません。次のマルチリンク技術がサポートされます。

- マルチリンク PPP over Frame Relay（マルチリンク グループ インターフェイス設定）
- マルチリンク PPP over Frame Relay（仮想テンプレート インターフェイス設定）
- マルチリンク PPP over ATM（マルチリンク グループ インターフェイス設定）
- マルチリンク PPP over ATM（仮想テンプレート インターフェイス設定）
- シリアル上のマルチリンク PPP
- マルチリンク フレームリレー

（注）　マルチリンクは Cisco IOS でのみサポートされ、Cisco IOS XR ではサポートされません。

（注）　マルチリンク アクセス回線インターフェイスでは、レイヤ 2 フレーム リレー、ATM、およびイーサネットのトラブルシューティングは実行されません。

各マルチリンク バンドルには、関連付けられている多数のインターフェイスがあります。マルチリンク アクセス回線で MPLS VPN 接続性検証テストを設定するときは、正しいインターフェイスを [MPLS VPN Test Configuration] ウィンドウの [PE Access Circuit Interface] フィールドに入力する必要があります。入力する必要があるインターフェイスは、使用するマルチリンク設定に応じて異なります。表 11-5 で、[PE Access Circuit Interface] フィールドに入力する必要があるインターフェイスについてマルチリンク技術ごとに説明します。

表 11-5　マルチリンク インターフェイス

マルチリンク技術	PE アクセス回線インターフェイス
ML-PPPoFR（マルチリンク グループ）	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-PPPoFR（Virtual-Template）	マルチリンク バンドルを表す仮想アクセス インターフェイス。
ML-PPPoATM（マルチリンク グループ）	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-PPPoATM（Virtual-Template）	マルチリンク バンドルを表す仮想アクセス インターフェイス。
ML-PPPoSerial	マルチリンク バンドルを表すマルチリンク インターフェイス。
ML-FR	仮想回線を設定しているフレーム リレー インターフェイス。これは、Multilink Frame Relay（MFR; マルチリンク フレーム リレー）インターフェイスまたは MFR インターフェイスのフレーム リレー サブインターフェイスの場合があります。

マルチリンク フレーム リレー（MFR）を除き、マルチリンク バンドルを表すインターフェイスを [PE Access Circuit Interface] フィールドに入力する必要があります。マルチリンク フレーム リレーの場合は、フレーム リレー インターフェイス、または仮想回線が設定されているサブインターフェイスを入力する必要があります。これは、MFR インターフェイスまたは MFR インターフェイスのサブインターフェイスの場合があります。いずれの場合も、[PE Access Circuit Interface] フィールドに入力されたインターフェイスには IP アドレスと VRF が必要で、アップ/アップ状態になっている必要があります。

PE デバイスの有効なマルチリンク バンドル インターフェイスを判別するには、**show ppp multilink** または **show frame-relay multilink** IOS コマンドを使用します。PE デバイスにアクティブなマルチリンク バンドルがない場合、設定済みマルチリンク バンドルがないか、設定済みマルチリンク バンドルのすべてのバンドル リンクがダウン/ダウン状態になっている可能性があります。

（注）　仮想アクセス インターフェイスは、動的に作成されて、割り当てられます。仮想アクセス インターフェイスが属するマルチリンク バンドルと、その役割は、インターフェイスの状態が変化するに従って変化することがあります。そのため、仮想アクセス インターフェイスは Prime Provisioning/Diagnostics リポジトリに保存されません。仮想アクセス インターフェイスを使用して VPN 接続性検証テストを設定するときは、手動でインターフェイス名を [MPLS VPN Test Configuration] ウィンドウの [PE Access Circuit Interface] フィールドに入力する必要があります。[Interface Selection] ポップアップ ダイアログボックスから仮想アクセス インターフェイスを選択することはできません。

カスタマー VRF 情報を使用した設定

[MPLS VPN Connectivity Verification] ウィンドウに情報を入力するときは、PE ホスト名または PE インターフェイスの詳細を入力する必要があります。場合によっては、PE ホスト名または PE インターフェイスの詳細がわからないことがあります。ただし、この情報は対応する既知の VRF 名によって識別できます。対応する VRF 名は、VRF 検索を使用して識別できます。

（注） VRF 名でインターフェイスを検索するには、あらかじめ Prime Provisioning タスク マネージャの Collect Configuration タスクを実行し、VRF 名を Prime Provisioning にアップロードしておく必要があります。VRF 検索は、最後に実行した Collect Configuration タスク内の情報に基づきます。タスク マネージャの Collect Configuration タスクの実行方法の詳細については、「デバイス設定の収集」（P.11-12）を参照してください。

ステップ 1　[MPLS VPN Connectivity Verification] ウィンドウの [Find by VRF] ボタンをクリックします。

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

（注） [Select Device for VRF Search] ウィンドウに表示されるフィールドは、PE データ フィールドに入力されているかどうかにかかわらず、最初は空です。

ステップ 2　[Select Device for VRF Search] ウィンドウに表示されるフィールドを設定します。

表 11-6 に、[Select Device for VRF Search] ウィンドウのフィールドの説明を示します。

ワンポイントアドバイス まず、該当する検索パターンを入力します。これによって、大規模なネットワークで発生する、大きくて時間がかかる余分な検索をせずに済みます。VRF 名のパターンを入力し、[Find] ボタンをクリックします。たとえば、*t** と入力して [Find] をクリックすると、文字 *t* で始まるすべての VRF のリストが表示されます。[Show Devices with] ドロップダウン ボックスから選択し、[matching] フィールドに情報を入力して [Find] をクリックすると、結果リストをさらにフィルタリングできます。表 11-6 に、[Select Device for VRF Search] ウィンドウのフィールドの説明を示します。

表 11-6　[Select Device for VRF Search] ウィンドウのフィールドの説明

フィールド	説明
VRF Search String	検索する VRF 名の文字列を入力します。部分文字列として VRF 名の文字列を入力します。ワイルドカードもサポートされます。
Show Devices with	[Show Devices with] ドロップダウン ボックスを使用して、検索結果を調整できます。ドロップダウン メニューから [Device Name]、[Interface Name]、[IPV4 Address]、[IPV6 Address]、または [Interface Description] を選択して、検索結果を調整するカテゴリを選択します。
matching（オプション フィールド）	[Show Devices with] ドロップダウン ボックスで選択したカテゴリ内の検索を調整するための情報を、[matching] フィールドに入力します。部分文字列としてテキストを入力します。ワイルドカードもサポートされます。
Find	[Find] をクリックして、[Select Device for VRF Search] ウィンドウで設定した情報を使用して VRF 検索を実行します。

表 11-6　[Select Device for VRF Search] ウィンドウのフィールドの説明 （続き）

フィールド	説明
Device Name	検索の実行後、見つかったデバイス名のリストが表示されます。[Device Name] カラムのヘッダーをクリックすると、デバイス名のリストがソートされます。
Interface Name	検索の実行後、見つかったインターフェイスのリストが表示されます。[Interface Name] カラムのヘッダーをクリックすると、インターフェイス名のリストがソートされます。
IPV4/IPV6 Address	検索の実行後、見つかった IPV4/IPV6 アドレスのリストが表示されます。[IPV4/IPV6 Address] カラムのヘッダーをクリックすると、IPV4/IPV6 アドレスのリストがソートされます。 IPV6 アドレスを選択するには、既存のリストから選択するか、手動で入力します。
VRF Name	検索の実行後、見つかった VRF 名のリストが表示されます。[VRF Name] カラムのヘッダーをクリックすると、VRF 名のリストがソートされます。
Interface Description	検索の実行後、見つかったインターフェイスの説明のリストが表示されます。[Interface Description] カラムのヘッダーをクリックすると、インターフェイスの説明のリストがソートされます。
Rows per page	表に表示される行の行数が表示されます。テーブルの行を選択するには、対応するオプション ボタンをクリックします。
Select	[Select] をクリックして、テーブルでの選択を確認します。テーブルで選択した値が [PE Device Name] および [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが表示されます。
Cancel	[Cancel] をクリックすると、[Select Device for VRF Search] ウィンドウが閉じます。

ステップ 3　[Find] をクリックして、検索を開始します。

[Select Device for VRF Search] ウィンドウに表示されるテーブルに、検索結果が入力されます。

ヒント　各カラムに表示されている情報をソートするには、カラム見出しをクリックします。

ヒント　[VRF Name] および [Interface Description] カラムの情報を表示するため、必要に応じてテーブルの幅が自動的に拡大されます。テーブルの幅が拡大された場合は、水平方向のスクロールバーを使用してウィンドウの右側にスクロールします。

ステップ 4　（任意）[Show Devices with] ドロップダウン ボックスおよび [matching] フィールドを設定して、検索結果を調整します。

[Find] をクリックして、検索結果でテーブルを更新します。

ステップ 5　オプション ボタンをクリックして、必要な PE デバイス名とインターフェイス名を選択します。

ステップ 6　[Select] をクリックします。

[Select Device for VRF Search] ウィンドウが閉じます。選択した値が [PE Device Name] および [PE Access Circuit Interface] フィールドに入力された状態で、[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが表示されます。

カスタマー VPN/VRF 情報を使用した設定

Diagnostics は、他の Prime Provisioning 機能から独立して、スタンドアロンで使用できます。ただし、Prime Provisioning VPN/VRF プロビジョニング機能を使用してネットワーク内で VPN/VRF をプロビジョニングしている場合は、MPLS VPN 接続性検証テストを設定する代替手段として、カスタマーおよび VPN/VRF に関連付けられているこのプロビジョニング情報を使用できます。デバイス固有の設定を指定するのではなく、カスタマー、VPN/VRF、ローカル サイト、およびリモート サイトを指定します。必要なすべてのテスト設定は、この情報から取得されます。

（注）　カスタマー VPN/VRF 情報を使用して MPLS VPN 接続性検証テストを設定するオプションは、Prime Provisioning VPN/VRF プロビジョニング機能を使用してネットワーク内で VPN/VRF をプロビジョニングしている場合にのみ使用できます。

ステップ 1　[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの [Find by Service] ボタンをクリックします。

[Populate using VPN/VRF] ウィンドウが表示されます。

ステップ 2　[Populate using VPN/VRF] ウィンドウに表示されるフィールドを設定します。

表 11-7 に、[Populate using VPN/VRF] ウィンドウのフィールドの説明を示します。

表 11-7　[Populate using VPN/VRF] ウィンドウのフィールドの説明

フィールド	説明
カスタマーの詳細	
Customer Name	[Select] ボタンをクリックして、[Select Customer] ポップアップ ウィンドウからカスタマーを選択します。
VPN/VRF Name	[Select] ボタンをクリックして、[VPN/VRF name] ポップアップ ウィンドウから VPN/VRF 名を選択します。 （注）　カスタマー名を選択してからでないと、VPN/VRF 名は選択できません。
サイトの詳細	
Local Site	[Select] ボタンをクリックして、[Local Site] ポップアップ ウィンドウからローカル サイトを選択します。 （注）　カスタマー名および VPN/VRF 名を選択してからでないと、ローカル サイトは選択できません。
Remote Site	[Select] ボタンをクリックして、[Remote Site] ポップアップ ウィンドウからリモート サイトを選択します。 （注）　カスタマー名および VPN/VRF 名を選択してからでないと、リモート サイトを選択できません。 （注）　[Remote Site] フィールドは、PE to attached CE テスト タイプでは使用できません。

ステップ 3　[OK] をクリックします。

[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウが再表示されます。[Populate using VPN/VRF] ウィンドウで指定したカスタマー VPN/VRF 情報に基づいて、必要なフィールドが入力されます。

（注）　カスタマー デバイスをテストする場合は、ローカルまたはリモート サイトの [Customer Device IP Address] フィールドに IP アドレスを入力できます。

（注）　自動入力された [L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの任意のフィールドを編集できます。

ステップ 4　[L3VPN - CE to CE Diagnostics - Test Setup] ウィンドウの [OK] をクリックして、テストを実行します。

[Progress] ウィンドウが表示されます（「[Progress] ウィンドウ」（P.11-39）を参照）。

VPN トポロジ

デフォルトで、MPLS VPN 接続性検証テストでは、ローカル サイトとリモート サイトはフル メッシュ VPN トポロジで接続され、これらのサイトは直接通信できると見なされます。テストするサイトがフル メッシュ以外の VPN トポロジで接続されている場合、MPLS VPN 接続性検証テストに必要な設定が異なる場合があります。この場合、テストから誤った結果が得られることがあります。そのため、テスト結果を解釈するときには注意が必要です。サポートされる各 VPN トポロジで必要な設定の詳細、およびテスト結果の解釈方法については、「VPN トポロジ」（P.11-51）を参照してください。

L3VPN - PE to attached CE テストの選択、設定および実行

この項では、L3VPN - PE to attached CE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

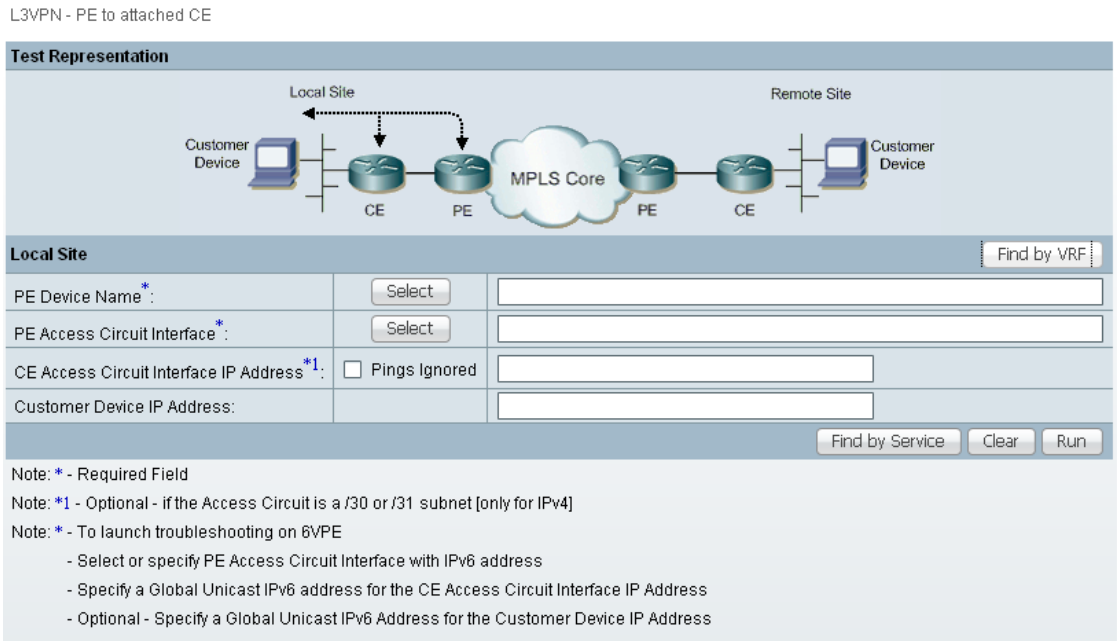
ステップ 1　[Diagnostics] メニューから、[L3VPN - PE to Attached CE] テスト タイプを選択します。

ステップ 2　[L3VPN - PE to attached CE] 接続性検証テスト タイプをクリックします。

PE to attached CE 接続性検証テスト タイプの詳細については、「L3VPN - PE to attached CE 接続性テスト」（P.11-15）を参照してください。

[MPLS VPN Connectivity Verification Configuration] ウィンドウ（図 11-13 を参照）が表示され、PE to attached CE テスト タイプに対応したフィールドが表示されます。[MPLS VPN Connectivity Verification Configuration] ウィンドウで、実行する接続性テストを設定できます。

図 11-13　L3VPN - PE to Attached CE テスト タイプ



[L3VPN - PE to Attached CE] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [L3VPN - PE to Attached CE] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to attached CE テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

L3VPN - CE to PE across Core テストの選択、設定、および実行

この項では、L3VPN - CE to PE across Core テスト タイプを選択、設定、および実行する方法の詳細について説明します。

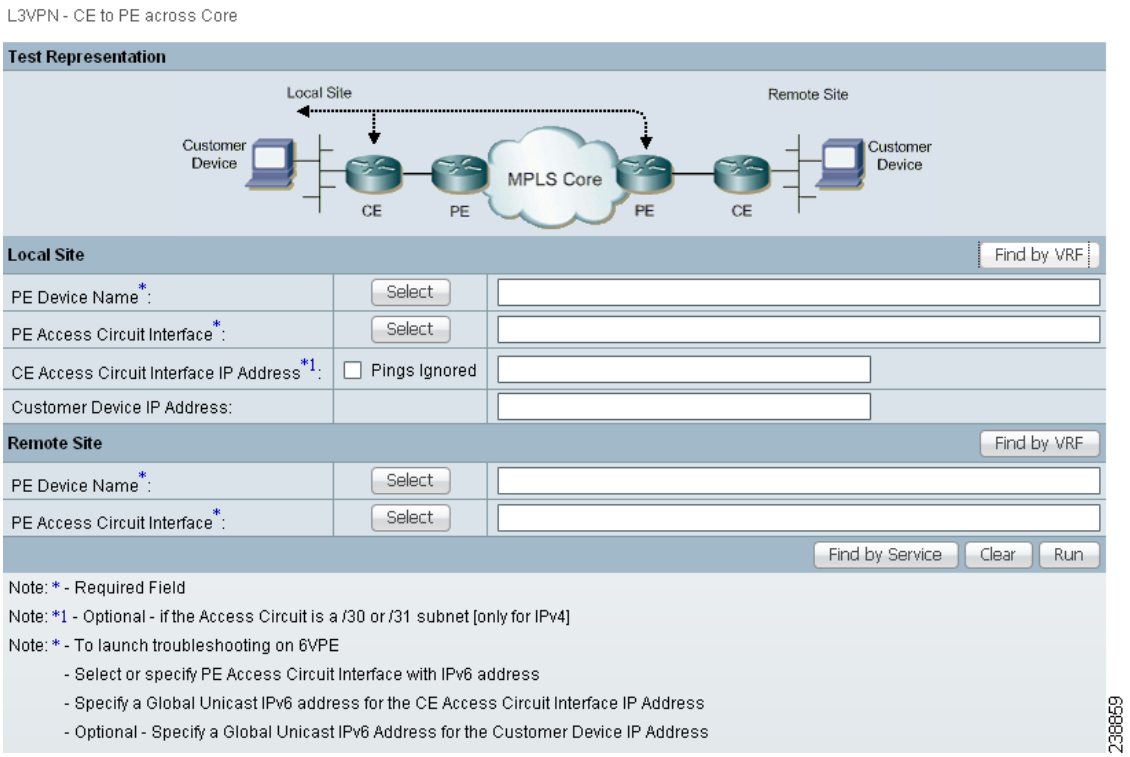
ステップ 1　[Diagnostics] メニューから、[L3VPN - CE to PE across Core] テスト タイプを選択します。

ステップ 2　[L3VPN - CE to PE across Core] 接続性検証テスト タイプをクリックします。

[L3VPN - CE to PE across core] 接続性検証テスト タイプの詳細については、「L3VPN - CE to PE across Core 接続性テスト」（P.11-16）を参照してください。

[L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup] ウィンドウ（図 11-14 を参照）が表示され、L3VPN - CE to PE across Core テスト タイプに対応したフィールドが表示されます。[L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup] ウィンドウで、実行する接続性テストを設定できます。

図 11-14　L3VPN - CE to PE across Core テスト タイプ



[L3VPN - CE to PE Across Core] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [L3VPN - CE to PE across Core] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - CE to PE across core テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

L3VPN - PE to PE テストの選択、設定および実行

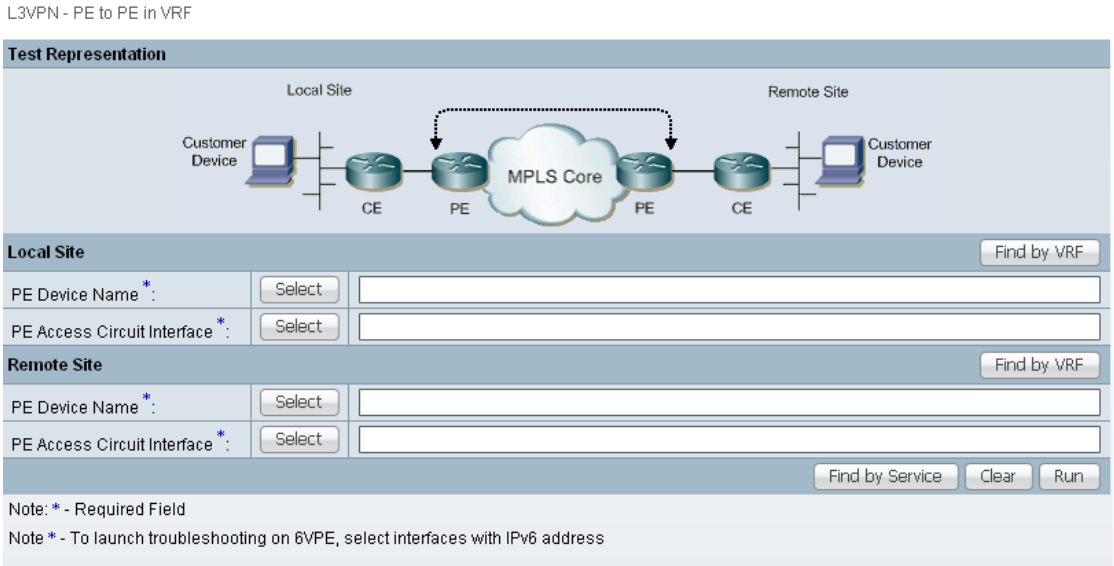
この項では、L3VPN - PE to PE テスト タイプを選択、設定、および実行する方法の詳細について説明します。

ステップ 1　[Diagnostics] メニューから、[L3VPN - PE to PE] テスト タイプを選択します。

L3VPN- PE to PE in VRF 接続性検証テスト タイプの詳細については、「L3VPN - PE to PE in VRF 接続性テスト」（P.11-17）を参照してください。

[L3VPN- PE to PE in VRF Diagnostics - Test Setup] ウィンドウ（図 11-15 を参照）が表示され、L3VPN - PE to PE in VRF テスト タイプに対応したフィールドが表示されます。[L3VPN- PE to PE in VRF Diagnostics - Test Setup] ウィンドウで、実行する接続性テストを設定できます。

図 11-15　　L3VPN - PE to PE テスト タイプ



[L3VPN - PE to PE in VRF Diagnostics - Test Setup] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

  これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 2　必要に応じて [L3VPN - PE to PE in VRF Diagnostics - Test Setup] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to PE in VRF テスト タイプに対応するフィールドの説明を示します。

ステップ 3　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

MPLS - PE to PE テストの選択、設定および実行

この項では、L3VPN - PE to PE（コア）テスト タイプを選択、設定、および実行する方法の詳細について説明します。

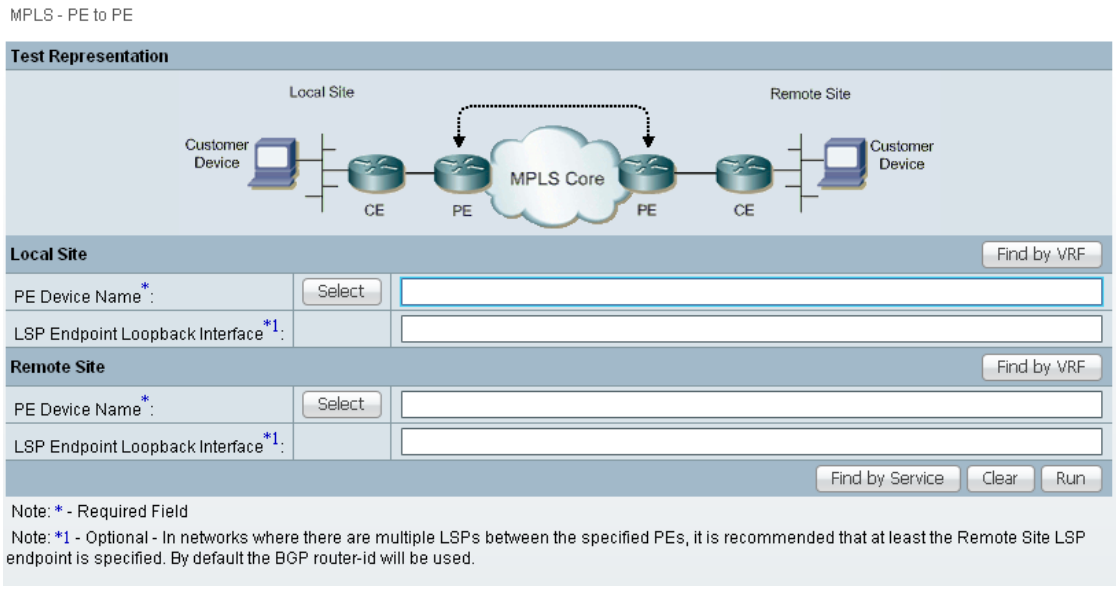
ステップ 1　[Diagnostics] メニューから、[MPLS - PE to PE] テスト タイプを選択します。

ステップ 2　[MPLS - PE to PE] 接続性検証テスト タイプをクリックします。

PE to PE 接続性検証テスト タイプの詳細については、「L3VPN - PE to PE 接続テスト」（P.11-17）を参照してください。

[MPLS - PE to PE] ウィンドウ（図 11-16 を参照）が表示され、MPLS - PE to PE テスト タイプに対応したフィールドが表示されます。[MPLS - PE to PE] ウィンドウを使用して、実行する接続性テストを設定できます。

図 11-16　　MPLS - PE to PE テスト タイプ



[MPLS - PE to PE] ウィンドウには、次のコンポーネントが表示されます。

- ネットワーク図
- ローカル サイト設定領域
- リモート サイト設定領域

これらのコンポーネントおよびテスト範囲については、「L3VPN - CE to CE テストの選択、設定および実行」（P.11-19）に詳しい説明があります。

ステップ 3　必要に応じて [MPLS - PE to PE] ウィンドウのフィールドを設定します。

表 11-3（P.11-22）に、L3VPN - PE to PE テスト タイプに対応するフィールドの説明を示します。

ステップ 4　すべての必須フィールドに入力したら、[OK] をクリックしてテストを実行します。

[Progress] ウィンドウが表示されます。「[Progress] ウィンドウ」（P.11-39）を参照してください。

MPLS - PE to PE テストへの LSP エンドポイント ループバック IP アドレスの設定

この項では、MPLS - PE to PE テスト タイプで LSP エンドポイント ループバック インターフェイスおよび IP アドレスを設定する方法の詳細について説明します。

リモート LSP エンドポイント ループバック IP アドレス

L3 VPN カスタマー トラフィックは、カスタマー ルートの BGP ネクスト ホップ アドレスを使用して LSP を選択します。コアをテストするときは、ローカル PE からリモート PE に MPLS OAM ping およびトレースが実行されます。トラフィックが経由するものと同じ LSP を Diagnostics でテストするには、Diagnostics がテストする IP プレフィックスがカスタマー ルートの BGP ネクスト ホップ アドレスになるようにします。

PE to PE コア テスト タイプでは、Diagnostics はカスタマー ルート情報を持っていません。そのため、Diagnostics は BGP ネクスト ホップを識別できません。デフォルトで、Diagnostics は ping およびトレースの宛先をネクスト ホップではなくリモート PE の BGP ルータ ID に基づいて選択します。複数のコアがある、複数のループバック アドレスが制御トラフィックおよびデータ プレーン トラフィックに使用されるなど一部のネットワーク設定では、この BGP ルータ ID がカスタマー トラフィックで使用されるネクスト ホップと一致せず、不正な LSP がテストされる（または、どの LSP もテストされない）ことがあります。

ローカル LSP エンドポイント ループバック IP アドレス

進行方向で実行したテストで問題を検出できなかった場合は、MPLS - PE to PE テスト タイプで逆方向のテストを実行できます。ローカル LSP エンドポイント ループバック IP アドレスを設定すると、逆方向のテストを実行するときに、正しい LSP が選択されます。

LSP エンドポイント ループバック IP アドレスを指定する場合

次の場合に、LSP エンドポイント ループバック IP アドレスを指定します。

- BGP ルータ ID が、LSP が割り当てられていないループバックのアドレスである。
- BGP ルータ ID がループバックのアドレスでない。
- 複数の LSP が定義されており、トラフィックはルータ ID により与えられた LSP 以外の LSP を使用している。
- 複数の定義済み LSP があり、トラフィックがルートマップに基づいて LSP を切り替える。

（注） リモート LSP エンドポイントを指定するときは、正しい BGP ネクスト ホップを指定する必要があります。

図 11-17 に、[LSP Endpoint Loopback IP Address] フィールドの使用方法を表したネットワーク トポロジの例を示します。このネットワーク トポロジの例には 3 つの論理 MPLS コアが存在し、一部の PE BGP ルータ ID はループバック インターフェイスに関連付けられていません。さらに、2 つの CE は、別々のコアにデュアルホーム接続されています。

図 11-17　ネットワーク トポロジの例

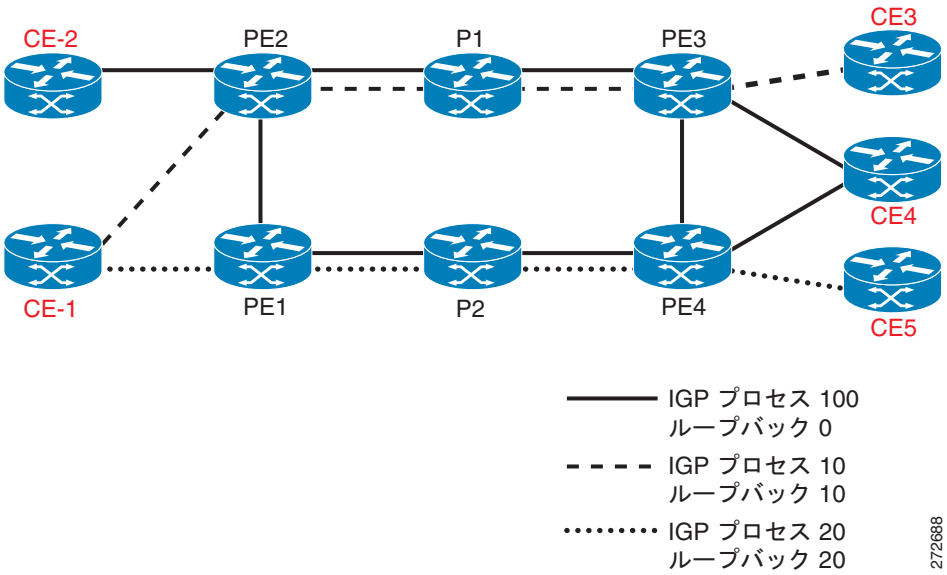


表 11-8 に、図 11-17 に示されているネットワーク トポロジの例に関連する IP アドレッシング情報を示します。

表 11-8　IP アドレス指定

PE	BGP ルータ ID	ループバック 0	ループバック 10	ループバック 20
PE2	1.1.1.1	1.1.1.1	N/A	20.20.20.1
PE3	1.1.1.3	1.1.1.3	N/A	20.20.20.3
PE1	50.50.50.1	1.1.1.6	10. 10.10.1	N/A
PE4	50.50.50.3	1.1.1.8	10. 10.10.3	N/A

表 11-9 に、各 LSP をテストするときにリモート LSP エンドポイント IP アドレスとして使用できる IP アドレスを示します。

表 11-9　各 LSP のテストに必要な入力

テスト対象の LSP	対象 CE	リモート サイトの PE	リモート エンドポイント
実線	CE-2	PE2	ネクスト ホップが BGP ルータ ID のため、必要ありません。
実線	CE-4	PE4	1.1.1.8（ループバック 0）
実線	CE-4	PE3	ネクスト ホップが BGP ルータ ID のため、必要ありません。
点線	CE-1	PE2	20.20.20.1（ループバック 20）
点線	CE-3	PE3	20.20.20.3（ループバック 20）
破線	CE-1	PE1	10. 10.10.1（ループバック 10）
破線	CE-5	PE4	10. 10.10.3（ループバック 10）

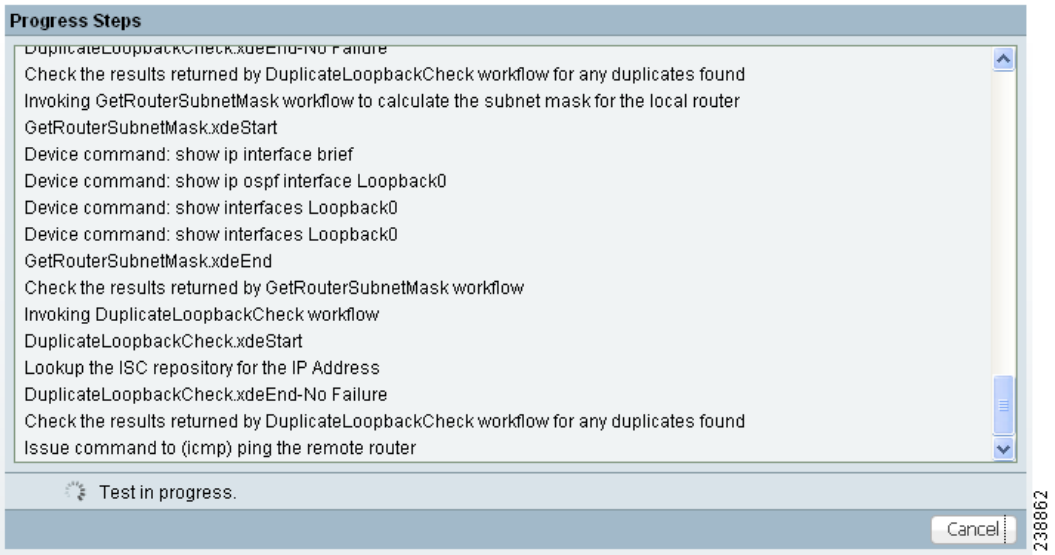
[Progress] ウィンドウ

テストの実行中に、[Progress] ウィンドウ（図 11-18 を参照）が表示されます。

（注）　MPLS VPN 接続性検証テストの実行時間は、場合によって異なります。ネットワークのサイズ、選択したテスト タイプ、接続性の問題が識別されたかどうか、および、この接続性の問題の性質によっては、テストの完了までにしばらく時間がかかることがあります。

[Progress] ウィンドウには、完了した各ステップに関する 1 行のテキストによるサマリーと、現在実行中のステップが表示されます。

図 11-18　[Progress] ウィンドウ



必要な場合、[Cancel] ボタンをクリックするとテストがキャンセルされます。[Cancel] をクリックすると、テストを本当にキャンセルするかどうかの確認を求められます。確認すると、現在のステップが完了し次第、テストがキャンセルされます。現在のステップでデバイス間のやり取りが行われている場合は、それが完了してからテストがキャンセルされます。キャンセルを実行すると、[Test Results] ウィンドウが表示され、テストをキャンセルしたことが表示されます。テスト ログには、完了したステップすべてが表示されます。

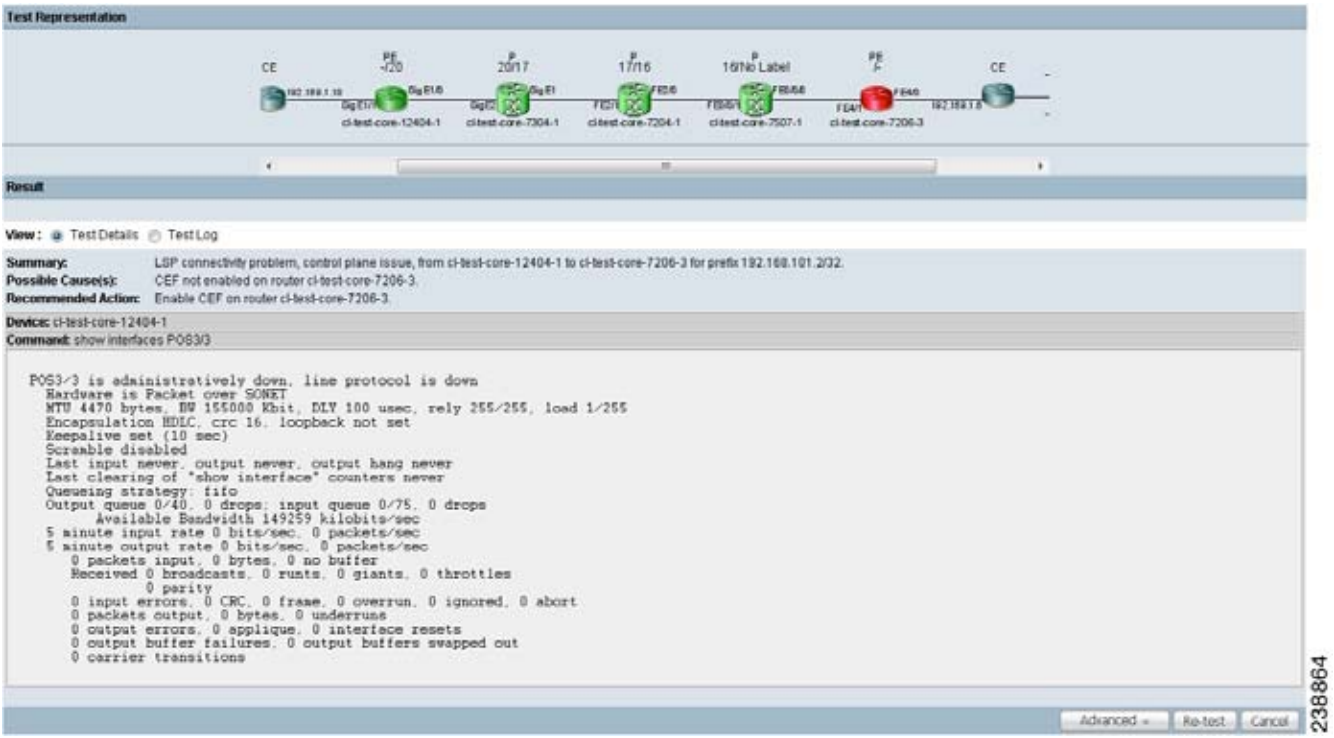
テストが完了すると、[Test Results] ウィンドウが表示されます。詳細については、「テスト結果の解釈」（P.11-39）を参照してください。

テスト結果の解釈

この項では、テスト結果の解釈方法について説明します。ここでは、次の項目について説明します。

MPLS VPN 接続性検証テストが完了すると、[Test Results] ウィンドウが表示されます（図 11-19 を参照）。

図 11-19　障害固有の追加情報が表示された [Test Results] ウィンドウ



[Test Result] ウィンドウには、見つかった問題の場所、原因、推奨されるアクション、観察結果、および実行された自動トラブルシューティングと診断ステップの詳細が表示されます。また、[Test Result] ウィンドウから、必要に応じて高度なトラブルシューティング オプションを起動できます（表 11-10 を参照）。

[Test Results] ウィンドウは、次のコンポーネントで構成されています。

表 11-10　[Test Results] ウィンドウのフィールドの説明

フィールド / ボタン	説明
Data path	「データ パス」（P.11-41）を参照してください。
Test Details	「Test Details」（P.11-43）を参照してください。
Test Log	「Test Log」（P.11-44）を参照してください。
[Export] ボタン	[Test Log] オプション ボタンを選択すると、[Export] ボタンが表示されます。「Export」（P.11-45）を参照してください。
[Advanced] ボタン	高度なトラブルシューティングを起動するには、[Advanced] ボタンをクリックします。「高度なトラブルシューティング オプション」（P.11-46）を参照してください。このボタンで使用できるオプションは、テスト結果およびテスト タイプに応じて動的に設定されます。

表 11-10　[Test Results] ウィンドウのフィールドの説明 （続き）

フィールド/ボタン	説明
[Re-test] ボタン	既存の設定を使用して再度接続性テストを実行するには、[Re-test] ボタンをクリックします。実装したフィックスを確認するために使用できます。
[Cancel] ボタン	現在のテストをキャンセルして [Test Configuration] ウィンドウに戻るには、[Cancel] ボタンをクリックします。キャンセルの確認は求められません。

テストしたパスに複数の障害がある場合、報告される障害は、Diagnostics が実行するトラブルシューティングの順序によって決まります。CE to CE 接続性テスト タイプの場合、Diagnostics トラブルシューティングは次の順序で実行されます。

1. アクセス回線（ローカルおよびリモート）。
2. MPLS Traffic Engineered（TE）トンネル。
3. MPLS コア。
4. MPLS VPN エッジ。

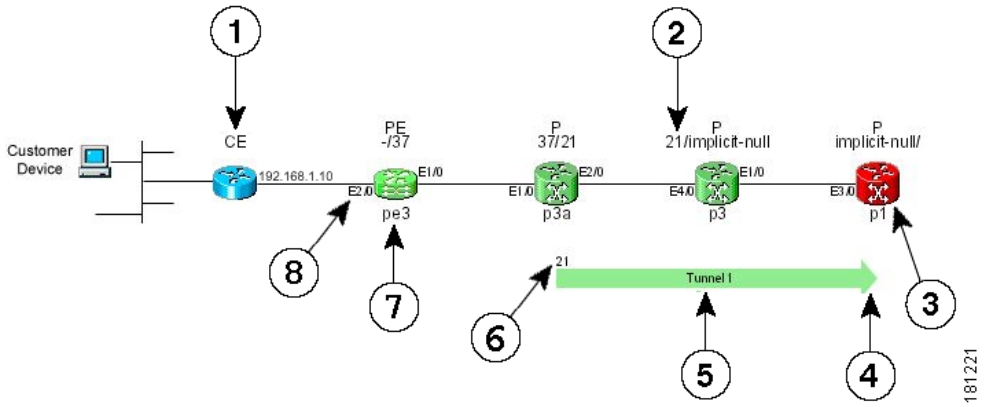
その他のテスト タイプも同じ順序でトラブルシューティングを実行しますが、すべてのステップを実行するわけではありません。

（注）　[Test Result] ウィンドウには、最初に見つかった障害の詳細が表示されます。複数の障害が存在する場合は、現在の障害を修復してテストを再実行しないと、後続の障害はレポートされません。

データ パス

データ パス（図 11-20 を参照）は、テスト対象の 2 つのサイト間のパスを図で示します。MPLS Traffic Engineered トンネルで障害が見つかった場合は、データ パスにはトンネルが表示されます。パス内の障害ポイントよりも前で見つかった、重複していない P-P、PE-P、または P-PE MPLS TE トンネルも、データパスに表示されます。

図 11-20　データ パス



1. デバイスのロール（CE、PE、または P）。
2. MPLS ラベル（入力/出力）。
3. 障害の発生したデバイス。

4. トンネルの方向を示す矢印。
5. トンネル名。
6. トンネル ラベル。
7. デバイスのホスト名。
8. インターフェイス名。

MPLS TE トンネルが存在する場合は、デバイス パスの下に表示されます。

カスタマー デバイス IP アドレスを指定した場合は、この IP アドレスは「Customer Device」という文字の横に表示されます。

（注）　MPLS TE トンネルは、そのトンネルが接続の問題の原因であると判明した場合のみ表示されます。

障害が見つかった場合は、データ パスで障害のあるデバイスまたはリンクが強調表示されます。データ パス内で使用されるデバイスの色については、表 11-11 を参照してください。

表 11-11　データ パスのデバイス カラー コード

色	アイコン	説明
緑色		デバイスはテスト済みで、正常に機能しています。
青色		デバイスはテストされていないか、ステータスが不明です。
赤		デバイスに障害が発生しています。
黄色		デバイスに障害が発生している可能性があります。
グレー		デバイスにアクセスできません。

データ パス内で使用されるリンクの色については、表 11-12 を参照してください。

表 11-12　データ パスのリンク カラー コード

色	アイコン	説明
赤		接続の問題が見つかっています。この障害の原因は、接続されているデバイスの片方または両方の問題である可能性があります。

各コア PE および P デバイスの場合は、次の情報が表示されます。

- ロール（PE または P）
- デバイス名
- インターフェイス名
- 入力および出力 MPLS ラベル（MPLS コアの障害のみ）

CE デバイスおよびカスタマー デバイスについては、最小限の情報しか表示されません。通常、これらのデバイスについては、テストの設定時に指定された情報だけが表示されます。

MPLS Traffic Engineered トンネルについては、次の情報が表示されます。

- トンネル名
- トンネルの方向（方向を示す矢印）
- トンネル ラベル

（注）　[Test Result] ウィンドウのデータ パスからは、デバイスには Telnet 接続できません。

Test Details

[Test Results] ウィンドウの [Test Details] セクション（図 11-19（P.11-40）を参照）には、自動トラブルシューティングおよび診断結果の概要、トラブルシューティング中の観察結果、その他の障害固有の情報、および推奨アクションが表示されます。Diagnostics によってレポートされる障害および観察結果の詳細について、およびトラブルシューティングの一環として Diagnostics により実行される IOS および IOS XR コマンドすべてのリストの詳細については、「障害シナリオ」（P.11-59）を参照してください。

テストの詳細の概要は、すべての場合で表示されます。テストの詳細の概要は、次の 3 つの詳細説明フィールドで構成されています。

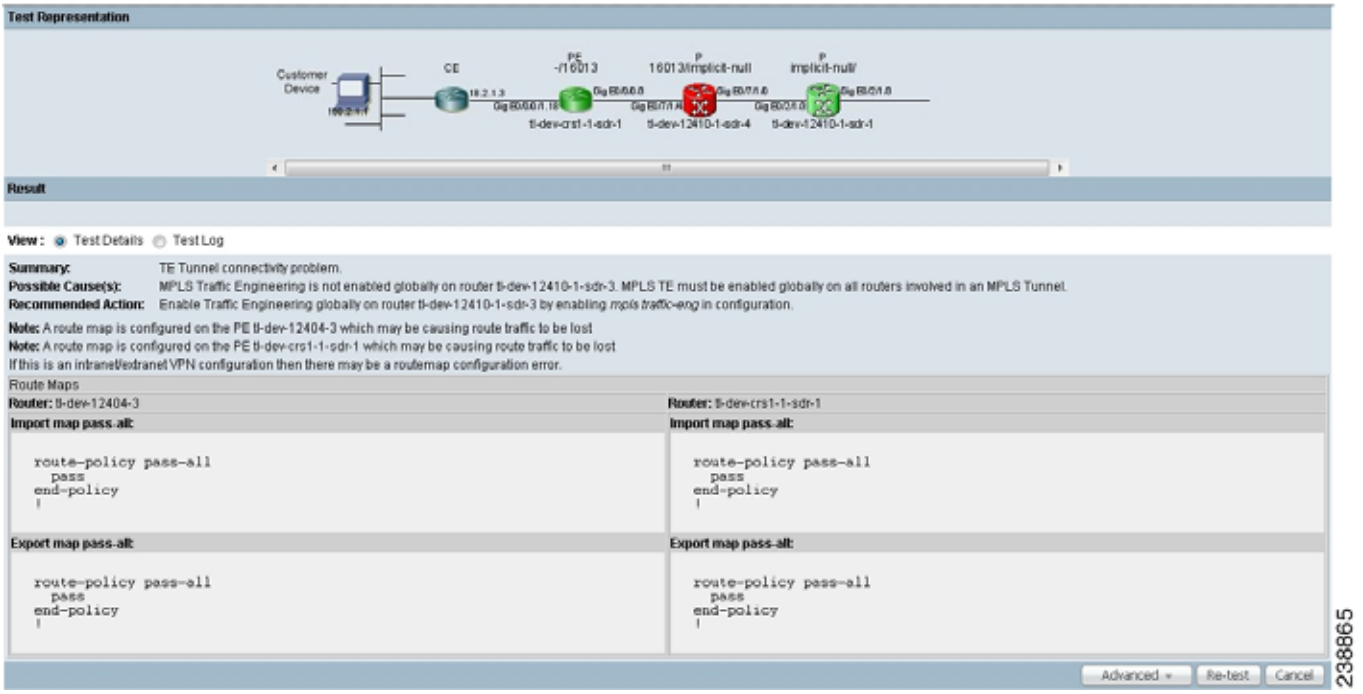
- [Summary]：見つかった障害の簡単な概要が表示されます。
- [Possible Cause(s)]：考えられる障害の原因です。
- [Recommended Action]：問題を解決するために推奨されるアクションです。

その他の障害固有の情報は、必要に応じて概要の下に表示されます。これが表示された場合は、見つかった問題についてのその他の情報が提供されます。たとえば、Forwarding Information Base（FIB; 転送情報ベース）、ラベル転送情報ベース（LFIB）、ボーダー ゲートウェイ プロトコル（BGP）のテーブル エントリおよびルート ターゲット インポート/エクスポートです。このその他の障害固有の情報は、FIB、LFIB、BGP の矛盾およびルート ターゲット インポート/エクスポートの不一致などの問題を明確にするために役立ちます。一部の障害については、その他の情報は表示されません。

図 11-19（P.11-40）に、テストの詳細の概要の下に障害固有の情報が表示された [Test Results] ウィンドウの例を示します。[Test Details] オプション ボタンはデフォルトで選択されています。

トラブルシューティング中に観察された内容は、テストの詳細の概要の下に注記として表示されます。観察の注記は、障害に関連する可能性のある、トラブルシューティング中に観察された内容の詳細を示します。この内容は、追加のトラブルシューティング情報と見なします。図 11-21 に、観察の注記が 2 つ表示された [Test Results] ウィンドウの例を示します。観察の注記は、まったく表示されない場合、または複数表示される場合があります。

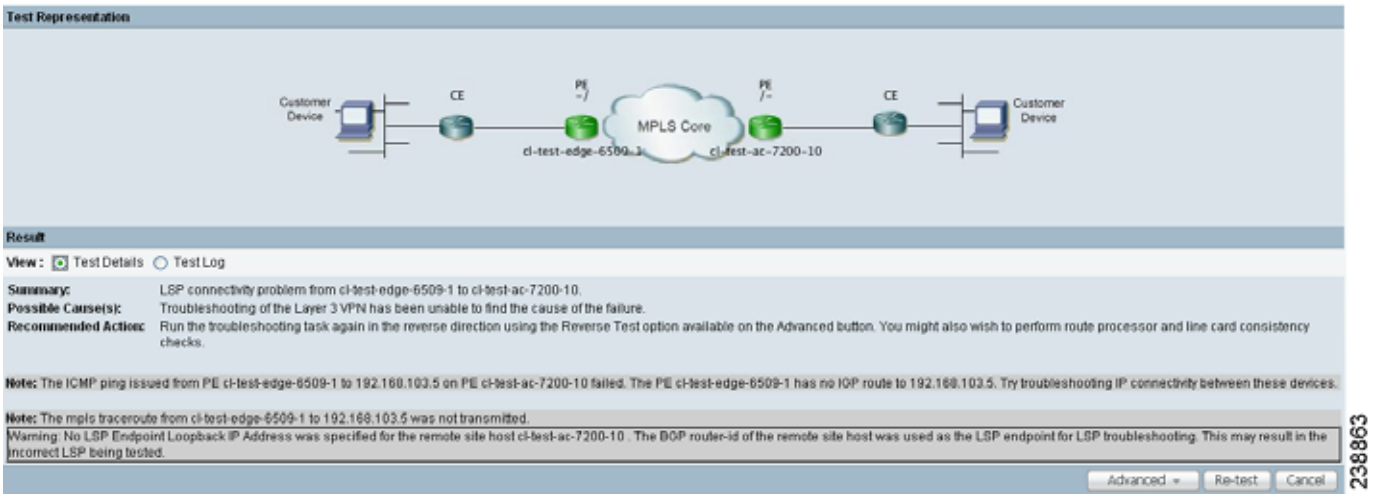
図 11-21　観察の注記が表示された [Test Results] ウィンドウ



Test Log

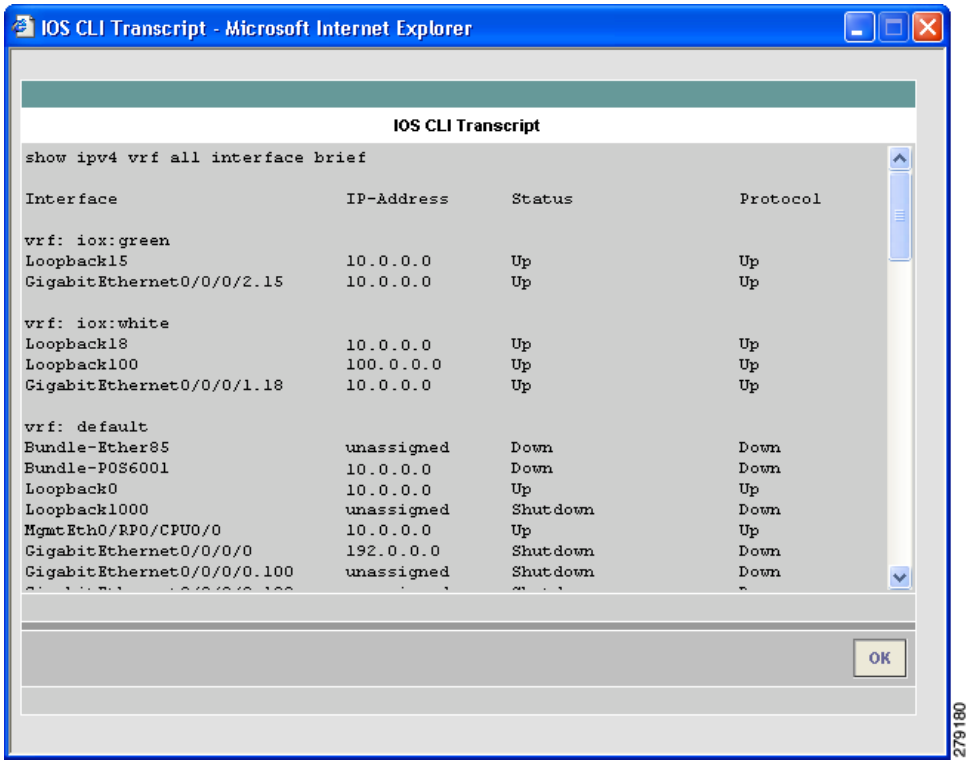
[Test Log]（図 11-22 を参照）オプション ボタンをクリックして、すべてのトラブルシューティングおよび診断ステップの詳細を、実行された順序で表示します。

図 11-22　[Test Results] ウィンドウ：テスト ログ



一部のステップでは、IOS または IOS XR CLI コマンドの実行など、デバイスからの入力が必要な場合があります。これらのステップは、テスト ログではハイパーリンクとして表示されます。ハイパーリンクをクリックすると、そのステップの IOS または IOS XR CLI トランスクリプトを示したポップアップ ウィンドウが表示されます（図 11-23 を参照）。このトランスクリプトには、実行された IOS または IOS XR コマンドおよびすべての結果の出力が含まれます。

図 11-23　[IOS CLI Transcript] ウィンドウ



Export

テスト ログをエクスポートして、トラブル チケットに含めたり、問題をエスカレーションしたり、または Cisco TAC に問い合わせしたりする際に使用できます。テスト ログは、テスト ログの下部にある [Export] ボタン（図 11-22（P.11-44）を参照）を使用してファイルにエクスポートできます。IOS および IOS XR CLI トランスクリプトを含め、テスト ログに表示されるすべてのステップはテキスト形式でエクスポートされます。

ステップ 1　[Export] ボタンをクリックします。

ブラウザ標準のファイル ダウンロード ウィンドウが表示され、ファイル名はデフォルトで「*export.rtf*」と表示されます。

ステップ 2　ファイルを保存します。

高度なトラブルシューティング オプション

この項では、次の高度なトラブルシューティング オプションについて説明します。

- 「リバース パス テスト」（P.11-46）
- 「LSP 可視化」（P.11-46）

高度なトラブルシューティングにより提供される追加オプションを、ネットワークのトラブルシューティングに使用できます。

サポートされている高度なトラブルシューティング オプションの詳細については、表 11-13 を参照してください。

表 11-13　高度なトラブルシューティング オプション

高度なトラブルシューティング オプション	説明
リバース パス テスト	障害が見つかった場合に使用できます。
LSP 可視化	障害が見つからなかった場合に使用できます。
LSP トラブルシューティング	IP の障害が見つかった場合に使用できます。

高度なトラブルシューティング オプションは、[Test Results] ウィンドウの下部にある [Advanced] ドロップダウン ボタンを使用して適切なものを使用できます。

リバース パス テスト

（注）　リバース パス テスト オプションは、PE to attached CE テスト タイプ以外のすべてのテスト タイプで使用できます。

場合によっては、MPLS VPN 接続性検証テストは接続の問題を検出しても、障害の原因を特定できない場合があります。逆方向（つまり、ローカル サイトとリモート サイトの設定を逆にした状態）でテストを繰り返すことにより、問題の原因を特定できる場合があります。その他の場合では、逆方向でテストを繰り返すことにより、結果として見つかった問題がさらに正確に診断される場合もあります。たとえば、接続性テストを進行方向で実行している間に、LSP 接続の問題がデバイスで特定される場合があります。しかし、この問題はダウンストリームの LSP ネイバーでの LDP 誤設定によって引き起こされた可能性もあります。逆方向でテストを繰り返すことにより、誤設定されたダウンストリーム ルータに最初に遭遇し、LDP 後設定が診断されます。この状況が発生した場合、[Test Results] ウィンドウに表示されるテストの詳細には、テストを逆方向で実行するように勧めるメッセージが表示されます。リバース テスト オプションは、[Test Results] ウィンドウの [Advanced] ドロップダウン ボタンから使用できます。

高度なトラブルシューティングのリバース テスト オプションを選択すると、逆方向状態で MPLS VPN 接続性検証テストが起動されます。それ以上の設定は必要ありません。

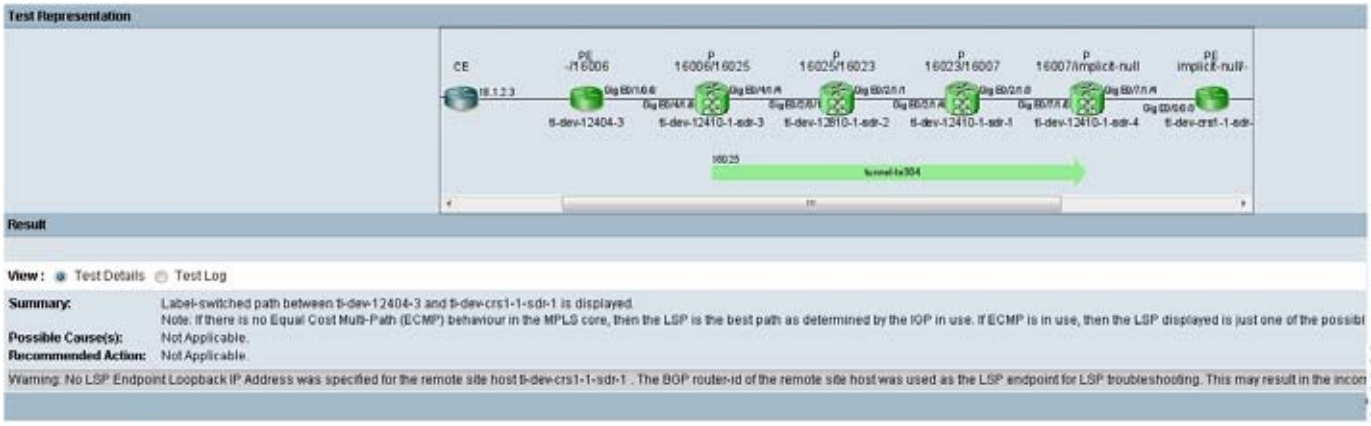
リバース パス テストの結果は、[Test Results] ウィンドウに表示されます。

LSP 可視化

（注）　LSP 可視化は、PE to attached CE テスト タイプ以外のすべてのテスト タイプで使用できます。

障害が見つからなかった場合、[Test Results] ウィンドウのデータ パスには、実行されたテストの概要が表示されます。テストされたコアを通過するパスの詳細は表示されません。LSP 可視化は、ローカル サイトとリモート サイト間の MPLS ラベル スイッチド パス（LSP）のホップバイホップ データ パスの図を表示します（図 11-24 を参照）。LSP 可視化では、転送パスの中間に見つかった、すべての重複していない PE-P 間、P-P 間、および P-PE 間のトンネルが表示されます。表示されるパスは、MPLS VPN 接続性検証テスト中にテストされたパスです。

図 11-24　[Test Results] ウィンドウ：LSP 可視化



データ パスには、テストされたパス内の各 PE および P デバイスについて、次の内容が表示されます。

- ロール（PE または P）
- デバイス名
- インターフェイス名
- 入力および出力ラベル

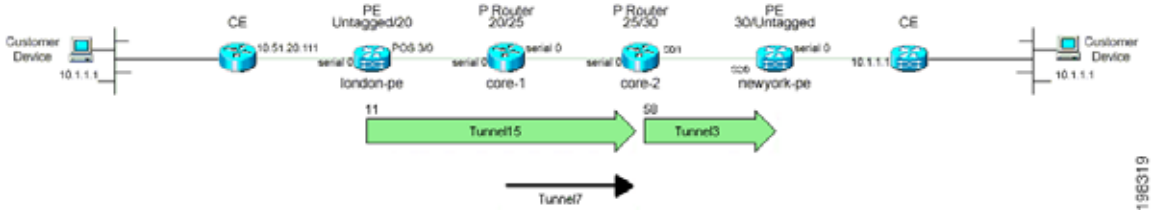
データ パスには、各 PE-PE 間の MPLS Traffic Engineered トンネルについて、次の内容が表示されます。

- トンネル名
- トンネルの方向（方向を示す矢印）
- トンネル ラベル
- トンネル タイプ

（注）　複数の MPLS TE トンネルが設定されている場合は、実際にトラフィックを伝送しているトンネルのみがデータパスに表示されます。

次の例では、Tunnel 7 は重複している（つまり、Tunnel 7 のヘッドエンドはアップストリーム ルータに設定されている Tunnel 15 のミッドポイントに設定されている）ため、表示されません。

図 11-25　複数の MPLS TE トンネル設定



データ パスに表示される内容についての詳細は、「データ パス」（P.11-41）を参照してください。

LSP 可視化は、MPLS VPN 接続性検証テストで接続の問題が検出されなかった場合のみ提供されます。

（注）　MPLS VPN 接続性検証テストをポストプロビジョニング検証に使用している場合は、LSP 可視化では MPLS コアを通過する LSP パスを表示することで、より高度な検証を提供します。

トンネル チェックのオフ：他社製 P ルータを使用したネットワークの場合

トンネルの診断中、Diagnostics はすべてのデバイスを確認して、そのポイントにトンネルが存在するかを確認する必要が生じる場合があります。Diagnostics は、他社製のデバイスにはログインしないため、他社製デバイスで発生している障害の誤診断を招き、（たとえそのデバイスが障害の実際の原因ではないとしても）トラブルシューティング ワークフローを進めることができなくなる場合があります。そのため、他社製デバイスが含まれるネットワークでは、トンネル診断をディセーブルにすることが役立ちます。

デフォルトでは、トンネル診断はイネーブルになっています。デフォルト値は、Admin ユーザが Prime Provisioning Control Center（[Administration] タブ > [Control Center] > [Hosts]）で変更できます。トンネル診断は、Command Flow Runner（CFR）コンポーネント（disableTunnelDiagnostics パラメータ）でイネーブルまたはディセーブルにできます。適切な disableTunnelDiagnostics パラメータが true に設定されている場合は、Diagnostics はトンネル診断を実行しません。

[Test Results] ウィンドウには、Diagnostics のトンネル診断がディセーブルであることを示す観察メッセージが表示されます。デバイスがインベントリに含まれていないことを示すエラー メッセージは、パス上の他社製デバイスが原因である可能性があること、およびエラーがこのデバイスまたはその近くのネイバーで発生していることを意味します。

Diagnostics の動作

この章では、Diagnostics アプリケーションの動作について説明します。

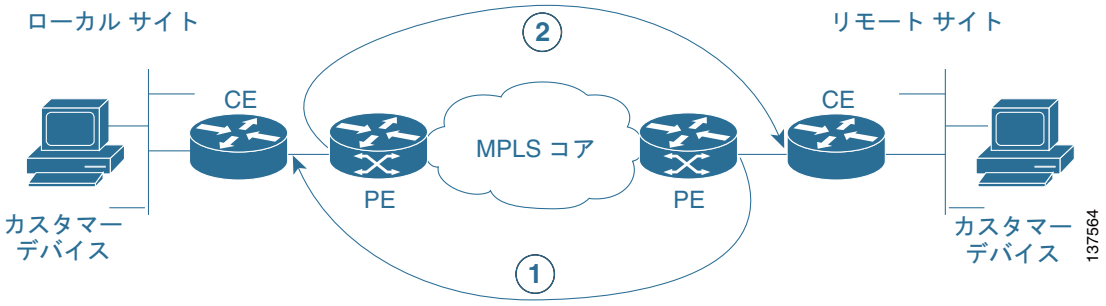
MPLS VPN 接続性検証テストは、接続性テスト、トラブルシューティング、および診断のステップで構成されています。各テストで実行される実際のステップは、検出された障害、およびネットワーク内の障害の場所によって異なります。テスト設定は簡単で結果はわかりやすいため、トラブルシューティングおよび診断のロジックについて理解する必要はほとんどありません。ただし、特にテスト ログを調べる場合など、トラブルシューティングおよび診断のプロセスを理解した方がよい場合があります。この章では、接続性のテスト、トラブルシューティング、および診断ロジックの概要について説明します。

（注）　この章で詳しく説明する手順は、Diagnostics が実行するテストのタイプの実例を示しています。ただし、このテストの一覧はすべてを網羅しているわけではなく、Diagnostics はこの他にも多くのテストを実行します。

テスト範囲は、入力したテスト設定によって決まります。たとえば各サイトでは、テストは、サイト内のカスタマー デバイスに対して実行することも、CE アクセス回線インターフェイスに対して実行することもできます。簡単にするために、この章ではすべてのサイトのテストが、CE アクセス回線インターフェイスに対するものであることを前提としています。

最初のステップでは、2 つのサイト間の VPN 接続性をテストして、問題がないかどうか判断します。これは、Cisco IOS VRF の ping 機能を使用して行います。このテストは、ローカル サイト サブネットのデバイスから、リモート サイト サブネットの宛先 IP アドレスに対して開始されることが理想的です。ただし、Prime Provisioning は管理対象および管理対象外のシスコ製 CE デバイスおよび他社製 CE デバイスをサポートしています。トラブルシューティングおよび診断の機能は、すべての場合に有効です。このため、このテストはコア ネットワーク内の PE および P デバイスからのみ開始できます。この制限を回避するには、接続性テストを 2 段階に分けて実行する必要があります（図 11-26 を参照）。

図 11-26　IOS VRF ping 接続性テスト



1. 第 1 段階（図 11-26 を参照）では、リモート サイト PE からローカル サイト CE への接続性をテストします。これは、Cisco IOS の **ping vrf** コマンドを使用して、宛先としてローカル サイト CE アクセス回線インターフェイスの IP アドレスを指定し、送信元 IP アドレスとしてリモート サイト PE アクセス回線インターフェイスを指定して実行します。
2. 第 2 段階（図 11-26 を参照）では、ローカル サイト PE からリモート サイト CE への接続性をテストします。このテストは、最初のテストの **ping vrf** コマンドで接続が正常であることが示された場合のみ実行します。これは、Cisco IOS **ping vrf** コマンドを使用し、宛先としてリモート サイト CE アクセス回線インターフェイスを指定し、送信元 IP アドレスとしてローカル サイト PE アクセス回線インターフェイスを指定して実行します。

リモート サイト PE からローカル サイト CE への接続性テストを先に実行しておくと、ローカル アクセス回線での問題が先に見つかるようになります。そのため、順方向パスの問題よりも前に、リバース パス MPLS VPN、MPLS コア、および MPLS TE トンネルの問題が見つかります。

2 段階に分けて接続性をテストすることにより、トラブルシューティングおよび診断機能で、ローカル サイトの CE からリモート サイトの CE へのエンドツーエンド テストのシミュレーションが可能になるため、サイト間のあらゆる VPN 接続の問題を識別できます。この接続性テストでは、2 つのサイト間の VPN、MPLS、および IP 接続を調べます。

VPN 接続性の問題は検出されないため、トラブルシューティングおよび診断は実行されません。VRF 接続の問題が検出された場合は、さらに一連の接続性テストを実行して、接続の問題の分離を試みます。これらのテストは PE デバイス上で開始され、VPN の障害が検出された方向で実行されます。次の内容で構成されています。

- コアから PE アクセス回線インターフェイス全体にわたる VRF ping。これにより、障害がアクセス回線にあるのか、CE と PE 間にあるのか、またはコア内にあるのか識別されます。
- コアから PE ループバック全体にわたる ICMP ping：これにより、IP 接続がコア全体で動作しているかどうか確認されます。
- コアから PE ループバック全体にわたる LSP ping：これにより、MPLS LSP パスがコア全体で動作しているかどうか確認されます。

障害が分離されると、テストがいずれかのポイントで停止することがあります。その後、自動トラブルシューティングおよび診断のステップが実行され、障害の原因が診断されます。実行されるステップは、障害の性質および場所によって異なります。トラブルシューティングは次の順序で実行されます。

1. アクセス回線（ローカルおよびリモート）。
   a. L3 接続性（CE およびカスタマー デバイスへの VRF ping とトレース）およびルート チェック。
   b. L2（ATM、イーサネット、フレーム リレー、シリアル）接続性およびステータス チェック。
   c. PE-CE ルーティング プロトコル判定およびステータス チェック。
   d. PE-CE ルーティング プロトコルおよび MP-BGP 再配布チェック。
2. MPLS VPN エッジ。
   a. MP-BGP ネイバーおよび VPN ルート チェック。
   b. VRF ルート制限およびチェック。
   c. ルート マップの存在チェック。
   d. PE–PE VRF（MPLS コア全体の VRF ping とトレース）接続性チェック。
   e. PE MPLS OAM 機能チェック。
3. MPLS Traffic Engineered（TE）トンネル。
   a. トンネル接続性（TE 対応の ping とトレース）およびステータス チェック。
4. MPLS コア。
   a. IP 接続性（ICMP ping）チェック。
   b. LSP 接続性（LSP ping とトレース）およびステータス チェック。
   c. LSP データパス生成。
   d. LSP 障害ローカリゼーション。
   e. LDP セッションおよびネイバー チェック。
   f. ラベル チェック。
   g. MPLS VPN エッジ。
   h. VPN ラベル チェック。
   i. VRF ルート ターゲット チェック。

（注）　コアのトラブルシューティングは、Cisco IOS の MPLS LSP ping および traceroute 機能をサポートしている PE デバイスのみに対して実行されます。サポートされているデバイス タイプおよび MPLS OAM がサポートされる Cisco IOS バージョンの詳細については、「サポートされているハードウェア、IOS、および IOS XR バージョン」（P.11-3）を参照してください。

（注）　プライマリ トンネルに FRR 保護が設定されている場合は、Diagnostics はプライマリ トンネルをトラブルシューティングし、（プライマリ トンネルに FRR 保護を提供しながら）プライマリ トンネルおよびバックアップ トンネルで検出された、障害の可能性をレポートします。トラブルシューティングの対象となるバックアップ トンネルは、ABR 間に設定された、FRR に対応しているプライマリ トンネルを保護するように設定されたトンネルに限られます。

障害の診断後、[Test Results] ウィンドウに診断結果および障害を解決するための適切な推奨アクションが表示されます。実行された接続性テストと、自動トラブルシューティングおよび診断の正確なステップは、[Test Results] ウィンドウの [Test Log] セクションに表示できます。

よくあるご質問

Q. MPLS VPN 接続性検証テストを実行すると、[Progress] ウィンドウがハングアップするように見え、同じステップが最大 5 分間実行されます。5 分後、[Test Results] ウィンドウに次のメッセージが表示されます。

```
Summary: Cannot connect or login to device router1.
Possible Cause(s): Device could be down, there could be problems with network
connectivity, or the login details in the repository might be incorrect
Recommended Action: Restore connectivity to the device before attempting the test.
If in-band network management is in use then you might want to consider performing
a Traceroute from the management station to device router1 to find where IP
connectivity fails.
```

A. デバイスにログインしようとしても、デバイスが応答しません。デバイスがダウンしていないことを確認します。Prime Provisioning サーバからデバイスへの IP 接続が確立されていることを確認します。Prime Provisioning リポジトリに設定されているデバイスのログイン詳細情報が、物理デバイスに設定されているログイン詳細情報に一致していることを確認します。デバイス上の使用可能なすべての VTY セッションが、使用されていないことを確認します。

Q. MPLS VPN 接続性検証テストを実行すると、ローカル サイトとして設定したデバイスが、時々 [Test Results] ウィンドウのデータ パスの左側に表示されることがあります。その他の場合では、ローカル サイト デバイスは [Test Results] ウィンドウのデータ パスの右側に表示されます。なぜでしょうか。

A. MPLS VPN での接続の問題は、特定の方向だけしか検出できない場合が多くあります。MPLS VPN 接続性検証テストでは、両方向（ローカル サイトからリモート サイト、およびその逆）についてテストされます。問題が発見されたときのテストの方向によって、ローカル サイトのデバイスは [Test Results] ウィンドウのデータ パスの左側または右側のいずれかに表示されます。

Q. 同じクライアント マシンで複数の MPLS VPN 接続性検証テストを並行して実行すると、このうちの 1 つのテスト結果が、すべてのテストの結果画面に表示されます。その他のテストの結果は失われます。回避する方法を教えてください。

A. 同じクライアント マシンで並行して複数の MPLS VPN 接続性検証テストを実行する場合は、各テストが異なる HTTP セッションを使用して実行されていることを確認する必要があります。これを実行するには、コマンドライン、またはデスクトップのブラウザのアイコン、または [Start] メニューから起動した個別のブラウザで各テストを実行します。同じブラウザ ウィンドウの別のタブ、または既存のブラウザ ウィンドウから起動したブラウザ ウィンドウで、複数のテストを並行して実行しないでください。

VPN トポロジ

この付録では、サポートされる VPN トポロジに MPLS VPN 接続性検証テストを実行する方法の詳細を示します。この付録の内容は、次のとおりです。

- 「セントラル サービス VPN トポロジでのテスト」（P.11-59）

フル メッシュ VPN トポロジでのテスト

デフォルトで、MPLS VPN 接続性検証テストでは、ローカル サイトとリモート サイトはフル メッシュ VPN トポロジで接続され、これらのサイトは直接通信できると見なされます。フル メッシュ VPN トポロジに MPLS VPN 接続性検証テストを設定する方法の詳細については、「MPLS VPN 接続性検証テストの実行」（P.11-18）を参照してください。

ハブ アンド スポーク VPN トポロジでのテスト

ハブ アンド スポーク VPN で接続されたカスタマー サイト同士は直接通信できません。カスタマー サイト（スポーク）はハブ ルータで通信します。ハブ アンド スポーク VPN で接続された 2 サイト間の接続性をテストする場合は、次の手順でテストを実行します。

ステップ 1　ローカル サイトとリモート サイト間の MPLS VPN 接続性検証テスト。

ステップ 2　ローカル サイトと、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

ステップ 3　リモート サイトと、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

ステップ 4　ローカル サイトと、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

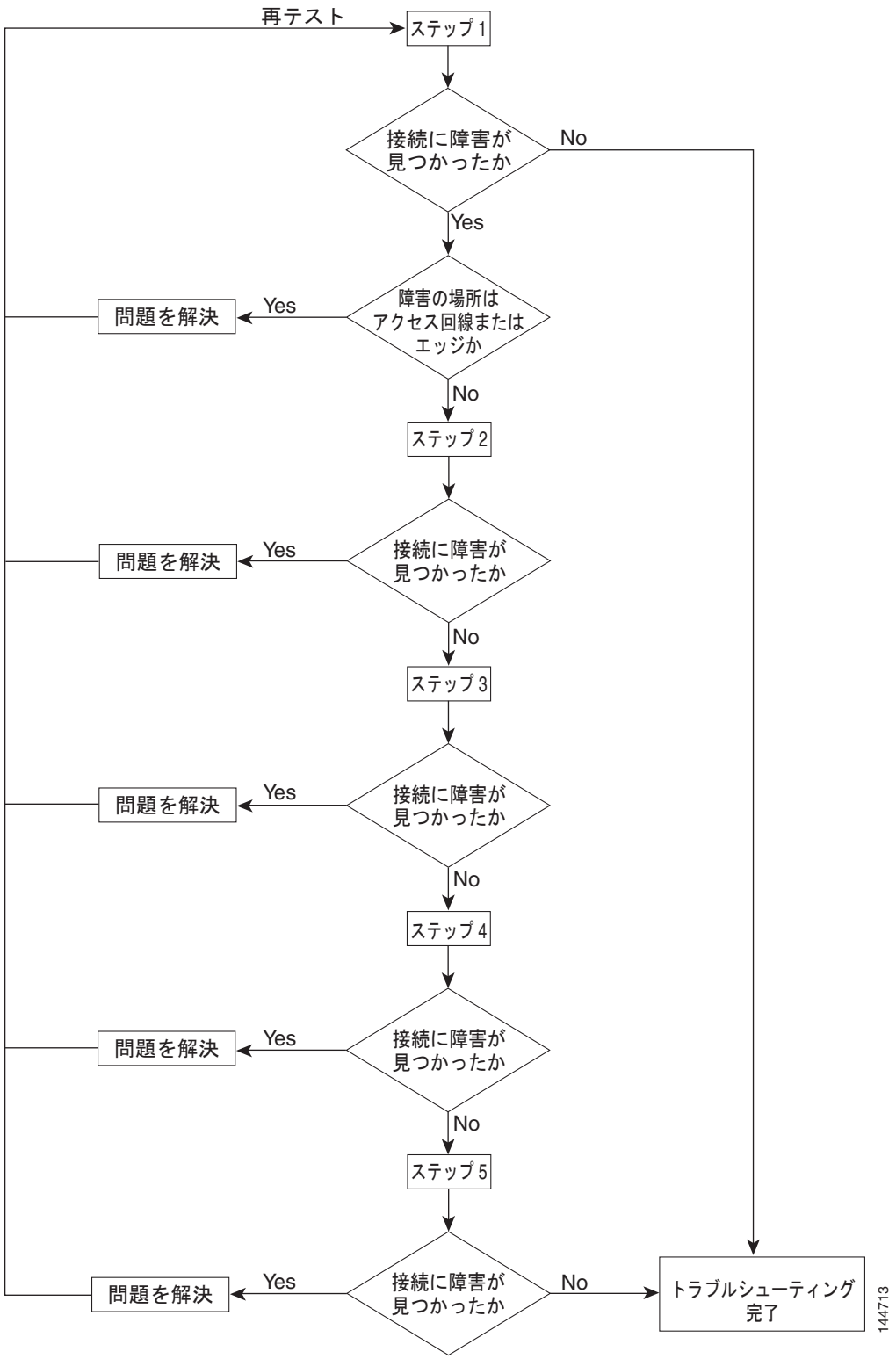
ステップ 5　リモート サイトと、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス間の MPLS VPN 接続性検証テスト。

各ステップでは、さまざまなポイント間で MPLS VPN 接続性検証テストを実行します。接続性障害があるかどうかと、この障害の場所によっては、5 つすべてのステップを実行する必要がない場合があります。図 11-27 に、ハブ アンド スポーク VPN をテストするワークフローを示します。

ステップ 1 からステップ 5 で報告された問題を解決してから、ステップ 1 を繰り返してサイト間の接続性が復元されたことを確認してください。

（注）　アクセス回線または VPN エッジの問題に起因する接続性障害がステップ 1 で検出された場合、その問題は、ステップ 1 で実行した MPLS VPN 接続性検証テストによって正しく診断されます。テスト結果の説明に従って問題を解消してください。接続性障害がハブ アンド スポーク MPLS VPN のコア内部の問題に起因する場合、ステップ 1 で報告される結果は正しくないことがあるため無視してください。ステップ 2 からステップ 5 を、問題が正しく診断されるまで実行してください。

図 11-27　ワークフロー

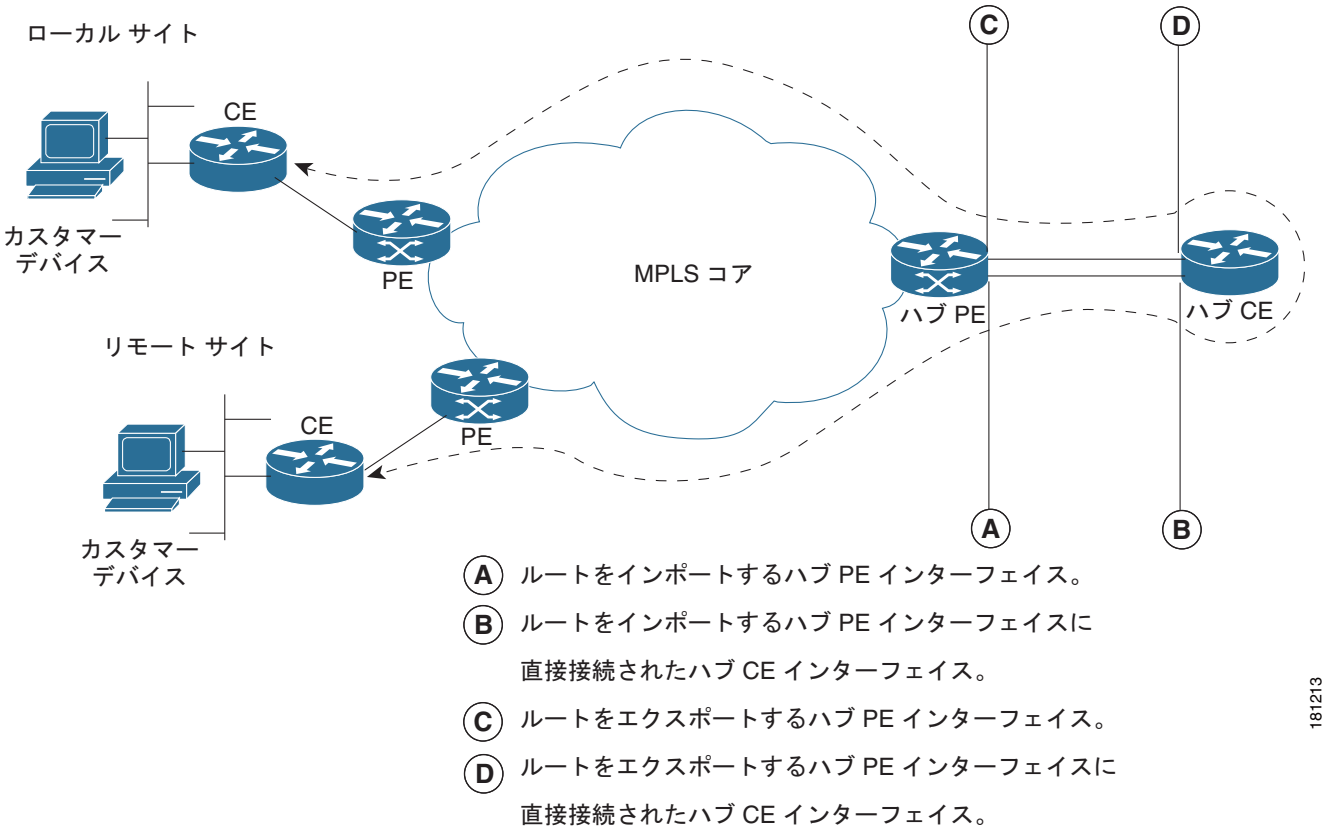


1. ローカル サイトとリモート サイト間の MPLS VPN 接続性検証テストを実行します。このテストで接続性の問題が見つからなければ、トラブルシューティングはこれ以上必要ありません。このテストで MPLS の問題が原因による接続性障害が報告された場合は、テスト結果を無視して 2. に進みます。MPLS VPN 接続性検証テストはフル メッシュ VPN トポロジを前提としているため、報告される問題は正しくありません。ハブ アンド スポーク VPN での問題を識別するためにさらに MPLS VPN 接続性検証テストを実行する必要があります。このテストで MPLS 以外の問題（たとえば、アクセス回線または VPN エッジの障害）が原因による接続性障害が報告された場合は、報告されたとおりに問題を解決して再度テストを行います。

（注）　接続性障害がコアで見つかった場合、1. で実行した MPLS VPN 接続性検証テストでは、ハブ アンド スポーク VPN トポロジがテスト中であることが検出され、以下のステップで説明されている、ハブ アンド スポークに固有のトラブルシューティングの実行を提案されることがあります。MPLS VPN 接続性検証テストは、ルート ターゲットのインポートおよびエクスポートを調べることでハブ アンド スポーク VPN トポロジを検出します。同じルート ターゲットが一方または両方の PE ルータによってインポートおよびエクスポートされると、ハブ アンド スポーク VPN と見なされます。

図 11-28 に、ハブ アンド スポーク VPN の 2 サイト間の接続性をテストするために必要な MPLS VPN 接続性検証テストを示します。

図 11-28　ハブ アンド スポーク VPN トポロジのテスト：ステップ 1



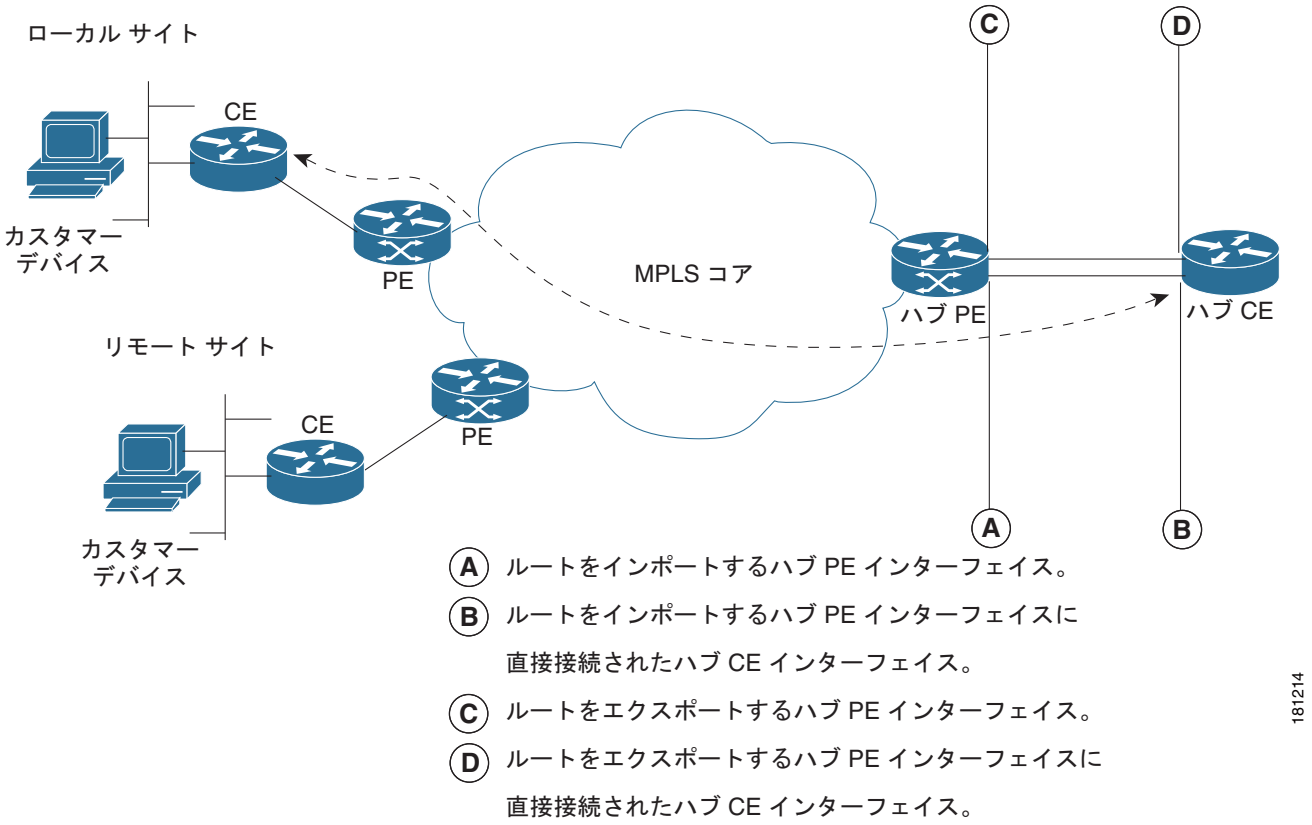
2. ローカル サイト（スポーク）と、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-29 の *B*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[MPLS VPN Connectivity Verification

Configuration] ウィンドウの [Local Site] フィールドに、ローカル カスタマー サイトの詳細を設定する必要があります。[Remote Site] フィールドには、ルートをインポートするハブ PE および CE インターフェイス（図 11-29 の *A* および *B*）の詳細を設定する必要があります（表 11-14 を参照）。

表 11-14　テストの設定：ルート インポート ハブ インターフェイスのテスト

フィールド名	ハブの詳細
PE Device Name	ハブ PE デバイス名
PE Access Circuit Interface	ルートをインポートするハブ PE インターフェイス。
CE Access Circuit Interface IP Address	ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイスの IP アドレス。
Customer Device IP Address	ブランクのままにします。

図 11-29　ハブ アンド スポーク VPN トポロジのテスト：ステップ 2



A　ルートをインポートするハブ PE インターフェイス。

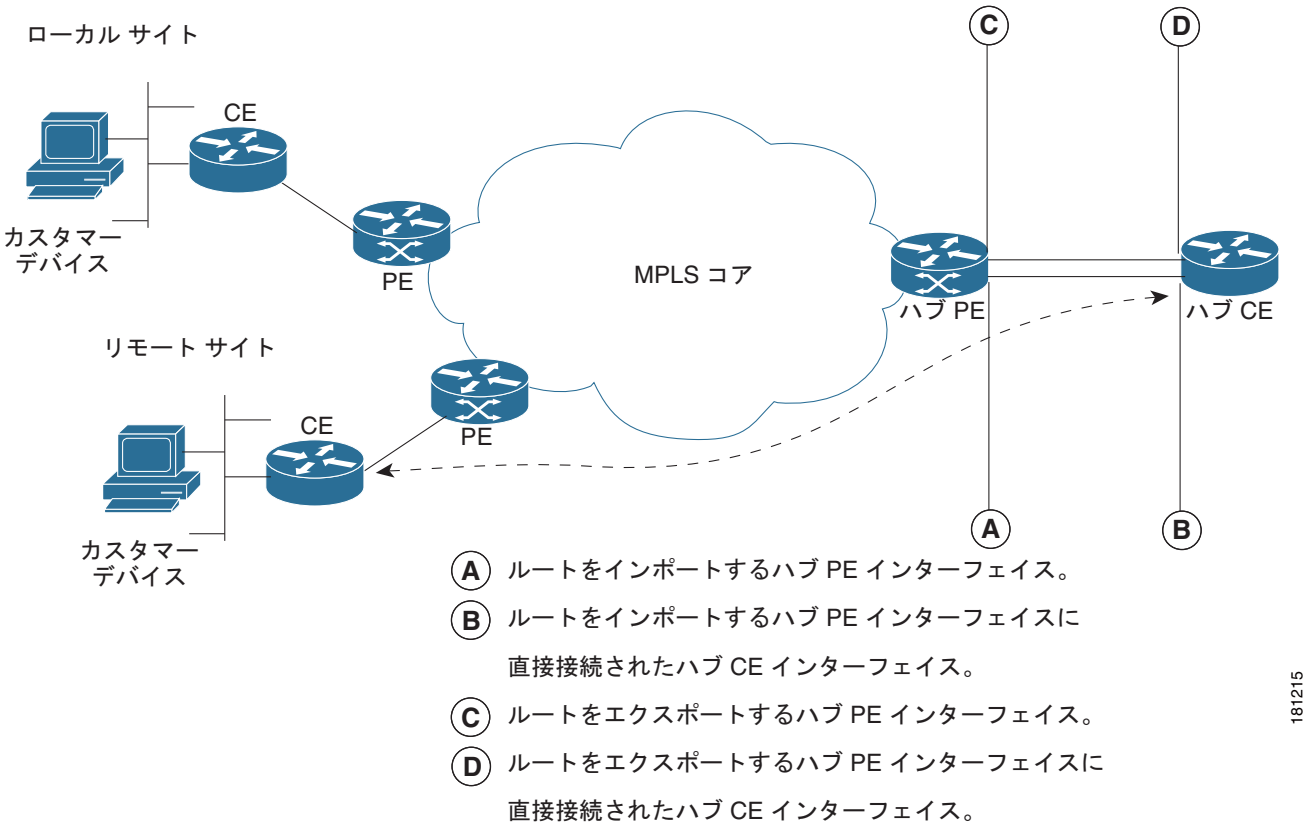
B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

3. リモート サイト（スポーク）と、ルートをインポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-30 の *B*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[Local Site] フィールドに、ルートをインポートするハブ PE および CE インターフェイス（図 11-30 の *A* および *B*）の詳細を設定する必要があります（表 11-14 を参照）。[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Remote Site] フィールドには、リモート カスタマー サイトの詳細を設定する必要があります。

図 11-30　ハブ アンド スポーク VPN トポロジのテスト：ステップ 3



A　ルートをインポートするハブ PE インターフェイス。

B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

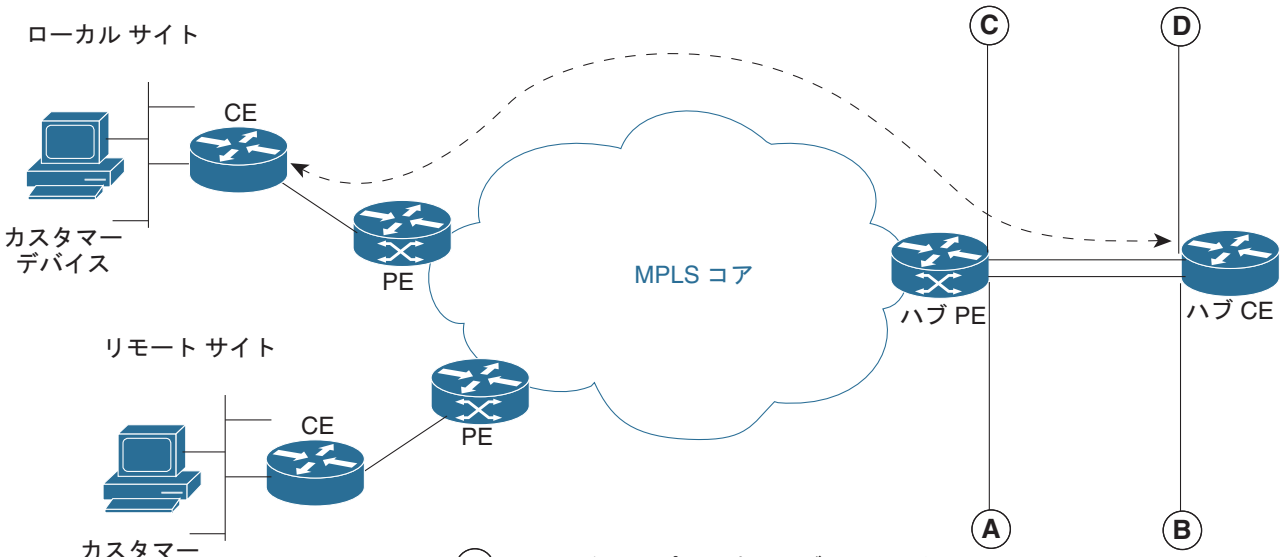
D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

4. ローカル サイト（スポーク）と、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-31 の *D*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Local Site] フィールドに、ローカル カスタマー サイトの詳細を設定する必要があります。[Remote Site] フィールドには、ルートをエクスポートするハブ PE および CE インターフェイス（図 11-31 の *C* および *D*）の詳細を設定する必要があります（表 11-15 を参照）。

表 11-15　テストの設定：ルート エクスポート ハブ インターフェイスのテスト

フィールド名	ハブの詳細
PE Device Name	ハブ PE デバイス名
PE Access Circuit Interface	ルートをエクスポートするハブ PE インターフェイス。
CE Access Circuit Interface IP Address	ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイスの IP アドレス。
Customer Device IP Address	ブランクのままにします。

図 11-31　ハブ アンド スポーク VPN トポロジのテスト：ステップ 4



A　ルートをインポートするハブ PE インターフェイス。

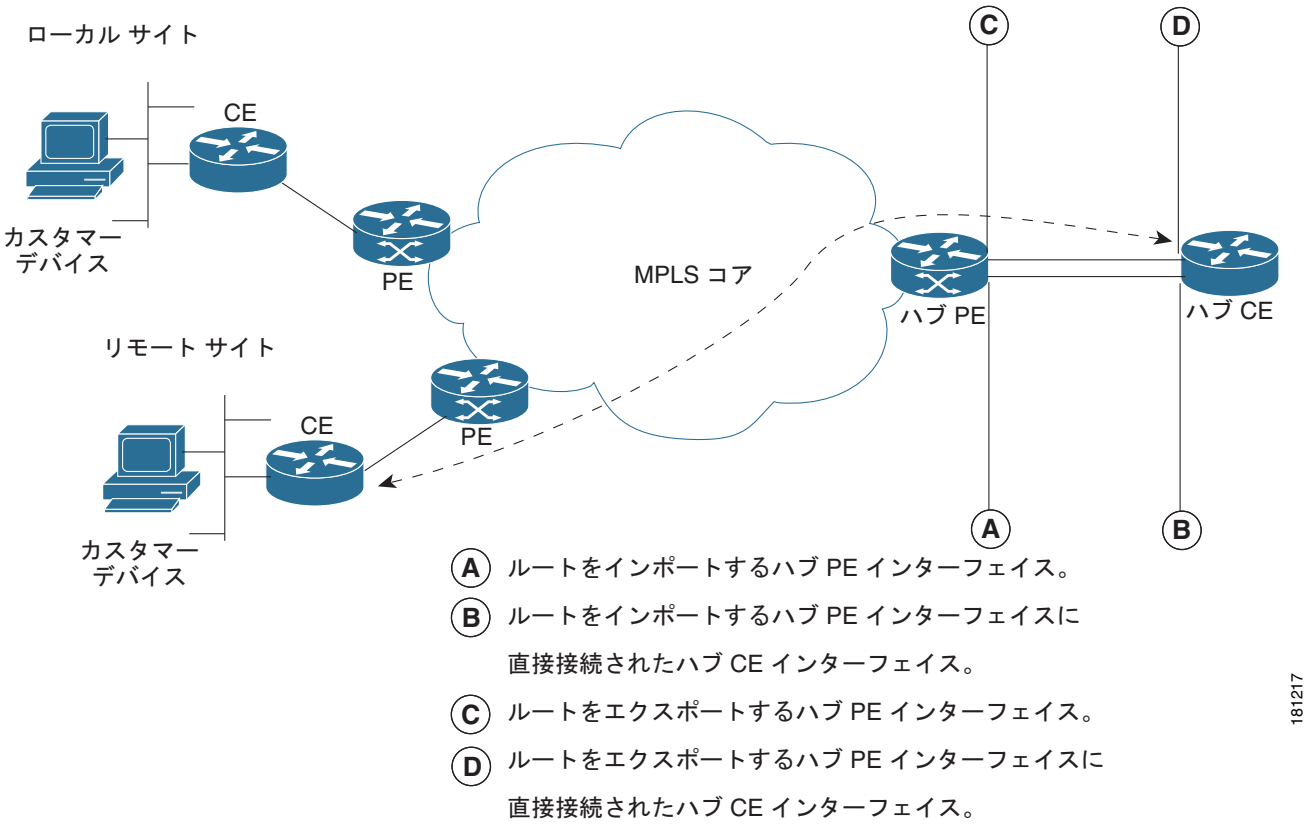
B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

C　ルートをエクスポートするハブ PE インターフェイス。

D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

5. リモート サイト（スポーク）と、ルートをエクスポートするハブ PE インターフェイスに接続されたハブ CE インターフェイス（図 11-32 の *D*）間の MPLS VPN 接続性検証テストを実行します。MPLS VPN 接続性検証テストを設定する際は、[Local Site] フィールドに、ルートをエクスポートするハブ PE および CE インターフェイス（図 11-32 の *C* および *D*）の詳細を設定する必要があります（表 11-15 を参照）。[MPLS VPN Connectivity Verification Configuration] ウィンドウの [Remote Site] フィールドには、リモート カスタマー サイトの詳細を設定する必要があります。

図 11-32　ハブ アンド スポーク VPN トポロジのテスト：ステップ 5



A　ルートをインポートするハブ PE インターフェイス。
B　ルートをインポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。
C　ルートをエクスポートするハブ PE インターフェイス。
D　ルートをエクスポートするハブ PE インターフェイスに直接接続されたハブ CE インターフェイス。

Intranet/Extranet VPN トポロジでのテスト

Intranet/Extranet VPN トポロジを介して接続しているサイト間では、フル メッシュ VPN トポロジの場合と同様に、直接通信が可能です。Intranet/Extranet VPN で接続された 2 サイト間の MPLS VPN 接続性検証テストを設定する際は、通常どおりにテストを設定する必要があります。

Intranet/Extranet VPN で接続されたサイト間の接続性をテストすると、Diagnostics はアクセス回線、VPN エッジ、および MPLS コアの問題を含む MPLS VPN 接続性の問題をトラブルシューティングします。Diagnostics は、不足しているルート マップまたは誤設定されたルート マップなど、Intranet/Extranet VPN に固有の問題のトラブルシューティングは行いません。

MPLS VPN 接続性検証テストによって接続性障害が検出されたが、その障害の原因はアクセス回線、VPN エッジ、および MPLS コアの問題を含む MPLS VPN 接続性の問題にあると考えられない場合は、イントラネット/エクストラネット構成のトラブルシューティングが [Test Results] ウィンドウで推奨されます。

（注）　いずれかの PE でルート マップが設定されていることを見つけると、Diagnostics は、Intranet/Extranet VPN トポロジであると見なします。

セントラル サービス VPN トポロジでのテスト

セントラル サービス VPN トポロジでは、クライアント サイトは 1 つ以上のセントラル サイトと直接通信できますが、クライアント サイト同士では通信できません。セントラル サービス VPN トポロジを介して接続しているクライアント サイトと中央サイト間では、MPLS VPN 接続性検証テストは実行できません。クライアント サイトはローカル サイト、中央サイトはリモート サイトとして入力することで、通常どおりにテストを設定する必要があります。

セントラル サービス VPN の 2 クライアント サイト間の MPLS VPN 接続性検証テストを実行することはできません。

障害シナリオ

この章では、Diagnostics アプリケーションで報告されるすべての障害シナリオの詳細について説明します。また、IOS XR サポート警告についても説明します。

詳細については、mpls-diagnostics-expert@cisco.com まで電子メールでお問い合わせください。

（注）　Diagnostics は、サブインターフェイス/インターフェイスに実装された L3 サービスのみをサポートします。

障害シナリオ

この項では、Diagnostics によって報告される次の障害シナリオについて説明します。

- 「アクセス回線」（P.11-59）
- 「MPLS エッジ」（P.11-71）
- 「MPLS コア」（P.11-77）
- 「カスタマー サイト」（P.11-86）

各障害シナリオの表に、その障害シナリオが 5 つの Diagnostics テスト タイプそれぞれでサポートされているかどうかを示します。この表では、障害シナリオが IOS および IOS XR でサポートされているかどうかを示します。また、障害シナリオが IPv4 および IPv6 向けにサポートされるかどうかも示します。

（注）　この表で、NA は該当なし、NS はサポート適用外を意味します。

アクセス回線

IP 接続をブロックするアクセス回線

プロバイダー（PE）ルータのアクセス回線インターフェイスから送信先への IP 接続を阻止するブロッキング アクセス リストがあります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

無効な PE インターフェイスが指定されている

PE ルータ上にインターフェイスが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ATM インターフェイスに VPI/VCI がない

PE ルータ上の非同期転送モード（ATM）アクセス回線インターフェイスに Virtual Path Identifier（VPI; 仮想パス識別子）または Virtual Channel Identifier（VCI; 仮想チャネル識別子）が割り当てられていないか、VPI/VCI が宛先 IP アドレスにマッピングされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM インターフェイスのプロトコルがダウン

PE ルータで ATM アクセス回線インターフェイスのプロトコルがダウンしています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM サブインターフェイスのプロトコルがダウン

PE ルータで ATM アクセス回線サブインターフェイスのプロトコルがダウンしています。この障害は、間違ったサブインターフェイス パラメータか、あるいは障害を検出して自動的にインターフェイスをダウンさせる ATM Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能が原因で発生することがあります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

CE アクセス回線インターフェイス IP アドレスの計算は、PE インターフェイスがアンナンバード インターフェイスではなく、PE に /30 サブネット マスク インターフェイスがある場合のみ可能

PE 用のカスタマー エッジ（CE）アクセス回線インターフェイス IP アドレスを計算できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

ピアの eBGP 最大プレフィックスを超過

PE と CE 間で exterior Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）が動作していますが、ボーダー ゲートウェイ プロトコル（BGP）ネイバーが確立されていません。ピアが設定されたプレフィックス最大数を超えました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、ルートが存在しない

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。BGP ネイバーは PE とは異なるサブネット上にあり、VPN Routing/Forwarding（VRF; VPN ルーティング/転送）内にネイバーへのルートがありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、設定ミスの可能性

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。VRF 内に BGP ネイバーへのルートがあり、ping を介して BGP ネイバーに到達可能です。CE または PE BGP コンフィギュレーションに問題があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

eBGP ネイバーが確立されていない、ルートは存在する

PE と CE 間で eBGP が動作していますが、PE で BGP ネイバーが確立されていません。BGP ネイバーは PE とは異なるサブネット上にあり、VRF 内にネイバーへのルートが存在します。ただし、ping を介してこの BGP ネイバーに到達できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

複数の eBGP サイトが同じ AS 番号を使用している

ローカル サイトとリモート サイトが eBGP を使用し、同一の AS 番号を使用しており、ローカル PE ルータの VRF 内で BGP ネイバーに「allowas-in」も「as-override」も設定されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes

EIGRP がルートを交換していない

PE と CE 間で Enhanced Interior Gateway Routing Protocol（EIGRP）が動作しており、ピア関係が確立されています。ただし、CE の EIGRP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

イーサネット インターフェイス プロトコルのダウン

PE ルータ プロトコルのイーサネット アクセス回線インターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

イーサネット サブインターフェイス プロトコルのダウン

PE ルータ プロトコルのイーサネット アクセス回線サブインターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

フレーム リレー インターフェイスに DLCI がない

PE ルータのフレーム リレー アクセス回線インターフェイスに Data-Dink Connection Identifier（DLCI; データリンク接続識別子）が割り当てられていないか、DLCI が宛先 IP アドレスにマッピングされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイス プロトコルのダウン

PE ルータ プロトコルのフレーム リレー アクセス回線インターフェイスがダウンしています。原因として、回線パラメータまたはケーブル配線のミスが考えられます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイスに DLCI がない

PE ルータ上のアクセス回線インターフェイスのマルチポイント フレーム リレー相手先固定接続（PVC）に、宛先 IP アドレスにマッピングされた DLCI がありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー インターフェイスに DLCI がない

PE ルータのアクセス回線インターフェイスで、ポイントツーポイント フレーム リレー PVC に DLCI が割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

フレーム リレー PVC が削除済みとしてマークされている

PE ルータのアクセス回線インターフェイスで、フレーム リレー PVC が削除済みとしてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

フレーム リレー PVC が停止中としてマークされている

PE ルータのアクセス回線インターフェイスで、マルチポイント フレーム リレー PVC が停止中としてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

フレーム リレー PVC が停止中としてマークされている

PE ルータのアクセス回線インターフェイスで、ポイントツーポイント フレーム リレー PVC が停止中としてマークされています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

シリアル インターフェイスの搬送波が不完全

PE ルータのシリアル アクセス回線インターフェイスに不完全な搬送波があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

インターフェイスが管理上のダウン状態

PE ルータのアクセス回線インターフェイス（またはサブインターフェイス）が管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

インターフェイスが管理上のダウン状態

PE ルータのアクセス回線サブインターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

プロトコルのインターフェイスがダウン状態

PE ルータ プロトコルのアクセス回線インターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

PE のインターフェイスはバンドル リンクの仮想アクセス インターフェイスである

この PE のインターフェイスは、有効なアクセス回線インターフェイスではありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

インターフェイスが運用停止状態

PE ルータのアクセス回線インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

（ATM ネクスト ホップとの）断続的 ATM 障害

ATM アクセス回線は、ATM ネクスト ホップに断続的に ATM 接続しています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

（送信先との）断続的 ATM 障害

ATM アクセス回線は、送信先に断続的に ATM 接続しています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

無効なアクセス回線 IP アドレス コンフィギュレーション

CE ルータのアクセス回線インターフェイス IP アドレスが、接続先 PE のアクセス回線インターフェイス IP アドレスと同じサブネット内にありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

無効なアクセス回線 IP アドレス コンフィギュレーション

この CE のアクセス回線インターフェイス IP アドレスがネットワーク アドレスです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

無効なアクセス回線 IP アドレス コンフィギュレーション

この CE のアクセス回線インターフェイス IP アドレスがネットワーク ブロードキャスト アドレスです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

詳細については、「IPv6 サポート」（P.11-87）を参照してください。

無効なアクセス回線 IP アドレス コンフィギュレーション

CE のアクセス回線インターフェイス IP アドレスと、接続先 PE のアクセス回線インターフェイス IP アドレスが同じです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IP 接続の問題

IP 接続に関する未知の問題。PE インターフェイスから CE への VRF インスタンスで、アクセス回線の接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	Yes	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes

ルートの欠落

PE ルータのアクセス回線インターフェイスから送信先へのルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

ルートの欠落

PE ルータのアクセス回線インターフェイスからカスタマーの送信先へのルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

EIGRP ピア関係が確立されていない

PE と CE 間でルーティング プロトコル EIGRP は動作していますが、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

EIGRP ピア関係が確立されていない

PE と CE 間では、ルーティング プロトコル EIGRP が動作しています。PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していません。PE と CE が異なるサブネット上にあるため、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル EIGRP が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	該当なし	Yes	Yes	NS

OSPF ピアがない

PE と CE 間で Open Shortest Path First（OSPF）が動作していますが、PE にピアが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ピア インターフェイスの OSPF がイネーブルでない

ルータ上のインターフェイスで OPSF がイネーブルになっていません。両方のネイバー インターフェイスで OSPF をイネーブルにしておく必要があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

ピア インターフェイスの OSPF がパッシブ モード

ルータ上のインターフェイスで OSPF がパッシブ モードになっています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF エリアの不一致

ネイバー インターフェイス上で OSPF がイネーブルになっていますが、これらのインターフェイスは異なるエリア内に設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF エリア タイプの不一致

ネイバー インターフェイス上で OSPF がイネーブルになっていますが、これらのインターフェイスは異なるエリア タイプに設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

PE と CE 間で動作するルーティング プロトコルが確定しておらず、スタティック ルートが存在しない

VRF 内のアクセス回線に問題があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

OSPF がルートを交換していない

PE と CE 間で OSPF が動作していますが、ピア関係が確立されています。ただし、CE の OSPF からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

OSPF ピアが確立されていない

PE と CE 間で OSPF が動作していますが、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	該当なし

OSPF 時間の不一致

ネイバー インターフェイス上で OSPF はイネーブルになっていますが、これらのインターフェイスの [hello|dead] タイマーにはそれぞれ異なる値が設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF ピアが確立されていない

PE と CE 間では OSPF が動作しています。ただし、PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していないため、ピア関係が確立されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル OSPF が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	NS	Yes	Yes	NS

PE に CE へのルートがない

接続されている PE および CE インターフェイスは、異なるサブネット上にあります。PE と CE 間で動作するルーティング プロトコルが確定しておらず、CE へのスタティック ルートが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	NS

RIB 障害

PE から VRF 内の宛先へのルートが VRF ルーティング テーブルに設定されていません。これは Routing Information Base（RIB; ルーティング情報ベース）障害と見なされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

RIP の設定ミス

PE と CE 間で Routing Information Protocol（RIP）が動作していますが、CE の RIP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

RIP がルートを交換していない

PE と CE 間で RIP が動作していますが、PE および CE インターフェイスは異なるサブネット上にあり、IP アンナンバードを使用していないため、CE の RIP からルートを受信していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ルート再配布でルート ポリシーが指定されていない

PE と CE 間でルーティング プロトコル RIP が動作し、MP-BGP にルートが再配布されています。ただし、発信ルート ポリシーが指定されていないため、すべてのルートはアドバタイズされずにドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	該当なし	Yes	Yes	NS

ループバック モードのシリアル インターフェイス

PE ルータのシリアル アクセス回線インターフェイスがループバック モードに設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

シリアル インターフェイスが運用停止状態

PE ルータのシリアル アクセス回線インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

ATM ポイントツーポイント インターフェイスのスタティック IP アドレス

ATM アクセス回線の ATM ポイントツーポイント サブインターフェイスに、スタティック IP アドレス マッピングが指定されています。ポイントツーポイント サブインターフェイスでは、トラフィックに対する VC とパスはそれぞれ 1 つだけなので、スタティック マッピングもアドレス解決プロトコル（ARP）も必要ありません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

プロトコルのサブインターフェイスがダウン状態

PE ルータ プロトコルのアクセス回線サブインターフェイスがダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

未診断の ATM 障害（ATM ping は失敗したが、ATM セグメントの ping は成功）

ATM アクセス回線の接続が中断されています。エンドツーエンド ATM ping は失敗しましたが、ATM セグメントの ping は成功しました。原因として、ATM 回線パラメータの間違い、ATM ルーティングの設定ミス、CE または ATM クラウド インターフェイスのダウン、デバイスの停止など、さまざまな問題が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

未診断の ATM 障害（エンドツーエンドおよびセグメント ATM ping が失敗）

ATM アクセス回線の接続が中断されています。エンドツーエンド ping とセグメント ATM ping がどちらも失敗しました。原因として、ATM 回線パラメータの間違い、ATM ネクスト ホップでの ATM ルーティングの設定ミス、ネクスト ホップ インターフェイスのダウン、デバイスの停止など、さまざまな問題が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

PE アクセス回線インターフェイスに仮想テンプレート インターフェイスが指定されている

この PE の PE インターフェイスは、有効なアクセス回線インターフェイスではありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	該当なし	Yes	NS

MPLS エッジ

BGP ネクスト ホップ インターフェイスが管理上のダウン状態

PE の BGP ネクスト ホップがループバック インターフェイスに割り当てられています。ただし、このインターフェイスは管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP ネクスト ホップがインターフェイスに割り当てられていない

リモート サイト PE へのルートの BGP ネクスト ホップが、リモート PE のインターフェイスに割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP が非アクティブ

PE ルータで BGP がアクティブになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

複数の BGP ピアが同じ BGP ネクスト ホップを使用している

複数の BGP VPNv4/VPNv6 ピアが同一の BGP ネクスト ホップを使用しています。このため、PE ルートの正しいルート配布ができません。これ以外のルーティング問題も発生する可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

複数の BGP ピアが同じ Router Identifier（RID; ルータ ID）を使用している

複数の BGP VPNv4/VPNv6 ピアが同一のルータ ID を使用しています。このため、PE ルートの正しいルート配布ができません。これ以外のルーティング問題も発生する可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

同じサブネット内に複数のアクセス回線がある

LSP 接続およびコントロール プレーンに関する問題。リモート PE ルータに対して現在選択されている BGP ルートのネクスト ホップが、ローカル PE ルータのインターフェイスに割り当てられていません。ローカル PE ルータの VRF に、リモート プレフィックスへの VPNv4/VPNv6 ルートが複数存在します。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes

BGP と LFIB の不一致

BGP テーブルとラベル転送情報ベース（LFIB）テーブルのタグなしエントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP と LFIB の不一致

Forwarding Information Base（FIB; 転送情報ベース）と BGP のエントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP ネクスト ホップの重複

ネットワーク内で、PE の BGP ネクスト ホップの IP アドレスが重複しています。

CE から CE	PE から接続先 CE	CEからコア上のPE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

IP アドレスの重複

PE ルータに、アクセス回線インターフェイスと重複する IP アドレスが設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IP アドレスの重複

ネットワーク内で、PE の BGP ルータ ID の IP アドレスが重複しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

eBGP が MP-BGP に接続ルートを再配布していない

PE と CE 間でルーティング プロトコル eBGP が動作していますが、PE の eBGP は接続ルートを Multi Protocol（MP; マルチ プロトコル）-BGP に再配布しておらず、明示的なネットワーク文もありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

FIB と LFIB の不一致

FIB テーブルと LFIB テーブルの集約エントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

入力 FIB と出力 LFIB の不一致

入力 FIB と出力 LFIB が一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

BGP エントリの不一致

VRF の BGP エントリが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ラベルの不一致、または異なる VPN にあるインターフェイスがダウン

VRF で、PE から送信先への VPN 接続に問題が生じています。プレフィックスの BGP VPNv4/VPNv6 ラベルが一致しません。これは、ラベルの不一致、またはインターフェイスが異なる VPN にあることを示している可能性があります。選択されたインターフェイスが同じ VRF にあることを確認してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	Yes	該当なし	Yes	Yes	Yes	Yes

PE インターフェイスが管理上のダウン状態

PE ルータのアクセス回線インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	NS

Router Identifier（RID; ルータ ID）の欠落

PE のローカル ルータ ID を特定できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes	Yes

VPNv4 アドレス ファミリ コンフィギュレーションの欠落

VPNv4 コンフィギュレーションが欠落しています。バーチャル プライベート ネットワーク（VPN）ラベルの交換に問題があります。PE ルータの BGP ルータ コンフィギュレーションで、VPNv4 アドレス ファミリ コンフィギュレーションが欠落しています。このためルートはドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

VPNv6 アドレス ファミリ コンフィギュレーションの欠落

VPNv6 コンフィギュレーションが欠落しています。バーチャル プライベート ネットワーク（VPN）ラベルの交換に問題があります。PE ルータの BGP ルータ コンフィギュレーションで、VPNv6 アドレス ファミリ コンフィギュレーションが欠落しています。このためルートはドロップされます。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes

IOS XR ルータで MPLS LDP パッケージがイネーブルでない

IOS XR ルータで MPLS LDP パッケージがイネーブルになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

IOS XR ルータに MPLS パッケージがインストールされているがアクティブでない

IOS XR ルータに MPLS パッケージがインストールされていますが、アクティブになっていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

IOS XR ルータに MPLS パッケージがインストールされていない

IOS XR ルータに MPLS パッケージがインストールされていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

MP-BGP ネイバーがない

PE ルータで MP-BGP ネイバーが定義されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

MP-BGP ネイバー セッションが確立されていない

PE ルータで MP-BGP ネイバー セッションが確立されていません。

CE から CE	PE から接続先 CE	CEからコア上のPE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

プレフィックスの VPN ラベルがない

プレフィックスに VPN ラベルが割り当てられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

PE インターフェイスに VRF が関連付けられていない

PE ルータのインターフェイスに VRF が関連付けられていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

OSPF ループバック インターフェイスが /32 以外のネットマスクを使用している

PE によって VPNv4 ルートが IBGP ネイバーにアドバタイズされています。ネクスト ホップのアドレスは、/32 マスクが定義されていないループバック インターフェイスです。OSPF はこのループバック インターフェイス上で使用されており、このインターフェイスの OSPF ネットワーク タイプはループバックです。マスクの設定に関係なく、OSPF はこの IP アドレスをホスト ルートとして（マスク /32 を使用して）アドバタイズします。このアドバタイジングは、設定済みマスクを使用する TDP/LDP と

競合します。したがって、TDP/LDP ネイバーは、このルータによってアドバタイズされるルートのラベルを受信できない場合があります。このため、同じ VPN に属するサイト間の接続が中断される可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	該当なし

PE インターフェイスに IP アドレスがない

PE ルータのインターフェイスに IP アドレスがありません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ルータ ID ループバック インターフェイスのダウン

PE のローカル ルータ ID の関連付けに使用するループバック インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

MP-BGP との間でルートが再配布されていない

PE の MP-BGP との間でルートが再配布されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	該当なし	Yes	該当なし

リモート プレフィックスへのスタティック ルート

PE の VRF 内で、リモート プレフィックスへのスタティック ルートが設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

トラフィックの管理上のブロック

トラフィックが管理上の理由でブロックされているため、PE から送信先への VPN 接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

レイヤ 3 VPN のトラブルシューティングで障害の原因を特定できない

LSP 接続の問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

レイヤ 3 VPN のトラブルシューティングで障害の原因を特定できない

VRF で、PE から送信先への VPN 接続に問題が生じています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

VRF ルート ターゲット インポート/エクスポートの不一致

PE デバイス間で VRF ルート ターゲット インポート/エクスポートが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

MPLS コア

無効な PE インターフェイスが指定されている

LSP エンドポイントとして指定されたインターフェイスは、PE ルータ上に存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
該当なし	該当なし	該当なし	該当なし	Yes	Yes	Yes	Yes	該当なし

LDP ネイバー セッションの中断

ダウンストリーム ネイバーとの LDP セッションが中断されました。ルータのルート プロセッサ/ラインカード転送に不一致があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

ルータの CEF がイネーブルでない

ルータ上で CEF がイネーブルになっていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

配布された LFIB テーブルの不一致

ルート プロセッサとラインカードの LFIB テーブルが一致しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

配布された FIB テーブルの不一致

ルート プロセッサとラインカードの FIB テーブルが一致しません。

CE から CE	PEから接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	該当なし	Yes	Yes	Yes	Yes

ラベルの不一致

ルータ上で、LFIB ローカル タグ、受信パケット、および LDP ローカル バインディング ラベルに不一致があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ホストが到達不能

ラベル スイッチ ルータ（LSR）からホストに到達できません。原因として、ダウンストリーム ルータとの LDP セッションがルータ上で確立されていない、IGP の問題によって LDP ID に到達できない、LDP パケットをブロックする ACL が設定されている、認証上の問題などが考えられます。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP ラベルの不一致

プレフィックス用に受信したラベルと送信したラベルが一致しません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ネイバーが見つからない

LDP ネイバーが検出されませんでした。これは、ダウンストリーム ネイバーとデバイスとのインターフェイスでよく見られる LDP 検出問題です。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LDP ネイバーが見つからない

LDP ネイバーが検出されませんでした。ルータのインターフェイスに ACL が設定されているため、LDP ネイバーを検出できない場合があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP ネイバーが確立されていない

LSP 接続およびコントロール プレーンに関する問題。LDP セッションが確立されていません。インターフェイスに ACL が設定されているため、ポート 646 で LDP セッションを確立できない場合があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP/TDP の不一致

リンクの一方の終端では LDP、もう一方の終端では TDP がイネーブルになっています。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LSP 応答パスの問題

LSP 接続の応答パスに問題があります。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

LFIB エントリの欠落

LFIB エントリがありません。原因として、以前のルータでのルーティング ミス、またはループバックの重複が考えられます。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

リターン パスの欠落、またはタグのないリターン パス

コア ルータからのリターン パスがないか、リターン パスにプレフィックスのタグが付いていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

MPLS ラベル スペースの枯渇

ルータの MPLS ラベル スペースがなくなりました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

MPLS がグローバルにイネーブル化されていない

MPLS がルータ上でグローバルにイネーブル化されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

インターフェイスの MPLS がイネーブルでない

MPLS がインターフェイス上でイネーブルになっていません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベルのエントリがない

送信先プレフィックスへの着信ラベルの LFIB にエントリがありません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

ネイバーとの LDP セッションがない

ルータに上ネイバーとの LDP セッションが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

有効なネクスト ホップ エントリがない

現在のデバイスで、ネクスト ホップの有効なエントリが見つかりません。「IOS XR サポート」（P.11-86）を参照してください。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	Yes

転送パスのルーティング ループ

転送パスにルーティング ループがあります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

コアに接続するすべての MPLS 対応インターフェイスがダウン

LSP 接続およびコントロール プレーンに関する問題。MPLS 対応インターフェイスが動作していません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベル アドバタイジングがイネーブルでない

ルータ上でラベル アドバタイジングがディセーブルになっています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

ラベル アドバタイジングが ACL によって拒否される

ラベル アドバタイジングはグローバルにディセーブル化されていますが、一部は 1 つまたは複数のアクセス リストに対してイネーブルになっています。送信先プレフィックスへのラベルのアドバタイジングを ACL が拒否している可能性があります。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TTL の伝播がディセーブル

デバイスが存続可能時間（TTL）を伝播していないため、障害箇所のトラブルシューティングまたは検出ができません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

トンネル トラフィック アドミッション ポリシーを確認

TE トンネルに（autoroute announce を介して、あるいは Policy Based Tunnel Selection（PBTS; ポリシー ベースのトンネル選択）またはスタティック ルートなどの）トラフィック アドミッション ポリシーが設定されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

トンネル インターフェイスで MPLS がイネーブルかどうかを確認

MPLS TE トンネル インターフェイスで不完全なコンフィギュレーションが検出されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

プライマリおよびバックアップ トンネルのインターフェイスが動作していることを確認

ルータのトンネル インターフェイスが管理上の理由でダウンしています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ヘッドエンドにトンネル コンフィギュレーションがない

ヘッドエンド ルータに TE トンネル コンフィギュレーションが存在しません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルの発信インターフェイスが動作していることを確認

ルータに設定された FRR プライマリ トンネルの発信インターフェイスが動作を停止しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ルータの TE がグローバルにイネーブル化されていない

MPLS トラフィック エンジニアリングが、ルータ上でグローバルにイネーブル化されていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

インターフェイスの TE がグローバルにイネーブル化されていない

MPLS トラフィック エンジニアリングが、ルータのインターフェイスでイネーブルになっていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

IP アドレスがトンネルに割り当てられていない

MPLS トラフィック エンジニアリング トンネルに IP アドレスが割り当てられていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルの宛先が無効

トンネルに設定されている宛先アドレスは到達不能です。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネルが管理上のシャットダウン状態

管理上の理由により、ルータのトンネルがシャットダウンされました。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE の OSPF コンフィギュレーションの欠落

MPLS TE の OSPF がルータに設定されていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ノードが MPLS TE リンクをアドバタイズしていない

ルータは、自身を MPLS TE リンクとして OSPF 経由でアドバタイズしていません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

ターゲット LDP セッションがピア PE 間に存在しない

リモート サイト PE ルータが、ターゲット LDP セッション要求を受け付けません。

CE から CE	PE から接続先 CE	CEからコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

ブロッキング ACL を原因とするターゲット LDP セッションのセットアップ問題

ルータは、（TCP ポート 646 で）LDP メッセージをブロックするアクセス コントロール リストを保持しています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

PE 間でターゲット LDP が確立されていない、または動作していない

ピア PE ルータが到達不能なため、LDP はデバイス間でターゲット セッションを確立できませんでした。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

トンネル接続の障害、ターゲット LDP コンフィギュレーションがない

ネイバー デバイスに対する LDP 検出が失敗しました。トンネル テール エンド デバイスが、LDP ターゲット hello を受け付けません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

リンク保護のため、保護されたインターフェイスをバックアップ トンネルが通過しないよう確認

ルータに FRR バックアップ トンネルが設定されています。FRR バックアップ トンネルは、プライマリ トンネルが通過するパス上にあるルータ（NHOP）でリンクを保護するように設定されています。しかし、設定済みバックアップ トンネルは、このリンクを経由するように設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

プライマリ トンネルで「fast-reroute」を使用して FRR がイネーブルになっていることを確認

ルータ上でトンネルが検出されました。このトンネルはプライマリ トンネルとして使用されますが、必要とされる fast-reroute の設定が行われていないようです。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

ノードの保護：バックアップ トンネル パスが明示的かどうかと、保護されたノード インターフェイスがパスに含まれていないかどうかを確認

FRR バックアップ トンネルがルータに設定されています。FRR バックアップ トンネルは、プライマリ トンネルが通過するパス上にあるルータ（NNHOP）を保護するように設定されています。しかし、設定済みバックアップ トンネルは、このルータ上のリンクを経由するように設定されています。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

プライマリおよびバックアップ トンネルのマージ ポイントが到達可能かどうかを確認

FRR プライマリ トンネルと FRR バックアップ トンネルのマージ ポイント ルータが到達不能です。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE ping の失敗

ping mpls traffic-eng tunnel コマンドで failure が返されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

トンネルが運用停止状態

show mpls traffic-eng tunnels コマンドで、TE トンネルがダウンしていることが示されました。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	該当なし	Yes	NS	Yes	Yes	Yes

トンネル接続の障害

MPLS TE 接続に関する未知の問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	該当なし	Yes	Yes	Yes

MPLS TE 接続の問題をトラブルシューティングできない

このルータは OAM Cisco IOS 以外のバージョンを実行しています。トンネルの接続をテストできません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

未知の LSP 接続問題

LSP 接続、データ プレーン、または未知の原因による問題。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	Yes	Yes	Yes

サポートされていない IOS バージョン

コア ルータはサポートされていない IOS バージョンを実行しています。この IOS バージョンは、必要な OAM 機能をサポートしていません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	該当なし	Yes	Yes	Yes	Yes	該当なし	Yes	NS

VPN 接続テストが実行され、障害は検出されなかった（ただし CE への ping はブロックされ、VPN 接続の検証は不可）

VRF 内の PE から送信先への VPN 接続を検証できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

カスタマー サイト

カスタマー側のルーティングに問題がある可能性

PE には CE からの複数のルートがありますが、CE が ping に応答できません。

CE から CE	PE から接続先 CE	CE からコア上の PE	PE から PE（VRF 内）	PE から PE コア	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	該当なし	該当なし	Yes	Yes	Yes	Yes

IOS XR サポート

この項では、IOS XR サポート警告について説明します。

1. 「インターフェイスの MPLS がイネーブルでない」（P.11-80）

   IOS XR にはパッケージの概念が取り入れられています。Diagnostics に関係するパッケージの 1 つが MPLS パッケージです。Diagnostics トラブルシューティングでコアの IOS XR ルータを中心に扱う場合、さまざまな準備チェックが行われ、ルータが適切に設定されている、つまり、MPLS パッケージがインストールされてアクティブであることを確認してから、必要な機能（MPLS OAM および MPLS LDP）がイネーブルになっていることを確認します。これらのチェックのいずれかで不合格になると、障害シナリオが報告されます。「インターフェイスの MPLS がイネーブルでない」（P.11-80）は、IOS デバイスに対して、あるいは IOS XR デバイスのインターフェイスで MPLS がディセーブルの場合、引き続き有効です。

2. 「ルータの CEF がイネーブルでない」（P.11-77）

Diagnostics はこれまでどおり、コアの IOS ルータで CEF がディセーブルになっている状況を特定できます。たとえば、CLI コンフィギュレーションによって、あるいはルータが過負荷になって自動的にシャットダウンした場合に CEF がディセーブルになることがあります。その場合、IOS CLI コマンド **show cef state** によって CEF が *enabled/running* または *disabled/not running* のいずれの状態であるかが報告され、Diagnostics は CEF がディセーブルであると判断できます。

IOS XR ルータで CEF をディセーブルにすることはできません。IOS XR ルータの CEF スイッチング機能が過負荷になっても、ルータはシャットダウンしません。代わりに、CEF スイッチング プロセスの負荷を減らす目的で、未処理要求のキューにバック プレッシャーを適用します。このため、IOS XR ルータでは関連する CLI **show** コマンドで CEF の運用停止状態は報告されません。したがって、この障害シナリオは IOS XR ルータでは有効ではありません。

3. 「LDP/TDP の不一致」（P.11-79）

   直接接続された IOS XR ルータが存在する場合、これは有効なシナリオではありません。なぜなら、IOS XR は Label Distribution Protocol（LDP; ラベル配布プロトコル）を 1 つしかサポートしないからです。IOS-IOS XR、IOS XR-IOS、または IOS-IOS コンフィギュレーションで設定されたアプリケーションでは、LDP-TDP の不一致が検出される場合があります。

4. 「LDP ネイバー セッションの中断」（P.11-77）

   「ラベルの不一致」（P.11-78）

   「LDP ラベルの不一致」（P.11-78）

   「LDP ネイバーが見つからない」（P.11-78）

   「LSP 応答パスの問題」（P.11-79）

   「LFIB エントリの欠落」（P.11-79）

   「リターン パスの欠落、またはタグのないリターン パス」（P.11-80）

   「ラベルのエントリがない」（P.11-80）

   「有効なネクスト ホップ エントリがない」（P.11-81）

   これらの障害シナリオは、IOS バージョン固有のバグが原因であり、IOS XR には適用されません。

5. 「ATM インターフェイスのプロトコルがダウン」（P.11-60）

   「ATM サブインターフェイスのプロトコルがダウン」（P.11-60）

   「（ATM ネクスト ホップとの）断続的 ATM 障害」（P.11-64）

   「（送信先との）断続的 ATM 障害」（P.11-65）

   「ATM ポイントツーポイント インターフェイスのスタティック IP アドレス」（P.11-70）

   「未診断の ATM 障害（ATM ping は失敗したが、ATM セグメントの ping は成功）」（P.11-70）

   「未診断の ATM 障害（エンドツーエンドおよびセグメント ATM ping が失敗）」（P.11-70）

   CRS-1 プラットフォーム上の ATM インターフェイスの場合、これらの障害はサポートされません。ただし、IOS デバイスと、Cisco 12000 XR シリーズに搭載された IOS XR には適用されます。

IPv6 サポート

この項では、IPv6 サポート警告について説明します。

- IOS および IOS XR デバイス向けの IPv4 トラブルシューティングに加え、PE-CE リンクで IPv6 アドレッシングが使用される IOS XR デバイスにもトラブルシューティングが拡張されています。IPv6 は、IOS デバイスではサポートされません。

- イーサネットは、IOS XR デバイスで IPv6 アドレッシングが使用される場合に Diagnostics がトラブルシューティングに利用できる、唯一のアクセス回線インターフェイス テクノロジーです。
- IPv6 サポートは限定的に拡張され、PE-CE ルーティング プロトコルとして eBGP のみをサポートします。
- IPv6 アドレスの範囲は接続回線リンク間に限られているので、LSP の終端は両側とも IPv6 または IPv4 のいずれかであり、一方が IPv6 で他方が IPv4、あるいはその逆になることはありません。
- IPv6 サポートでは、グローバル ユニキャスト IPv6 アドレスだけを使用する PE-CE リンク コンフィギュレーションをトラブルシューティングできます。
- IPv6 サポートでは、IPv4 ルータ ID は、BGP や LDP などのプロトコル向けにピア ルータを識別するために使用されます。
- IPv4 の場合と異なり、（適用可能なテスト タイプの）CE アクセス回線インターフェイス IP アドレスは自動的に入力されません。これは、IPv6 アンナンバードが IOS XR デバイスでサポートされておらず、IPv6 には /30 および /31 アドレスの概念がないためです。
- 次の障害シナリオは IOS XR には適用されますが、これらの検証は最初のデータ検証で行われるので、IPv6 のコンテキストには適用されません。この障害シナリオは、CE アクセス回線インターフェイス IP アドレスがネットワーク アドレスであることを報告するためのもので、最初のデータ検証で実行されます。IPv6 にブロードキャスト アドレスの概念はありません。
  - ブロードキャスト アドレス
  - ネットワーク アドレス

観察結果

観察結果とは、接続上の問題に発展する可能性のある状況です。Diagnostics は接続問題の原因を 1 つのカテゴリとして判断できないため、これらの状況は観察結果として報告されます。

詳細については、mpls-diagnostics-expert@cisco.com まで電子メールでお問い合わせください。

PE に ACL が設定されている

プロバイダー エッジ（PE）ルータにアクセス コントロール リスト（ACL）が設定されています。ACL は、この PE からリモート PE への VPN Routing/Forwarding instance（VRF; VPN ルーティング/転送インスタンス）ping が失敗する原因となります。ただしシスコでは、ACL の使用状況を確認するための分析は行っていません。ACL が原因で、PE からローカル カスタマー エッジ（CE）ルータまたはカスタマー デバイスへの接続に障害が発生することはありません。

BGP ネイバー セッションの問題

ボーダー ゲートウェイ プロトコル（BGP）ネイバー セッションで問題が検出されました。[BGP Neighbor]（ネイバー IP アドレス）および [BGP State]（BGP ネイバーの状態）カラムがある表が表示されます。

BGP ルータ ID がループバック インターフェイスでない

PE のローカル BGP ルータ ID がループバック インターフェイスに割り当てられていません。重複の可能性を減らすため、および安定性を高めるために、ルータ ID はループバック インターフェイスから取得することを推奨します。

接続ルートが MP-BGP に再配布されていない

直接接続されたルートは、MP-BGP に再配布されない場合があります。

コアのトラブルシューティングを実行できない。VPN ルートが外部ルートである。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*VRF name*> 内のリモート プレフィックス <*IP address*> への有効な VPN ルートを保持していないため、Diagnostics はテスト対象のラベルスイッチド パス（LSP）を特定できません。このルートは、内部のボーダー ゲートウェイ プロトコル（BGP）VPNv4 ネイバーからは特定できません。<*Routing Protocol Name*> から判断できます。この外部ルートのネクスト ホップは <*IP address*> です。トラフィックは、予測どおりに MPLS コアを通過しません。これは意図的なバック ドア リンクの可能性もありますが、多くの場合、PE と CE 間のルーティングミスの症状を示しています。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

コアのトラブルシューティングを実行できない。VPN ルートが外部ルートで、ネクスト ホップにアクセスできない。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*IP address*> 内のリモート プレフィックス <*IP address*> への有効なバーチャル プライベート ネットワーク（VPN）ルートを保持していないため、Diagnostics はテスト対象の LSP を特定できません。このルートは、内部の BGP VPNv4 ネイバーからは特定できません。<*Routing Protocol Name*> から判断できます。この外部ルートのネクスト ホップにはアクセスできません。これは意図的なバック ドア リンクの可能性もありますが、多くの場合、PE と CE 間のルーティングミスの症状を示しています。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

コアのトラブルシューティングを実行できない。VPN ルートのネクスト ホップにアクセスできない。

コアのトラブルシューティングを実行できませんでした。PE <*PE Name*> が VRF <*VRF name*> 内のリモート プレフィックス <*IP address*> への有効な VPN ルートを保持していないため、Diagnostics はテスト対象の LSP を特定できません。ネクスト ホップにアクセスできません。原因として、コアの Interior Gateway Protocol（IGP）または IP 接続の障害が考えられます。LSP 接続をテストするには、PE から PE コアへのテストを実行します。このテストでは、LSP エンドポイントを手動で指定できます。

BGP ルータ ID の重複

リストされているデバイスの 1 つまたは複数のインターフェイス上で、PE の BGP ルータ ID が重複しています。

eBGP 最大プレフィックス

PE と eBGP ネイバー間の exterior Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）セッションの最大プレフィックス数が PE に設定されています。このネイバーからの VRF には、現在 *X* 個のプレフィックスがあります。

eBGP ネイバーが確立されていない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。PE および CE インターフェイスは異なるサブネット上にあり、この PE には CE へのルートがありません。CE へのルートが確定するまで、この eBGP セッションは確立されません。

eBGP ネイバーが確立されていない

eBGP ネイバーは VRF 内で指定されていますが、確立されていないため到達不能です。

EIGRP ピア関係が確立されていない

PE インターフェイスは IP アンナンバードを使用して設定されています。Enhanced Interior Gateway Routing Protocol（EIGRP）でピア関係が確立されるには、CE インターフェイスも IP アンナンバードを使用するか、PE インターフェイスと同じサブネット上に存在する必要があります。

フルメッシュ VPN トポロジ

これらのルータは、フルメッシュ VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

ハブ アンド スポーク VPN トポロジ

これらのルータは、ハブ アンド スポーク VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

ハブ間およびハブ アンド スポーク VPN トポロジ

これらのルータは、ハブ間およびハブ アンド スポーク VPN コンフィギュレーションを使用して接続されているようです。これが正しくない場合、ルート ターゲット コンフィギュレーションに問題が生じます。

不完全な CEF 隣接

アクセス回線インターフェイス上の Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）隣接が不完全です。

不正なマルチリンク仮想アクセス インターフェイスが指定されている

PE にマルチリンク仮想アクセス回線インターフェイスを指定する場合は、指定する仮想アクセス インターフェイスがアクティブなマルチリンク バンドル インターフェイスであり、アクティブなバンドル リンクを保持していることを確認してください。

VLAN にインターフェイスがない

警告：イーサネット アクセス回線インターフェイスに仮想 LAN（VLAN）が関連付けられていません。

断続的な ping の成功

ping で断続的な接続のみが表示されました。

FR インターフェイスでインバース ARP がディセーブル

フレーム リレー インターフェイスは動的に設定されていますが、インバース アドレス解決プロトコル（ARP）が明示的にディセーブルになっています。

FR インターフェイスでインバース ARP が暗黙的にディセーブル

インターフェイス上にフレーム リレー スタティック マップがあります。このインターフェイスは動的に設定されますが、スタティック マップが存在するため、その副作用としてインバース ARP がディセーブルになります。

フレーム リレー インターフェイス上で LMI がディセーブル

警告：ローカル管理インターフェイス（LMI）がディセーブルになっているため、フレームリレー相手先固定接続（PVC）のステータスを確認できません。

LSP エンドポイントがループバック インターフェイスでない

VPNv4 ルートが IBGP ネイバーに送信されています。ただしネクスト ホップ アドレスは、直接接続された物理インターフェイスのうちの 1 つです。VPNv4 IBGP ネイバーのネクスト ホップにはループバック インターフェイスを使用することを推奨します。IGP 経由の正しいホップでこのアドレスを使用できない場合は、転送ラベル情報を入手できないので、VPN サイト間の接続は中断されます。

IOS XR ルータで MPLS OAM パッケージがイネーブルでない

IOS XR ルータで MPLS OAM パッケージがイネーブルになっていません。

IOS XR ルータで MPLS TE パッケージがイネーブルでない

IOS XR ルータで MPLS TE パッケージがイネーブルになっていません。

複数の等コスト パス

Equal Cost Multiple Path（ECMP; 等コスト マルチ パス）が検出されました。

PE ルータの IOS バージョンが不適合

プロバイダー エッジ（PE）ルータが MPLS OAM に適合しない Cisco IOS バージョンを実行しているため、コアのトラブルシューティングを実行できませんでした。

eBGP からルートを受信していない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。ただし、ネイバーからはルートを受信していません。

eBGP からリモート プレフィックスへのルートを受信していない

PE と CE 間のルーティング プロトコルとして eBGP が実行されているようです。ただし、ネイバーからはリモート プレフィックスへのルートを受信していません。PE とカスタマー エッジ（CE）の BGP コンフィギュレーションを確認してください。

VRF にプレフィックスの VPN ラベルがない

デバイスの VPN Routing/Forwarding（VRF; VPN ルーティング/転送）のアドレスに、バーチャル プライベート ネットワーク（VPN）ラベルが見つかりませんでした。

OSPF ピア関係が確立されていない

PE インターフェイスは IP アンナンバードを使用して設定されています。Open Shortest Path First（OSPF）でピア関係が確立されるには、CE インターフェイスも IP アンナンバードを使用するか、PE インターフェイスと同じサブネット上に存在する必要があります。

PE と PE コア間でテストのみが実行され、オプションのループバック IP アドレス パラメータが入力されていない

テストされた LSP は、リモート サイト PE の BGP ルータ ID に基づいて選択されました。2 つの PE 間に複数の LSP がある場合、報告された結果はカスタマー トラフィックに使用された LSP の状態を正確に反映していない可能性があります。正しい LSP をテストするには、テストの入力ウィンドウで LSP エンドポイントを入力します。

バックアップ リンクの可能性

PE から送信プレフィックスへの ping は成功しましたが、想定していた PE インターフェイスを介して PE から送信プレフィックスへのルートを特定できませんでした。バックアップ リンクが動作中であるか、間違ったパラメータを入力した可能性があります。

ブロッキング ルート マップの可能性

PE にルート マップが設定されており、ルート トラフィックが失われる原因になっています。内部/外部 VPN コンフィギュレーションの場合は、ルート マップ コンフィギュレーション エラーの可能性があります。

コア IP 障害の可能性

ローカル PE からリモート PE に発行されたインターネット制御メッセージ プロトコル（ICMP）ping が失敗しました。ローカル PE の Interior Gateway Protocol（IGP）ルート テーブルに、リモート PE へのルートがありません。これらのデバイス間の IP 接続をトラブルシューティングしてください。

イーサネット デュプレックスの不一致の可能性

警告：アクセス回線インターフェイスにレイト コリジョンが発生しました。原因として、イーサネット デュプレックスの不一致が考えられます。

ルート制限に到達

デバイスのルート数がルート制限に達しました。

traceroute が送信されない

MPLS traceroute が送信されませんでした。

この章では、Cisco Prime Provisioning 6.3 リリースの Diagnostics アプリケーションでのトラブルシューティング ワークフローで実行される IOS および IOS XR コマンドの詳細を説明します。

IOS コマンド

この項では、Diagnostics で使用される IOS コマンドを示します。TACACS+（またはその他の認証/認可システム）を使用する場合は、これらすべてのコマンドが Diagnostics に対して許可されていることを確認してください。

（注）　このリストは、Diagnostics リリースまたはパッチが入手可能になると更新されます。最新のリストについては、mpls-diagnostics-expert@cisco.com まで E メールでお問い合わせください。

1. attach <*slot*> show version
2. execute-on slot <*slot*> 'show mpls forwarding-table <*destinationPrefix*> <*subnetMask*>'
3. execute-on slot <*slot*> 'show mpls forwarding-table <*destinationPrefix*>'
4. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*> <*subnetMask*>'
5. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*>'
6. execute-on slot <*slot*> 'show mpls forwarding-table vrf <*vrfName*>'
7. execute-on slot <*slot*> 'show mpls forwarding-table'
8. execute-on slot <*slot*> show ip cef vrf <*vrfName*> <*networkPrefix*>
9. execute-on slot <*slot*> show ip cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*>
10. execute-on slot <*slot*> show version
11. ping（対話型）
12. ping <*targetIp*>

13. ping mpls ipv4 <*targetIp*>/<*targetIpSubnetMask*> source <*source*> sweep <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*> <*repeatCount*> timeout <*timeout*> replyMode <*replyMode*>
14. ping mpls traffic-eng Tunnel <*tunnelNumber*>
15. ping vrf <*vrfName*>（対話型）
16. show access-lists <*listName*>
17. show atm map
18. show atm pvc <*interface*>
19. show cef drop
20. show cef drop | include ^<*slot*>
21. show frame-relay lmi
22. show frame-relay lmi interface <*interface*>
23. show frame-relay map
24. show frame-relay pvc <*interface*> dlci <*dlci*>
25. show interfaces <*interface*>
26. show ip bgp summary
27. show ip bgp vpnv4 <*vrfName*> rib-failure
28. show ip bgp vpnv4 all neighbors
29. show ip bgp vpnv4 all neighbors <*destIp*>
30. show ip bgp vpnv4 all | include local router
31. show ip bgp vpnv4 vrf <*vrfName*> <*networkPrefix*>
32. show ip bgp vpnv4 vrf <*vrfName*> neighbors <*destIp*>
33. show ip bgp vpnv4 vrf <*vrfName*> <*prefix*> <*subnetMask*>
34. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*> | [0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
35. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*classfulPrefix*>
36. show ip bgp vpnv4 vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*>
37. show ip cef <*destinationPrefix*>
38. show ip cef summary
39. show ip cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*> detail
40. show ip cef vrf <*vrfName*> <*networkPrefix*> detail
41. show ip cef vrf <*vrfName*> adjacency <*interface*> <*destip*> detail
42. show ip eigrp <*vrfName*> interfaces <*vrfInterface*>
43. show ip interface <*interface*>
44. show ip interface <*interface*> | include access list is
45. show ip interface brief <*interface*>
46. show ip interface brief | include <*ip-address*>
47. show ip ospf <*processId*> <*area*> interface <*intName*>
48. show ip ospf mpls traffic-eng link

49. show ip protocols <*vrfName*>
50. show ip route <*targetIp*>
51. show ip route vrf <*vrfName*> <*targetIp*>
52. show ip traffic
53. show ip vrf detail <*vrfName*>
54. show ip vrf interfaces <*vrfName*>
55. show mpls forwarding-table <*destinationPrefix*>
56. show mpls forwarding-table <*destinationPrefix*> <*subnetMask*>
57. show mpls forwarding-table <*destinationPrefix*> detail
58. show mpls forwarding-table labels <*label*>
59. show mpls forwarding-table labels <*label*> detail
60. show mpls forwarding-table vrf <*vrfName*>
61. show mpls forwarding-table vrf <*vrfName*> <*destinationPrefix*>
62. show mpls forwarding-table
63. show mpls interfaces <*interface*>
64. show mpls interfaces all
65. show mpls ip binding <*destinationPrefix*> <*destinationMask*>
66. show mpls ip binding local
67. show mpls ip binding summary
68. show mpls label range
69. show mpls ldp bindings <*ip*> <*subnetMask*>
70. show mpls ldp bindings neighbor <*neighbor ip*> <*subnetMask*>
71. show mpls ldp discovery
72. show mpls ldp neighbor
73. show mpls ldp neighbor <*interface*>
74. show mpls traffic-eng tunnels
75. show mpls traffic-eng tunnels <*status*>
76. show mpls traffic-eng tunnels <*tunnelId*>
77. show mpls traffic-eng tunnels destination <*destination*> <*status*>
78. show mpls traffic-eng tunnels destination <*destination*>
79. show mpls traffic-eng tunnels role <*role*>
80. show mpls traffic-eng tunnels role <*role*> <*status*>
81. show mpls traffic-eng tunnels role <*role*> destination <*destination*> <*status*>
82. show mpls traffic-eng tunnels role <*role*> destination <*destination*> up
83. show mpls traffic-eng tunnels role head brief
84. show ppp multilink interface <*interface*>
85. show route-map <*mapName*>
86. show running-config

87. show running-config interface <*interface*>
88. show running-config interface <*interface*> | include frame-relay interface-dlci
89. show running-config interface <*interface*> | include map-group
90. show running-config interface <*interface*> | include no frame-relay inverse-arp
91. show running-config | begin router bgp
92. show running-config | include advertise-
93. show running-config | include ldp password
94. show running-config | include mpls label protocol
95. show running-config | include no
96. show version
97. show vlans
98. traceroute mpls ipv4 <*ipAddress*>/<*subnetMask*> source <*source*> destination <*destination*> ttl 15
99. traceroute mpls traffic-eng Tunnel <*tunnelNumber*>
100. traceroute vrf <*vrfName*>（対話型）

IOS XR コマンド

この項では、Diagnostics で使用される IOS XR コマンドを示します。TACACS+（またはその他の認証/認可システム）を使用する場合は、これらすべてのコマンドが Diagnostics に対して許可されていることを確認してください。

（注）　このリストは、Diagnostics リリースまたはパッチが入手可能になると更新されます。最新のリストについては、mpls-diagnostics-expert@cisco.com まで E メールでお問い合わせください。

1. ping <*targetIp*>
2. ping atm interface <*interface*> <*vpi*>/<*vci*>
3. ping atm interface <*interface*> <*vpi*>/<*vci*> end-loopback
4. ping atm interface <*interface*> <*vpi*>/<*vci*> seg-loopback
5. ping mpls ipv4 <*destination*>/<*subnetMask*>
6. ping mpls ipv4 <*destination*>/<*subnetMask*> reply mode router-alert
7. ping mpls ipv4 <*destination*>/<*subnetMask*> source <*source*>
8. ping mpls traffic-eng Tunnel <*tunnelId*>
9. ping vrf <*vrfName*>
10. ping vrf <*vrfName*> <*targetIp*> <*sourceInterface*> <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*>
11. show access-lists ipv4 <*listName*>
12. show bgp ipv4 all summary
13. show bgp vpnv4 unicast neighbors
14. show bgp vpnv4 unicast summary

15. 14.show bgp vpnv4 unicast vrf <*vrfName*> <*networkPrefix*>
16. show bgp vpnv4 unicast vrf <*vrfName*> <*prefix*> <*mask*>
17. show bgp vpnv4 unicast vrf <*vrfName*> labels
18. show bgp vrf <*vrfName*> advertised neighbor <*neighboreId*> summary | include <*ceDeviceIpAddr*>
19. show bgp vrf <*vrfName*> ipv4 unicast
20. show bgp vrf <*vrfName*> neighbors
21. show bgp vrf <*vrfName*> vpnv4 unicast neighbors
22. show cef ipv4 <*destinationPrefix*>
23. show cef ipv4 drops
24. show cef ipv4 drops location <*slot*>
25. show cef ipv4 summary
26. show cef vrf <*vrfName*> ipv4 <*networkPrefix*> detail
27. show cef vrf <*vrfName*> ipv4 <*networkPrefix*> <*subnetMask*> detail
28. show cef vrf <*vrfName*> <*networkPrefix*> <*subnetMask*> location <*location*>
29. show eigrp <*vrfName*> interfaces <*vrfInterface*>
30. show frame-relay lmi
31. show frame-relay lmi interface <*interface*>
32. show install active summary
33. show install inactive summary
34. show install location <*slot*>
35. show interfaces <*interface*>
36. show ip cef vrf <*vrfName*> adjacency <*interface*> <*destip*> detail
37. show ip ospf <*processId*> <*area*> interface <*intName*>
38. show ipv4 interface <*interface*>
39. show ipv4 interface brief <*interface*>
40. show ipv4 interface brief | include <*ip-address*>
41. show ipv4 traffic
42. show ipv4 vrf <*vrfName*> interface brief
43. show ipv4 vrf <*vrfName*> interface <*interface*>
44. show ipv4 vrf all interface brief
45. show mpls forwarding
46. show mpls forwarding labels <*label*>
47. show mpls forwarding prefix <*destinationPrefix*>/<*subnetMask*>
48. show mpls forwarding prefix <*destinationPrefix*>/<*subnetMask*> detail
49. show mpls forwarding vrf <*vrf*>
50. show mpls forwarding vrf <*vrf*> prefix <*destinationPrefix*>/<*subnetMask*>

51. show mpls forwarding vrf <*vrfName*> prefix <*destinationPrefix*>/<*subnetMask*> labels <*label*> location <*location*>
52. show mpls forwarding vrf <*vrfName*> prefix <*destinationPrefix*>/<*subnetMask*> location <*location*>
53. show mpls interfaces
54. show mpls interfaces <*interface*>
55. show mpls label range
56. show mpls label table summary
57. show mpls ldp bindings <*ip*> <*mask*>
58. show mpls ldp bindings neighbor <*neighbor*> <*ip*> <*mask*>
59. show mpls ldp discovery
60. show mpls ldp neighbor
61. show mpls ldp neighbor <*interface*>
62. show mpls traffic-eng tunnels
63. show mpls traffic-eng tunnels backup <*tunnelId*>
64. show mpls traffic-eng tunnels brief role head
65. show mpls traffic-eng tunnels <*status*> detail
66. show mpls traffic-eng tunnels <*tunnel-id*>
67. show mpls traffic-eng tunnels <*tunnelNumber*> detail
68. show mpls traffic-eng tunnels destination <*destination*>
69. show mpls traffic-eng tunnels name <*name*>
70. show mpls traffic-eng tunnels destination <*destination*> <*status*> detail
71. show mpls traffic-eng tunnels destination <*destination*> detail
72. show mpls traffic-eng tunnels detail
73. show mpls traffic-eng tunnels role <*role*> <*status*> detail
74. show mpls traffic-eng tunnels role <*role*> destination <*destination*> <*status*> detail
75. show mpls traffic-eng tunnels role <*role*> destination <*destination*> up detail
76. show mpls traffic-eng tunnels role <*role*> detail
77. show ospf
78. show ospf vrf <*vrf*>
79. show ospf border-routers | include ABR
80. show ospf | include ID
81. show ospf mpls traffic-eng link
82. show ospf vrf <*vrfName*> interface brief
83. show ospf vrf <*vrfName*> interface <*interfaceName*>
84. show protocols | include OSPF
85. show rib ipv4 tables
86. show rib vrf <*vrf*> ipv4 unicast statistics <*protocolName*>

87. show rib vrf <*vrf*> protocols
88. show rip vrf <*vrf*>
89. show route ipv4 <*targetIp*>
90. show route vrf <*vrfName*> ipv4 <*targetIp*>
91. show rpl route-policy <*mapName*>
92. show rsvp neighbors
93. show running-config
94. show running-config explicit-path name <*explicitPathName*>
95. show running-config interface <*interface*>
96. show running-config mpls ldp
97. show running-config mpls ldp label advertise
98. show running-config mpls traffic-eng
99. show running-config router bgp
100. show running-config router bgp <*asNumber*> vrf <*vrfName*> neighbor <*neighborIpAddr*>
101. show running-config router bgp <*asNumber*> neighbor-group <*neighborGroupName*>
102. show running-config router bgp | include redistribute <*protocol*>
103. show running-config router ospf
104. show running-config router <*protocol ID*> vrf <*vrf*>
105. show running-config rsvp interface <*interface-name*>
106. show vlan interface
107. show version
108. show vrf <*vrfName*> ipv4 detail
109. traceroute mpls ipv4 <*destination*>/<*subnetMask*>
110. traceroute mpls traffic-eng Tunnel <*tunnelId*>
111. traceroute vrf <*vrf*>
112. ping vrf <*vrfName*> <*targetIpv6Address*> <*sourceInterface*> <*minSweepSize*> <*maxSweepSize*> <*sweepInterval*>
113. show bgp vpnv6 unicast neighbors
114. show bgp vpnv6 unicast neighbors <*destIp*>
115. show bgp vpnv6 unicast vrf <*vrfName*> <*networkPrefix*>
116. show bgp vpnv6 unicast vrf <*vrfName*> <*networkPrefix*>/<*subnetMask*>
117. show bgp vpnv6 unicast vrf <*vrfName*> labels | include <*networkPrefix*>/<*subnetMask*>| [0-9A-Fa-f:]+[0-9A-Fa-f]*
118. show bgp vpnv6 unicast summary | include BGP router identifier
119. show bgp vrf <*vrfName*> ipv6 unicast
120. show bgp vrf <*vrfName*> ipv6 unicast advertised neighbor <*neighborId*> summary | include <*ceDeviceIpAddr*>
121. show cef ipv6 summary

122.show cef vrf <*vrfName*> ipv6 <*networkPrefix*> detail

123.show cef vrf <*vrfName*> ipv6 <*networkPrefix*>/<*subnetMask*> detail

124.show cef vrf <*vrfName*> ipv6 <*networkPrefix*> location <*location*>

125.show cef vrf <*vrfName*> ipv6 <*networkPrefix*>/<*subnetMask*> location <*location*>

126.show ipv6 interface <*interface*>

127.show ipv6 interface brief <*interface*>

128.show ipv6 vrf all interface brief

129.show ipv6 vrf <*vrfName*> interface brief

130.show ipv6 vrf <*vrfName*> interface <*interface*>

131.show rib ipv6 tables

132.show route ipv6 <*targetIp*>

133.show route vrf <*vrfName*> ipv6 <*targetIp*>

134.show vrf <*vrfName*> ipv6 detail

CHAPTER 12

トポロジ ツールの使用

この章では、トポロジ ツールが Prime Provisioning Web クライアントを介して設定されたネットワークのグラフィック ビューを提供する方法を説明します。これはネットワークのデバイスおよびリンクの両方について、さまざまな物理的および論理的部分をグラフィックで表現するツールです。次の事項について説明します。

はじめに

トポロジ ツールには 3 種類のビューがあります。

- VPN ビュー：カスタマー デバイス間の接続を表示します。VPN ビューは、すべてのサービスの集約ビューと、各サービスの個別論理ビューおよび物理ビューを提供します。
- 論理ビュー：選択されたプロバイダー リージョンでセットアップされた論理接続を表示します。
- 物理ビュー：プロバイダー リージョンで名前付き物理回線の接続性を表示します。

さらに、この章では、次の機能についても説明します。

- フィルタリングおよび検索：大きなグラフ内の不要な情報を除外したり、検索ツールを使用して特定のデバイスに直接ジャンプしたりします。
- マップの使用：個々のビューとマップを関連付けます。

ただし、ウィンドウの装飾など、一部の詳細はシステム固有で、環境が異なると表示も異なる可能性があります。しかし、機能は一貫性を保ちます。

トポロジ ツールの起動

トポロジ ツールを起動するステップは、次のとおりです。

ステップ 1　Prime Provisioning にログインします。

ステップ 2　[Inventory] > [Logical Inventory] > [Topology] を選択します。図 12-1 のようにウィンドウが表示されます。

ウィンドウの下部で指定されている適切な Java Runtime Environment（JRE）を使用していない場合、使用しているシステムに対応するリンクをクリックし、そのパスに従って進んでから、ブラウザを終了し、もう一度ログインして、[Topology Tool] ページに戻ります。

図 12-1　トポロジ起動ウィンドウ

ステップ 3　Web クライアントでトポロジ ツール アプリケーションを起動するには、図 12-1 の [ISC-VPN Topology] をクリックします。

これにより、Java Web Start アプリケーションが開始されます。

（注）　名前の解決が必要です。Prime Provisioning HTTP サーバのホストが Web クライアントが使用している Domain Name System（DNS）であるか、Prime Provisioning サーバの名前とアドレスがクライアント ホスト ファイルに含まれている必要があります。

ステップ 4　初めてインベントリ マネージャをアクティブ化すると、[Security Warning] ウィンドウが表示されます。[Start] をクリックして進めるか、[Details] をクリックしてセキュリティ証明書を確認すると、[Desktop Integration] ウィンドウが表示されます。

ステップ 5　デスクトップ環境に統合する場合は [Yes]、しない場合は [No]、次回、VPN トポロジを起動したときにもう一度このウィンドウを表示する場合は [Ask Later]、デスクトップの統合をカスタマイズする場合は [Configure ...] をクリックします。

[Desktop Integration] ウィンドウで選択したかどうかに関係なく、[Login] ウィンドウが表示されます。

ステップ 6　[User Name] および [Password] を入力し、[OK] をクリックします。

トポロジ ツールが起動し、マスタ Prime Provisioning サーバに接続します。

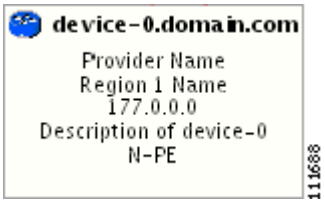
表記法

トポロジ ソフトウェアには、表示されたオブジェクトに関する情報を視覚的に伝えるための規則がいくつかあります。デバイスを表すノードの形状と色は、表 12-1 に示すとおり、デバイスのロールによって異なります。

表 12-1　　デバイス ロール アイコン

形状	説明
	CAT OS カスタマー デバイスを表す緑色のアイコン。これに続けて、次の情報が表示されます。 - デバイス名 - カスタマー名 - サイト名 - 管理 IP アドレス - 説明 - ロール（VPN の SPOKE または HUB）
	ルータ カスタマー デバイスを表す緑色のアイコン。これに続けて、次の情報が表示されます。 - デバイス名 - カスタマー名 - サイト名 - 管理 IP アドレス - 説明 - ロール（VPN の SPOKE または HUB）
	インターフェイスを表す緑色のアイコン。これに続けて、次の情報が表示されます。 - インターフェイス名 - 管理 IP アドレス - カプセル化タイプ - インターフェイス タイプ
	CAT OS プロバイダー デバイスを表す青色のアイコン。これに続けて、次の情報が表示されます。 - デバイス名 - プロバイダー名 - リージョン名 - 管理 IP アドレス - 説明 - ロール

表 12-1　デバイス ロール アイコン （続き）

形状	説明
	ルータ プロバイダー デバイスを表す青色のアイコン。これに続けて、次の情報が表示されます。 - デバイス名 - プロバイダー名 - リージョン名 - 管理 IP アドレス - 説明 - ロール
	リージョンを表す青色のアイコン。これに続けて、次の情報が表示されます。 - リージョン名 - プロバイダー名
	サイトを表す緑色のアイコン。これに続けて、次の情報が表示されます。 - サイト名 - カスタマー名 - サイトのデバイスが VPN に参加したときのロール（HUB、SPOKE、または HUB と SPOKE の組み合わせ）
	サイトを表す緑色のアイコン。これに続けて、次の情報が表示されます。 - サイト名 - カスタマー名 - サイトのデバイスが VPN に参加したときのロール（HUB、SPOKE、または HUB と SPOKE の組み合わせ）

リンクのタイプを強調するため、表 12-2 に示す配色パターンが使用されています。

表 12-2　リンクのタイプ別配色パターン

色	接続タイプ
（グリーン）	エンドツーエンド ワイヤ

表 12-2　リンクのタイプ別配色パターン （続き）

色	接続タイプ
（紫色）	接続回線
（茶色）	MPLS VPN リンク

最後に、表 12-3 に示す 4 種類のパターンはサービス要求の状態を示すために使用されます。

表 12-3　リンク状態を表すパターン

パターン	サービス要求の状態
	Deployed、Functional、Pending
	Failed Audit、Invalid、Broken、Lost
	Wait Deploy、Requested、Failed Deploy
	Closed

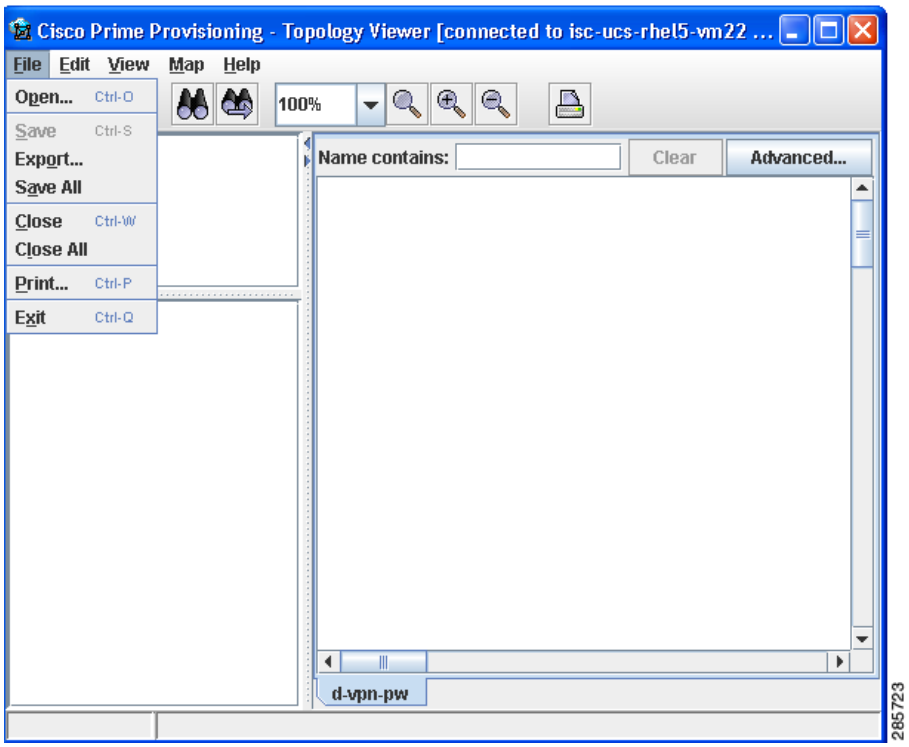
Prime Provisioning-VPN Topology でのトポロジ ツールへのアクセス

「トポロジ ツールの起動」（P.12-2）の「トポロジ起動ウィンドウ」にある図 12-1 の手順に従ってトポロジ ツールを起動し、次の手順に従って、**ISC-VPN Topology** ツールにアクセスします。

ステップ 1　[Inventory] > [Logical Inventory] > [Topology] > [ISC-VPN Topology] を選択します。

図 12-2 に示す [Topology] ウィンドウが表示されます。

図 12-2　トポロジ アプリケーション ウィンドウ



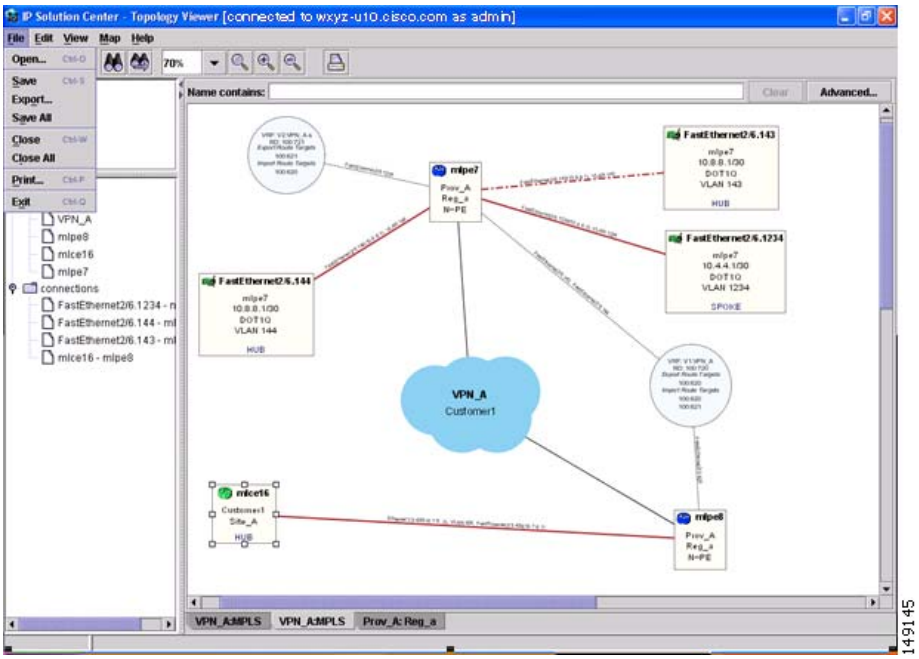
アプリケーション ウィンドウは、図 12-2 に示すとおり 4 つのエリアに分けられます。

- エリア（1）：左上には概要エリアが表示されます。色付きの長方形のパネルは「パナー」と呼ばれ、そのときメイン エリアに表示されているエリアに対応しています。パナーを移動すると、メイン エリアに表示されるグラフの部分が変わります。これは、大型のグラフでは特に便利な機能です。
- エリア（2）：左下のエリアには、グラフのツリー ビューが表示されます。グラフが何も表示されていない場合、[Unnamed] と呼ばれるノードが 1 つ表示されます。グラフが表示されると、デバイスを表すツリーと、そのインターフェイスおよび接続があればそれらが表示されます。このツリーは、デバイスや接続をすばやく見つけるために使用できます。
- エリア（3）：ウィンドウのメイン エリア（メイン ビュー）には、デバイス間の接続を表すグラフが表示されます。表示されているネットワークの名前は最下部に表示されます。ビューが表示されていない場合のデフォルト名は [Unnamed] です。
- エリア（4）：メイン ウィンドウの上にはフィルタ エリアがあります。ここにパターンを入力して、ノードをフィルタできます。入力したパターンを含む名前を持つノードの明るさのレベルは通常と変わりません。その他のノードやエッジはすべて淡色表示されます（図 12-14 および「フィルタリング」（P.12-20）を参照）。

（注）　すべてのエリアの下にあるバーはステータス バーです。

ビューのロード、保存、およびクローズには [File] メニューを使用します（図 12-3 を参照）。

図 12-3　[File] メニュー



[File] メニューには、次のメニュー項目が含まれます。

- [Open]：ビューを開きます。
- [Save]：開かれていてアクティブなビューを、すでにファイル名がつけられていればその名前で保存します。
- [Export]：Scalable Vector Graphics（SVG）、Joint Photographics Expert Group（JPG）、または Portable Network Graphics（PNG）フォーマットのいずれかでアクティブ ビューをエクスポートします。
- [Save All]：開かれているビューをすべて保存します。
- [Close]：開かれていてアクティブなビューを閉じます。
- [Close All]：開かれているビューをすべて閉じます。
- [Print]：開かれていてアクティブなビューを印刷します。
- [Exit]：トポロジ ツールを終了します。

ビューのタイプ

トポロジ アプリケーションには 3 種類のビュー ペインがあります。これ以降の項では、これらのペインについて説明します。

- 「VPN ビュー」（P.12-8）。VPN 内のデバイス間の接続を示します。
- 「論理ビュー」（P.12-12）。リージョン内の PE と CPE の間の接続を示します。
- 「物理ビュー」（P.12-14）。リージョン内の PE に対する物理デバイスとリンクを示します。

ビュー属性は、図 12-4 に示すとおり、[View] メニューを使って変更できます。

図 12-4　[View] メニュー

[View] メニューには、次のメニュー項目が含まれます。

- [Anti-Aliasing]：ビューを描画するときに、パフォーマンスを犠牲にして、より滑らかなラインと気持ちのよい外観を生み出します。
- [Grid]：磁気グリッドをアクティブ化します。グリッドは 10 X 10 の間隔で、ビュー内のノードをそろえやすくするために使用できます。
- [Auto-Layout]：ビュー内にノードの自動レイアウトを生成します。選択した場合、プログラムは、最も体裁のよいノード配置を見つけようと試行します。
- [Zoom]：ウィンドウが開かれます。このウィンドウでは、必要な拡大レベルを指定できます。
- [Zoom In]：拡大レベルを増やします。
- [Zoom Out]：拡大レベルを減らします。
- [Refresh]：ビューを再生成します。これは、リポジトリ内のデータが変化した場合に特に便利です。更新後のビューを確認するには、[Refresh] を選択するか、または [Refresh] ツールバー ボタンをクリックします。

VPN ビュー

VPN ビューは、指定された VPN を構成するデバイス間の接続を表示します。VPN ビューをアクティブ化するステップは、次のとおりです。

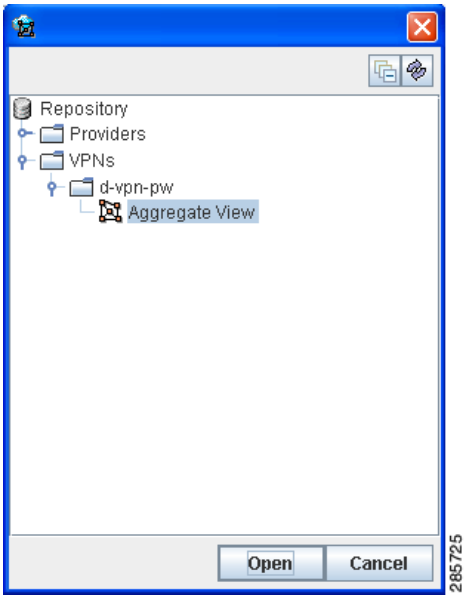
ステップ 1　メニュー バーで、[File] > [Open] を選択します。

または

ツールバーの [Open] ボタンをクリックします。

図 12-5 のフォルダ ビュー ウィンドウが開き、ディレクトリ ツリーと使用可能な VPN が表示されます。

図 12-5　フォルダ ビュー ウィンドウ



ステップ 2　目的の VPN フォルダを見つけ、このフォルダを選択して、[Open] をクリックします。

これにより、目的のフォルダが開かれ、この VPN に関連付けられている論理ビューと物理ビューがすべて表示されます。

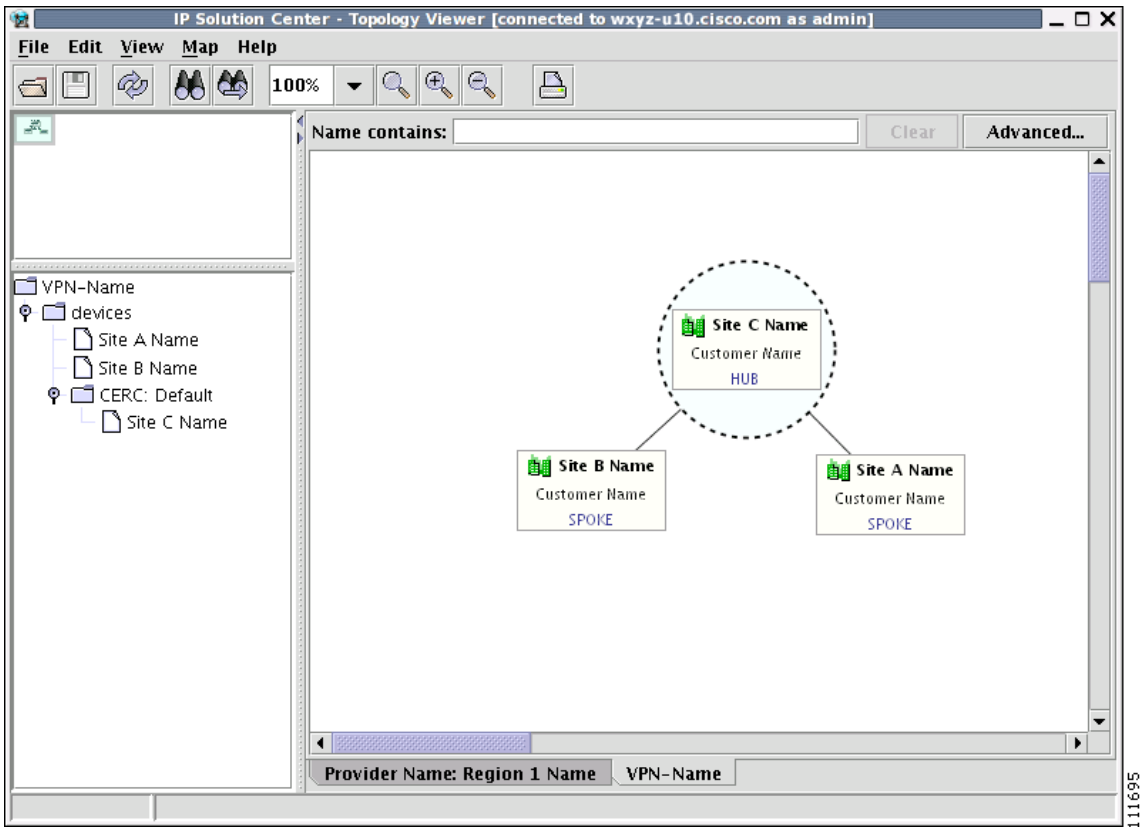
フォルダ ツリーから論理ビューまたは物理ビュー項目を 1 つクリックします。論理ビューは詳細の量を最小限に抑え、カスタマー デバイス間の接続を表示します。物理ビューは、VPN の物理的構造に関する詳細を明らかにします。たとえば、MPLS については、カスタマー デバイスとプロバイダー デバイスの間の接続とプロバイダーのコアが表示されます。

集約ビュー

図 12-6 に示す集約ビューには、カスタマー デバイスの接続に使用されているテクノロジーのタイプに関係なく、すべてのカスタマー デバイス間の接続を示します。

1 つのビューには、MPLS、レイヤ 2、および VPLS の組み合わせが表示されることもあります。MPLS については、顧客宅内装置（CPE）デバイスのみ表示されます。

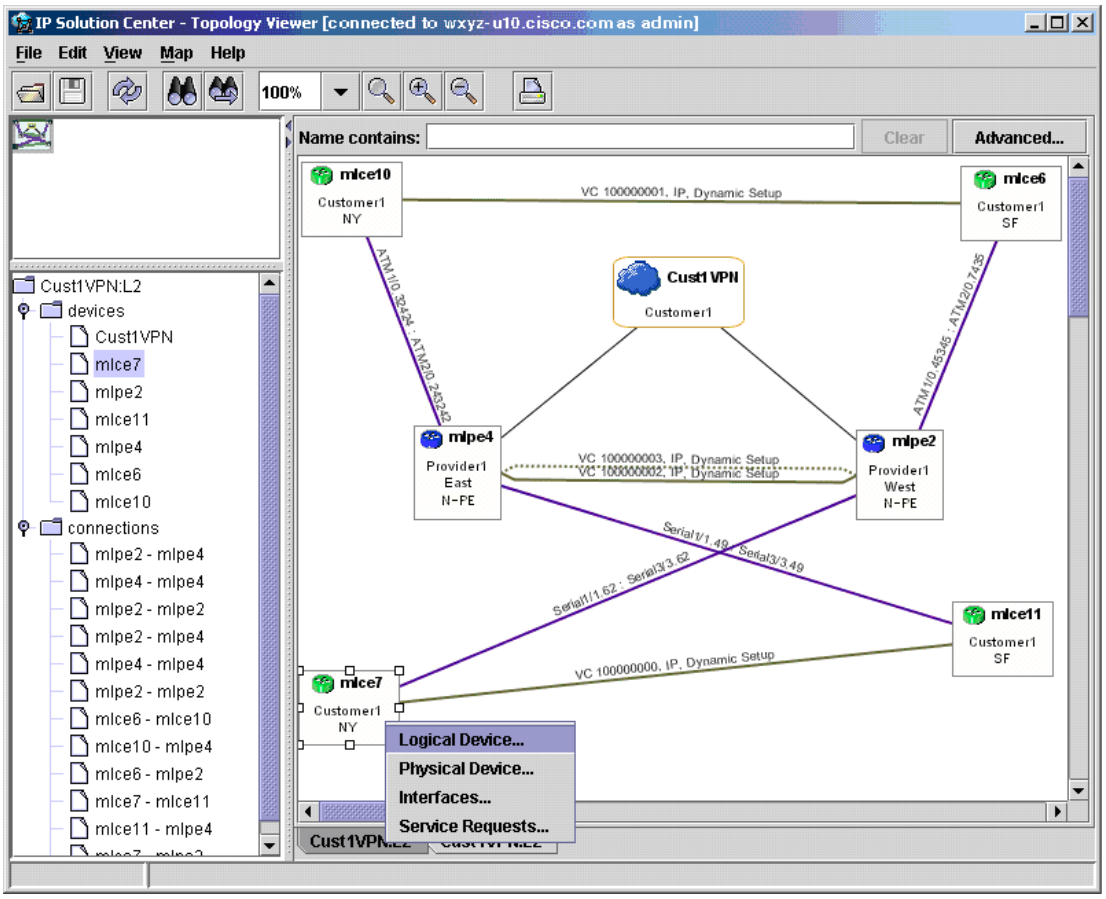
図 12-6　　集約ビュー



CPE に加えて、レイヤ 2 VPN に Customer Location Edge（CLE）デバイス間、またはプロバイダー エッジ（PE）デバイス間の接続が表示されることもあります。VPLS では、CPE 間の接続が表示されます。欠損 CPE では、PE への接続が表示されます。

MPLS レイヤ 2 VPN では、トポロジは、仮想回線（VC）を MPLS コアとともに（MPLS 文字列として）表示しますが、L2TPv3 では、図 12-7 に示すように、仮想回線（VC）を IP コアとともに（IP 文字列として）表示します。

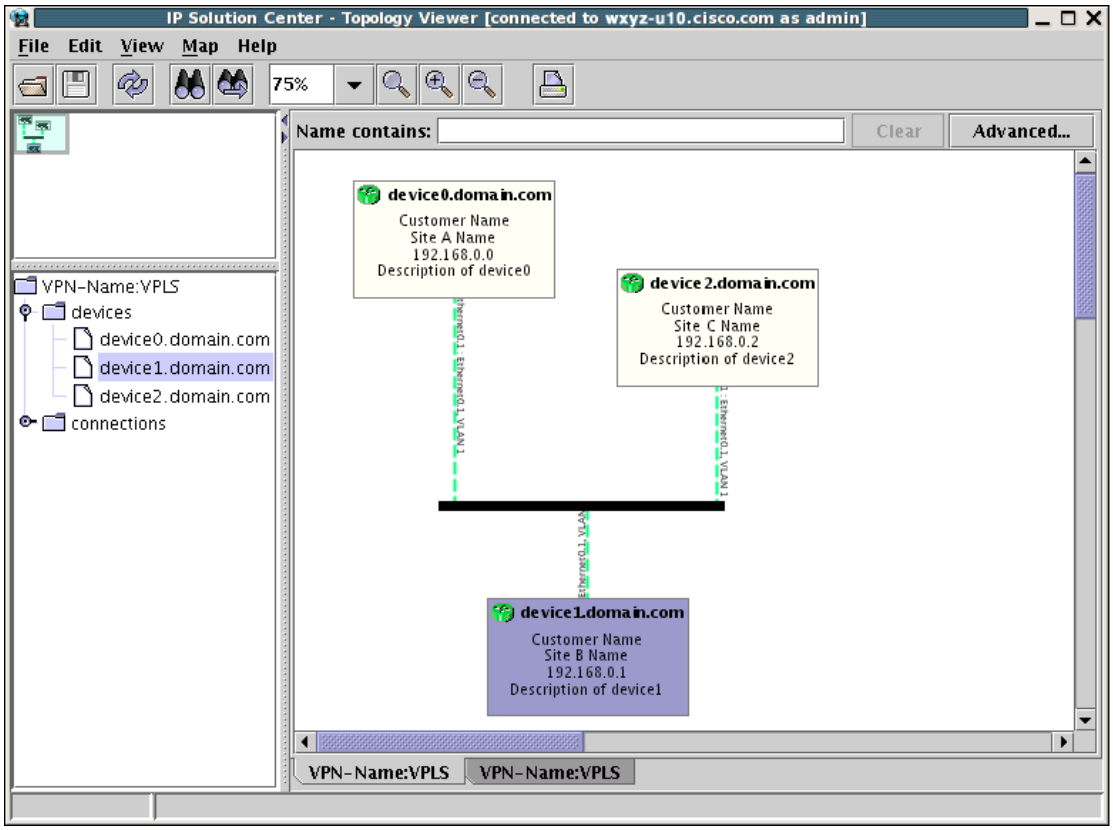
図 12-7　IP コアを持つ Virtual Circuit



VPLS トポロジ

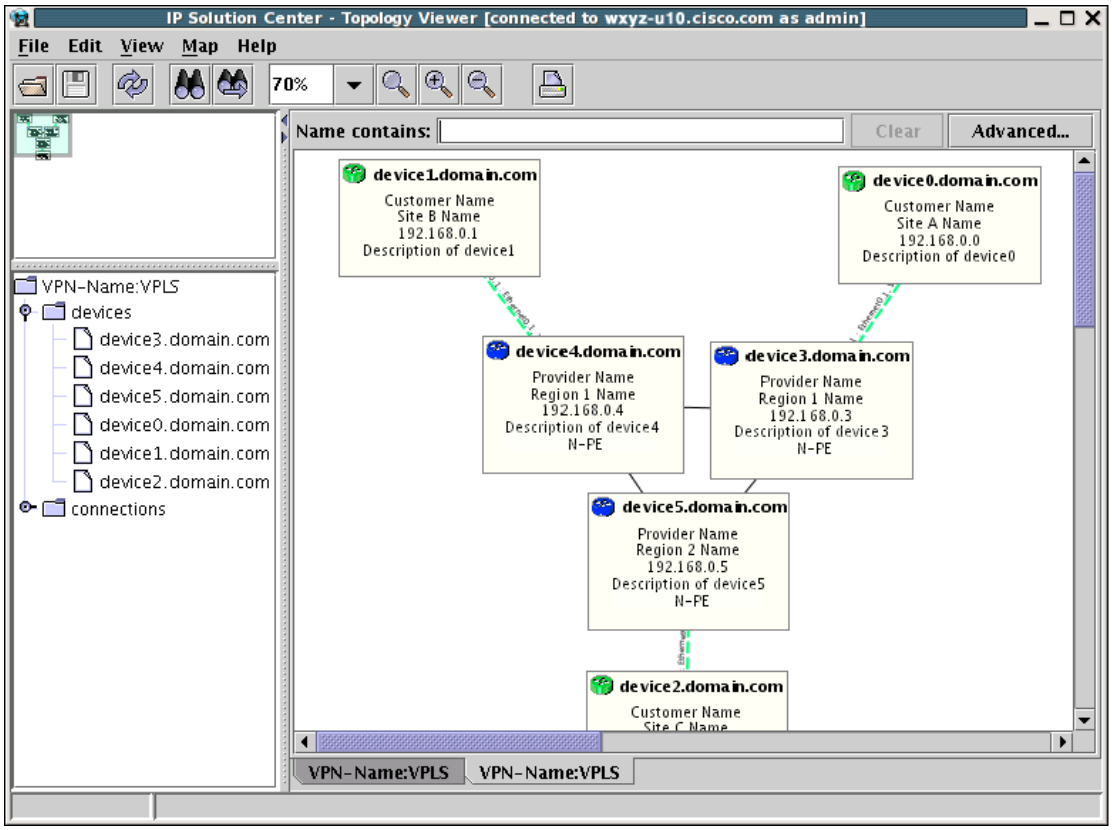
VPLS トポロジの場合、Attachment Circuit View または Emulated Circuit View にアクセスできます。Attachment Circuit View は、他のタイプの VPN にある論理ビューに相当します。このビューには、図 12-8 にあるとおり、仮想プライベート LAN に接続されているカスタマー デバイスが表示されます。

図 12-8　Attachment Circuit View



Emulated Circuit View には、Attachment Circuit View では省略されている物理接続に関する詳細が表示されます。このビューには、図 12-9 にあるとおり、プロバイダーのデバイスと、プロバイダーのデバイスに接続されているカスタマー デバイスの間の接続が表示されます。

図 12-9　Emulated Circuit View



論理ビュー

この論理ビューには、指定されたリージョンの PE と CPE の間にある、サービス要求により作成された接続が表示されます。

論理ビューをアクティブ化するステップは、次のとおりです。

ステップ 1　メニュー バーで、[File] > [Open] を選択します。

または

ツールバーの [Open] ボタンをクリックします。

フォルダ ビュー ウィンドウが表示されます（図 12-5 を参照）。

ステップ 2　目的の VPN のフォルダを見つけ、このフォルダをダブルクリックします。

この VPN に関連付けられている論理ビューおよび物理ビューがすべて表示されます。

ステップ 3　選択した VPN の論理ビューを開くには、次のいずれかを実行します。

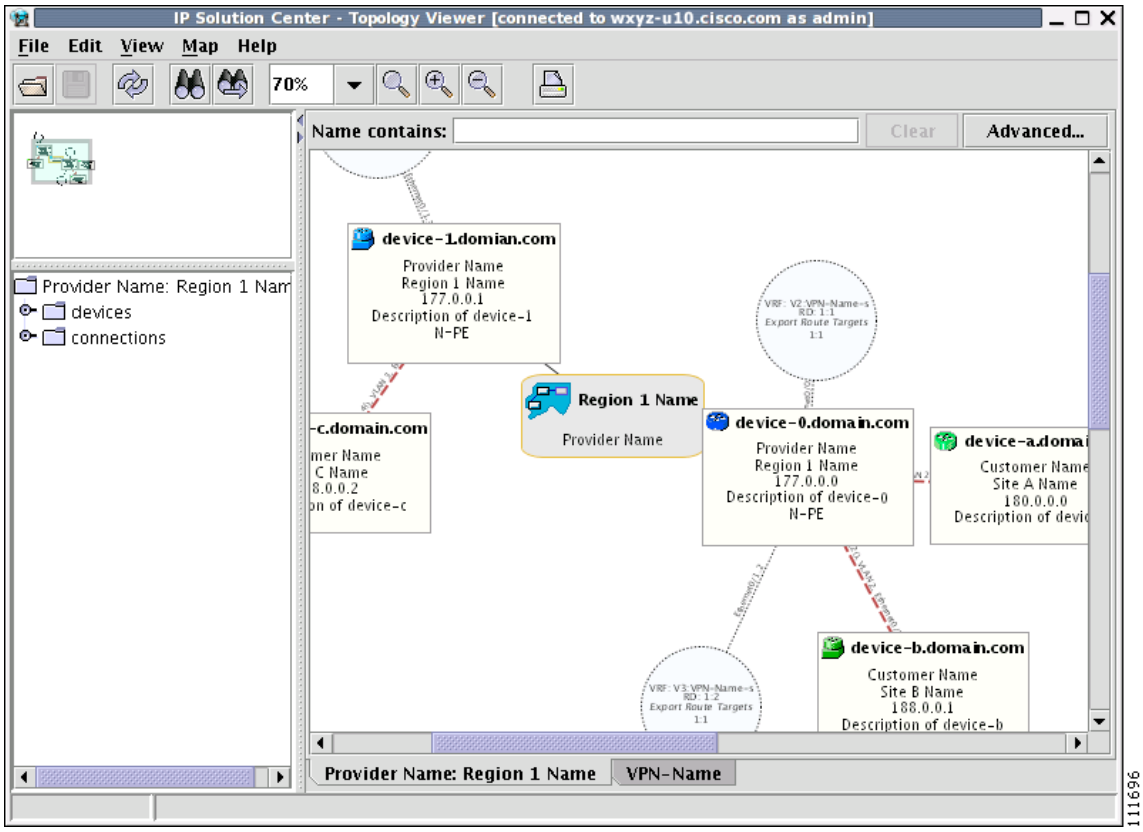
[Logical View] アイコンを 1 回クリックし、[Open] をクリックします。

または

[Logical View] アイコンをダブルクリックします。

これにより、図 12-10 に示すように、選択した VPN の論理ビューが作成されます。

図 12-10　論理ビュー



作成されたビューでは、通常、グラフの中央にあるノードは、あるプロバイダーに与えられたリージョンを表すノードです。このノードには、そのリージョンの名前とプロバイダーの名前が注釈として付けられています。

リージョンのノードに直接接続されているノードは PE を表します。ノードのアイコンは、それが表しているデバイスのタイプとロールによって異なります（「表記法」（P.12-3）を参照）。

個々の PE には、完全修飾デバイス名、プロバイダー名、リージョン名、管理 IP アドレスの説明、およびロールが注釈として付けられています。ノードを右クリックすると、このノードに関連付けられている論理デバイスと物理デバイス、インターフェイス、およびサービス要求の詳細が表示されます。リージョン内のノードに関する詳細は表形式で表示されます。

さまざまなノードやリンク プロパティの詳細については、「デバイスのプロパティとリンクのプロパティの表示」（P.12-16）で説明します。

また、リンクを右クリックすると、そのリンク プロパティについての説明が表示されます。たとえば、サンプル シリアル リンクの [Interfaces...] を選択すると、[Properties] ウィンドウが表示されます。

個々の PE は、1 つ以上の CPE に論理接続できます。このような接続は、MPLS VPN リンク、またはレイヤ 2 論理リンクによって作成されます。これらの接続はそれぞれ、指定された PE を CPE にリンクするエッジによって表されます。特定の PE と CPE の間にさらにその他にも接続がある場合は、これらもすべて表示されます。接続の状態に応じて、エッジは実線（機能している接続を表す）、点線（壊れている接続）、破線（まだ確立されていない接続）を使って描画されます。

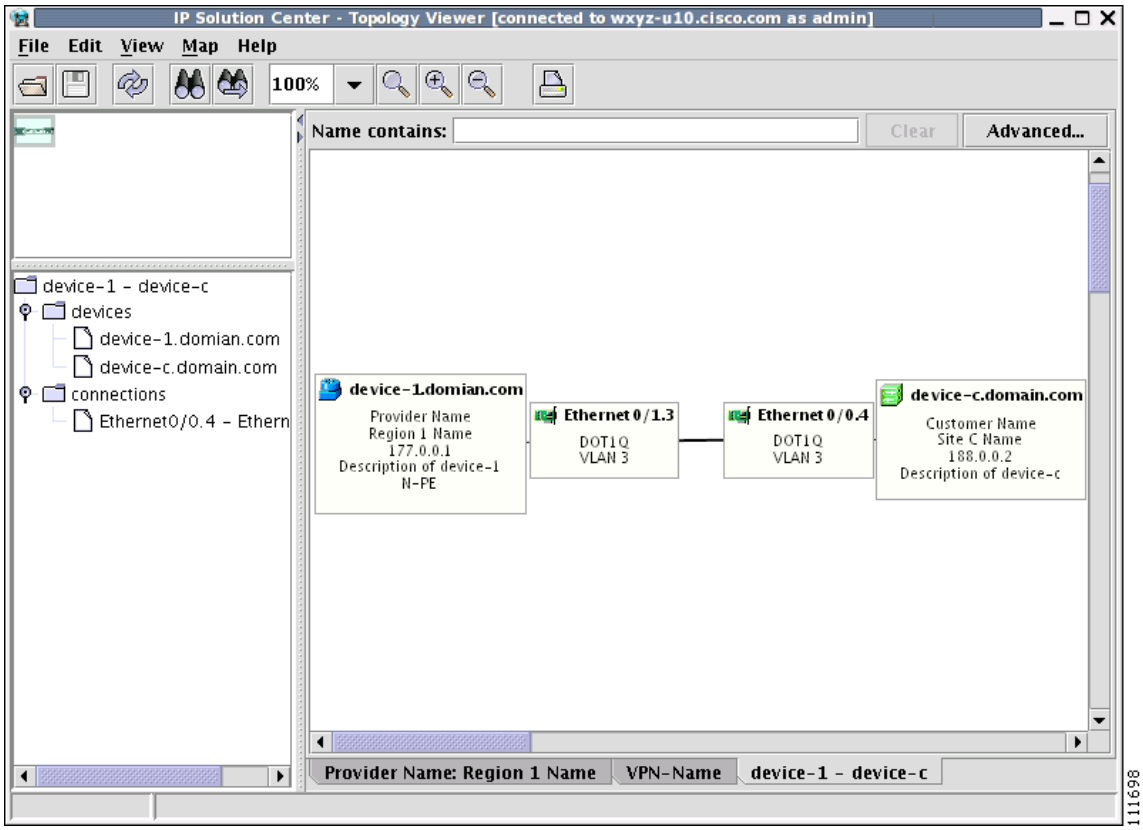
接続のタイプに応じて、接続は表 12-2 および表 12-3 で説明されているとおりに描画されます。個々の接続には、PE インターフェイス名（IP アドレス）、VLAN ID 番号、CPE インターフェイス名（IP アドレス）が注釈として付けられています。

概要エリアでは、接続の形成に多数のデバイスが使用されていたとしても、CPE と PE の間に直接接続が描画されます。

デバイス プロパティの表示の詳細については、「デバイスのプロパティとリンクのプロパティの表示」（P.12-16）を参照してください。

接続の詳細を表示するには、この接続を右クリックし、ポップアップ メニューから [Expand] オプションを選択します。展開されたビューが新しいタブに表示され、そこには指定された PE から CPE への接続を形成するすべてのデバイスとインターフェイスが表示されます（図 12-11 を参照）。

図 12-11　　接続詳細ビュー



物理ビュー

物理ビューには、指定されたリージョンで PE について定義されている名前付き物理回線がすべて表示されます。名前付き物理回線はそれぞれ、PE からそのインターフェイスを通って CLE または CPE のインターフェイスへと続く接続のシーケンスとして表されます。指定されたリージョンの PE と CLE または CPE の間の物理リンクがすべて表示されます。物理リンクは、完璧な動作順になっていることが前提であるため、エッジは常に実線で描画されます。

物理ビューをアクティブ化するステップは、次のとおりです。

ステップ 1　メニュー バーで、[File] > [Open] を選択します。

または

ツールバーの [Open] ボタンをクリックします。

フォルダ ビュー ウィンドウが表示されます（図 12-5 を参照）。

ステップ 2　目的の VPN のフォルダを見つけ、このフォルダをダブルクリックします。

この VPN に関連付けられている論理ビューおよび物理ビューがすべて表示されます。

ステップ 3　選択した VPN の物理ビューを開くには、次のいずれかを実行します。

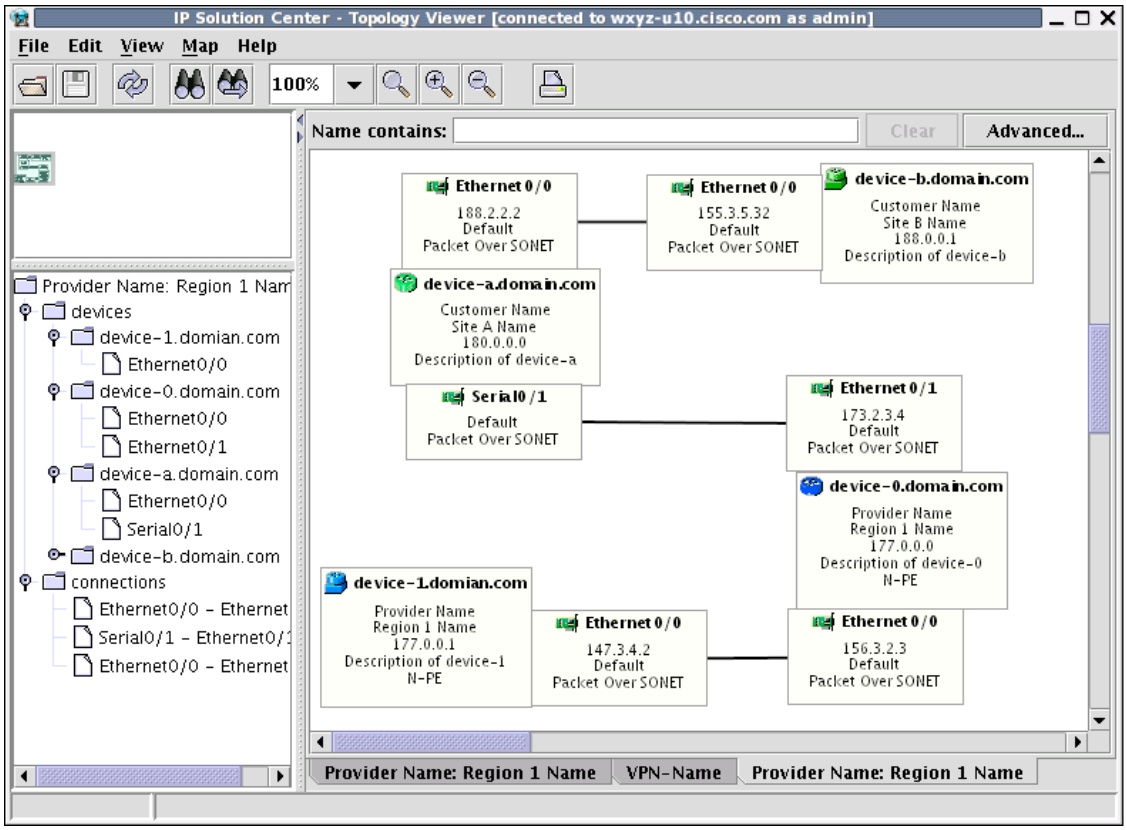
[Physical View] アイコンを 1 回クリックし、[Open] をクリックします。

または

[Physical View] アイコンをダブルクリックします。

これにより、図 12-12 に示すように、選択した VPN の物理ビューが作成されます。

図 12-12　　物理ビュー



このビューでは、各デバイスは、専用のインターフェイスに細い線で接続されています。インターフェイスは他のインターフェイスと太い線で接続されています。2 つのインターフェイスの間に複数の接続が存在する場合、すべての接続を表示するために、インターフェイスどうしは間を空けて表示されます。

ツリーにはデバイスと接続が表示されます。各デバイスが、ツリーに接続されたすべてのインターフェイスを持つフォルダである可能性もあります。

デバイスのプロパティとリンクのプロパティの表示

論理ビューには、デバイスとリンクの両方のプロパティを表示できます。物理ビューでは、物理デバイスのプロパティにのみアクセスできます。

したがって、デバイスのプロパティは論理ビューと物理ビューの両方で確認可能です。

Device Properties

デバイスのプロパティを表示するには、目的のデバイスを右クリックします。[Device Properties] メニューが表示されます。

次のプロパティを使用できます。

[Logical Device...]：デバイスの論理プロパティを表示します。

[Physical Device...]：デバイスの物理プロパティを表示します。

[Interfaces...]：デバイスのインターフェイス プロパティを表示します。

[Service Requests...]：デバイスに関連付けられたサービス要求プロパティを表示します。

Logical Device

デバイスを右クリックし、[Logical Device...] を選択すると、論理デバイスの [Properties] ウィンドウが表示されます。

論理プロパティ ウィンドウには、次の情報が表示されます。

[Device Name]：デバイスの名前。

[Provider Name]：このデバイスがサービスを提供しているプロバイダーの名前。

[Region Name]：プロバイダー リージョンの名前。

[Loopback Address]：ループバック アドレスの IP アドレス。

[Role Type]：このデバイスに割り当てられているロール。

Physical Device

デバイスを右クリックし、[Physical Device...] を選択すると、物理デバイスの [Properties] ウィンドウが表示されます。

物理プロパティ ウィンドウには、次の情報が表示されます。

[Name]：デバイスの名前。

[Description]：ユーザが入力したデバイスの説明。

[Collection Zone]：デバイス データの収集ゾーン。

[IP Address]：トポロジで使用されているインターフェイスの IP アドレス。

[User ID]：インターフェイスのユーザ ID。

[Enable User]：インターフェイスのパスワード。

[Device Access Protocol]：デバイスとの通信に使用されるプロトコル。

[Config Upload/Download]：コンフィギュレーション ファイルのアップロードおよびダウンロード方法。

[SNMP Version]：このデバイスの簡易ネットワーク管理プロトコル（SNMP）のバージョン。

[Community String RO]：[public] または [private]。

[Community String RW]：[public] または [private]。

[SNMP Security Level]：簡易ネットワーク管理プロトコル（SNMP）のセキュリティ レベル。

[Authentication User Name]：このデバイスで認証を行うユーザの名前。

[Authentication Algorithm]：認証の実行に使用されるアルゴリズム。

[Encryption Algorithm]：セキュアな通信に使用される暗号化アルゴリズム。

[Terminal Server]：ターミナル サーバの名前。

[Terminal Server Port]：ターミナル サーバにより使用されるポートの番号。

[Platform]：ハードウェア プラットフォーム。

[Software]：このデバイスに搭載されている IOS バージョン、またはその他の管理ソフトウェア。

[Image Name]：デバイス初期化用ブート イメージ。

[Serial Number]：デバイスのシリアル番号。

Interfaces

デバイスを右クリックし、[Interfaces...] を選択すると、インターフェイスの [Properties] ウィンドウが表示されます。

インターフェイス プロパティ ウィンドウには、次の情報が表示されます。

[Name]：デバイスの名前。

[IP Address]：デバイスの IP アドレス。

[IP Address Type]：[STATIC] または [DYNAMIC]。

[Encapsulation]：インターフェイス トラフィックで使用されるカプセル化。

[Description]：インターフェイスに割り当てられた説明（ある場合）。

[Select]（リンク）：接続がインターフェイスに付加されている場合、ウィンドウの下部にあるドロップダウン リストで、このデバイスで使用できるインターフェイスの中から選択できます。

Service Requests

デバイスを右クリックし、[Service Requests...] を選択すると、サービス要求の [Properties] ウィンドウが表示されます。

サービス要求プロパティ ウィンドウには、次の情報が表示されます。

[Job ID]：SR の ID。

[Type]：SR で使用されるプロトコルのタイプ。

[State]：SR の状態。

[Operation Type]：インターフェイス トラフィックで使用されるカプセル化。

[Creator]：インターフェイスに割り当てられた説明（ある場合）。

[Creation Time]：SR の作成日時。

[Customer Name]：SR に関連付けられているカスタマー名。

[Last Modified]：SR の最終変更日時。

[Description]：ユーザが入力した SR の説明。

[Select]（SR）：インターフェイスに複数の SR が関連付けられている場合、ウィンドウの下部にあるドロップダウン リストで、これらの SR の中から選択できます。

Link Properties

特定のリンクのプロパティを表示するには、目的のリンクを右クリックします。[Link Properties] メニューが表示されます。

次のオプションを使用できます。

[Expand]：全体的なトポロジには表示されていない、このリンクについてローカルなデバイスなど、リンクの詳細を表示します。

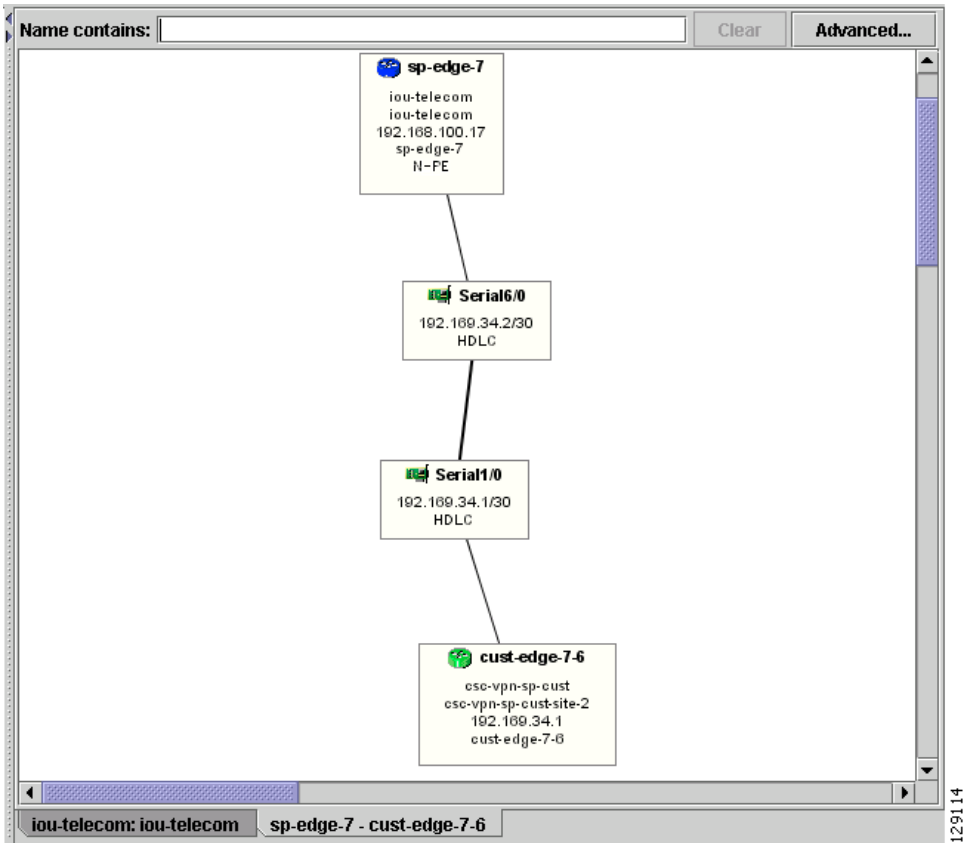
[Service Request...]：リンクに関連付けられたサービス要求プロパティを表示します。

[MPLS VPN]：リンクの MPLS VPN プロパティを表示します。MPLS VPN 以外のリンク プロトコル プロパティは現在使用できません。

Expand

リンクを右クリックして、[Expand...] を選択すると、トポロジ表示により、そのリンクについてローカルなデバイスと接続がすべて表示されます。図 12-13 に類似したリンク展開ウィンドウが表示されます。

図 12-13　　リンク展開ウィンドウ



デバイスおよびリンクのプロパティ情報は、この項で先に説明したとおり、マスター ビューでのみ入手可能です。

Service Request

リンクを右クリックし、[Service Requests...] を選択すると、サービス要求の [Properties] ウィンドウが表示されます。

サービス要求プロパティ ウィンドウには、次の情報が表示されます。

[Job ID]：SR の ID。

[Type]：SR で使用されるプロトコルのタイプ。

[State]：SR の状態。

[Operation Type]：インターフェイス トラフィックで使用されるカプセル化。

[Creator]：インターフェイスに割り当てられた説明（ある場合）。

[Creation Time]：SR の作成日時。

[Customer Name]：SR に関連付けられているカスタマー名。

[Last Modified]：SR の最終変更日時。

[Description]：ユーザが入力した SR の説明。

[Select]（SR）：インターフェイスに複数の SR が関連付けられている場合、ウィンドウの下部にあるドロップダウン リストで、これらの SR の中から選択できます。

MPLS VPN

MPLS VPN 用に設定されたリンクを右クリックし、[MPLS VPN...] を選択すると、MPLS VPN の [Properties] ウィンドウが表示されます。

サービス要求プロパティ ウィンドウには、次の情報が表示されます。

[Status]：MPLS VPN リンクのステータス。

[Status Message]：エラー メッセージ、または警告メッセージがあれば、すべて表示します。

[Operation Type]：MPLS 動作タイプ。

[Policy Type]：リンクに適用されるポリシー タイプ。

[Data MTD Threshold]：Memory Technology Driver（MTD）データしきい値。

[Default MTD Address]：デフォルト MTD の IP アドレス。

[Data MTD Subnet]：データ MTD のサブネット。

[Data MTD Size]：データ MTD のサイズ。

[SOO Enabled]：Site of Origin（SOO）のイネーブル化（[Yes] または [No]）

[Manual Config]：[Yes] または [No]。

フィルタリングと検索

大きなグラフでは、場合によっては詳細情報の量が非常に多くなります。このような場合、フィルタリングにより、必要のない情報を削除できます。一方、さらに詳しく調べたいデバイスをすばやく見つけるには、検索を行います。

高度なフィルタリングおよび検索の両方で、フィルタまたは検索されるノードに対する条件の入力に、同じウィンドウが使用されます。フィルタリング エリアでも、表示されているオブジェクトを名前ですばやくフィルタできます。

フィルタリング

トポロジ ビューのフィルタリングには、簡易フィルタリングと高度なフィルタリングの 2 通りがあります。

簡易フィルタリング

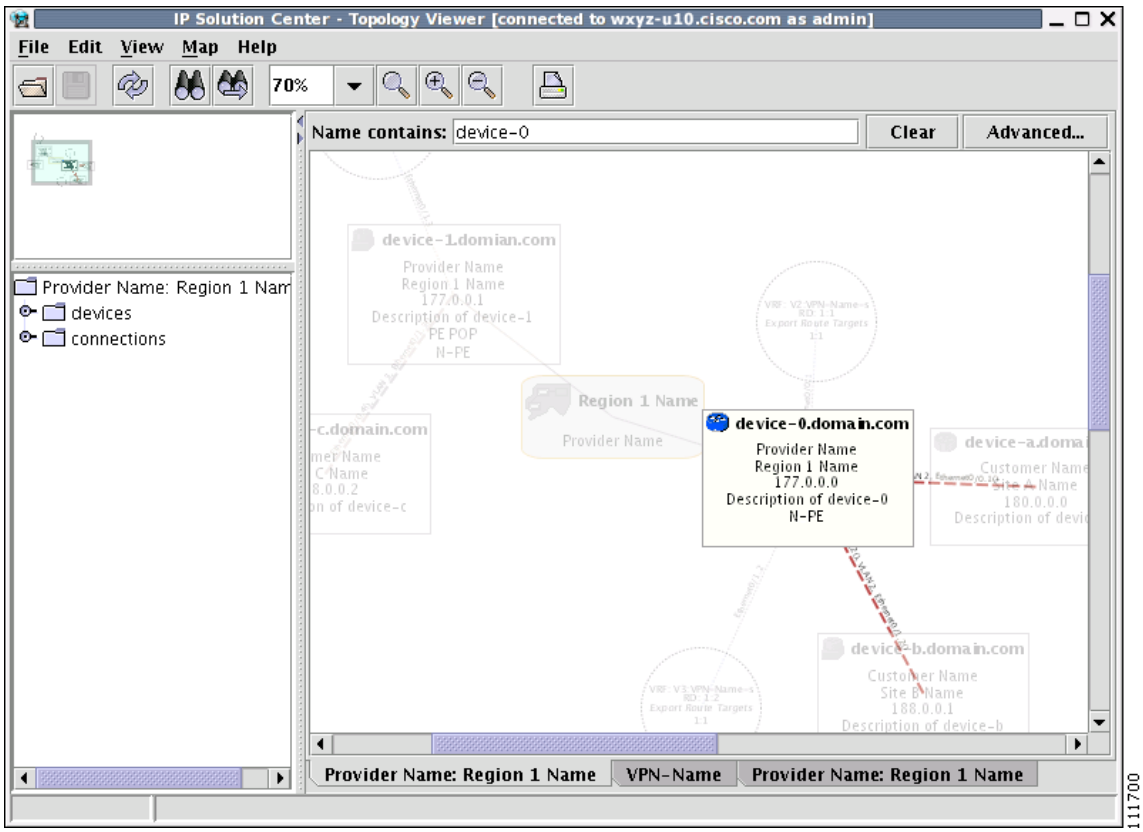
ビューの簡易フィルタリングを行うには、次のステップを実行します。

ステップ 1　メイン ウィンドウのエリア（4）に文字列を入力します（図 12-2 を参照）。

ステップ 2　Enter を押します。指定された文字列を含まない名前を持つオブジェクトがすべて淡色表示となります。

たとえば、名前に文字列「**router**」が含まれるノードを見つけるには、エリア（4）に「**router**」と入力し、Enter をクリックします。入力された文字列を含まない名前を持つオブジェクトはすべて淡色表示されます（図 12-14 を参照）。

図 12-14　物理ビューと淡色表示されたノード



（注）　正規表現もサポートされていますが、高度なフィルタリング ウィンドウでのみ使用できます（[Advanced...] ボタンをクリックします）。たとえば、「^foo.*a」と入力すると、先頭が「foo」で、その後に「a」を含む任意の文字列が続く名前を持つノードのみ要求されます。正規表現は、Java の正規表現で定義されているルールに従う必要があります。

高度なフィルタリング

高度なフィルタリングのステップは、次のとおりです。

ステップ 1　[Advanced...] ボタンをクリックして、高度なフィルタリング ウィンドウを開きます。

[Advanced Filter] ウィンドウが表示されます。

ステップ 2　目的のフィルタリング方法を選択します。

このウィンドウでは、フィルタされるノードに対する条件を 1 つ以上、入力できます。1 つめのドロップダウン リストでは、フィルタリング実行の基準となる属性を指定します。2 つめのドロップダウン リストには、属性の値と、3 列目に入力されるテキストの照合方法を指定します。

ドロップダウン リストから選択できる照合モードは、次のとおりです。

- [contains]：デバイスから取得された属性値に指定された文字列が含まれていた場合、この属性値が選択されます。この文字列が属性値の先頭、末尾、または中に含まれていた場合、この照合は成功します。たとえば、パターンが「**cle**」である場合、[contains] モードでは、「**clean**」、「**nucleus**」、「**circle**」が一致します。
- [starts with]：属性値は指定された文字列で始まらなければなりません。たとえば、パターンが「**foot**」である場合、「**footwork**」は一致しますが、「**afoot**」は一致しません。
- [ends with]：これは [starts with] とは逆のケースで、指定された属性の値が指定されたパターンで終わっていた場合のみ、この属性はパターンに一致します。このモードでは、たとえば、パターン「**foot**」は「**afoot**」には一致しますが、「**footwork**」には一致しません。
- [doesn't contain]：このモードでは、指定されたパターンを含まない文字列のみ一致します。結果は [contains] モードの逆です。たとえば、このモードで「**cle**」を指定した場合、「**clean**」、「**nucleus**」、および「**circle**」は却下されますが、「**foot**」には「**cle**」が含まれていないため、一致します。
- [matches]：これは最も汎用的なモードで、必要なノードを定義する表現の全体または一部を指定できます。

[Match any conditions] または [Match all conditions] オプション ボタンのいずれかをクリックして、いずれかの条件が一致すればよいか、すべての条件が一致する必要があるかを指定できます。最初のケースでは、たとえば、名前に「**cisco**」が含まれ、管理 IP アドレスが「**204**」で終わるデバイスを検索できます。すべての条件が一致しなければならない場合、たとえば、指定された名前やプラットフォームを持つデバイスを検索できます。

条件行を追加するには [More]、既存の条件行を削除するには [Fewer] をクリックします。

デフォルトでは、すべての照合が、大文字、小文字を区別せずに実行されます。しかし、大文字と小文字を考慮しながら、より正確な照合を実行した方が都合がよいこともあります。そのためには、[Match case] チェックボックスをオンにします。

ステップ 3　[OK] をクリックして、フィルタリング プロセスを開始します。フィルタの状態を変更せずにウィンドウを非表示にするには、[Cancel] をクリックします。

すべての条件をクリアするには、[Clear] ボタンを使用します。[Clear] に続けて [OK] をクリックすると、すべてのフィルタを効果的に削除し、すべてのノードの明るさのレベルをデフォルトに戻すことができます。フィルタリングがアクティブである場合は、メイン ウィンドウのエリア（4）（図 12-2 を参照）で [Clear] をクリックしても同じ結果を得ることができます。

検索

検索はメニュー、またはツールバーを使用して行います。検索のステップは、次のとおりです。

ステップ 1　[Edit] メニューで [Find] を選択します。

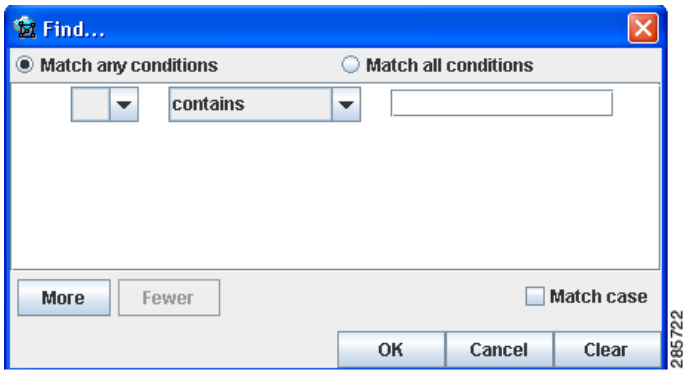
または

メイン ツールバーの [Find] アイコンをクリックします。

どちらの方法でも、同じウィンドウ（図 12-15 を参照）が表示されます。

ここでも、条件を 1 つ以上入力して、ノードを検索できます。

図 12-15　[Find] ウィンドウ



ステップ 2　目的のフィルタリング方法を選択します。

照合モード、大文字小文字の区別を指定するためのチェックボックス、オプション ボタンの使用方法については、「高度なフィルタリング」（P.12-21）を参照してください。

ステップ 3　[OK] をクリックします。指定された条件と一致する最初のノードの検索が開始されます。

見つかると、このノードがハイライトされ、そのときメイン ウィンドウに表示されているエリアに表示されるように、ビューの表示がずらされます。

ステップ 4　最初の検索後に F3 キーを押すか、[Find Again] ボタンをクリックすると、検索が繰り返されます。

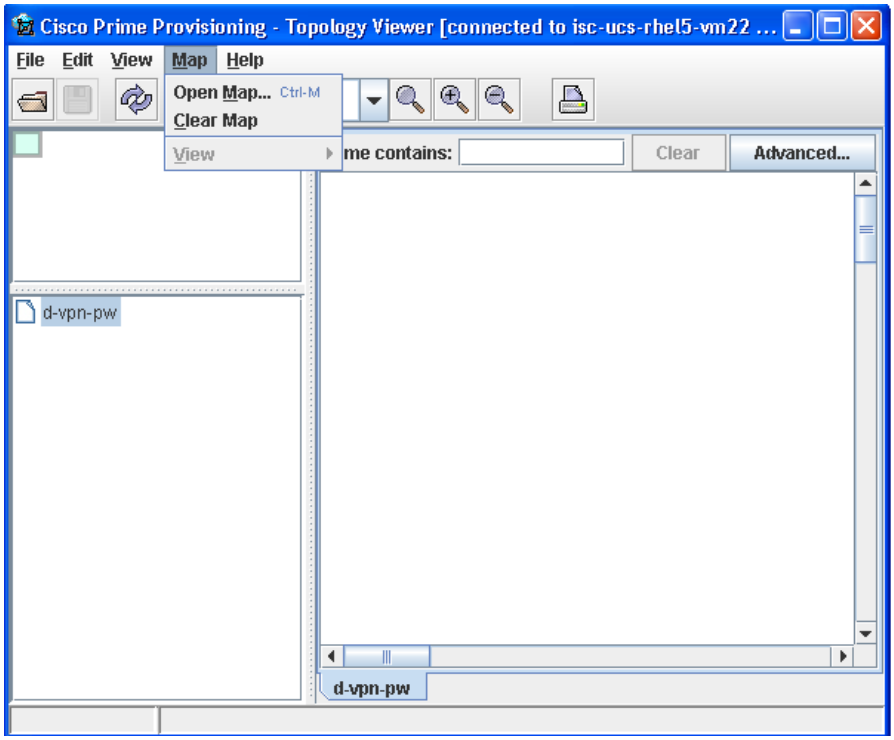
複数のノードが条件に一致する場合、[Find Again] 機能により、これらのノードが 1 つずつハイライトされます。入力した条件に一致するノードがない場合は、[Object Not Found] ウィンドウが表示されます。

マップの使用

各ビューには、マップを 1 つ関連付けることができます。現在、トポロジ ビューアでは、Environmental Systems Research Institute, Inc.（ESRI）のシェープ形式のマップのみサポートされています。以降の章では、マップをロードし、マップ レイヤと各マップに関連付けられているデータを選択的に表示する方法について説明します。

マップの機能を使用するには、[Map] メニュー（図 12-16 を参照）を使用します。

図 12-16　　[Map] メニュー



[Map] メニューには、次のメニュー項目が含まれます。

- [Open Map]：アプリケーションにマップをロードします。
- [Clear Map]：現在のビューからアクティブなマップをクリアします。
- [View]：マップにあるどのレイヤを表示するかを選択できます（例：国、都道府県、市町村）。

マップのロード

表示されたデバイスの物理的な位置を表示したバックグラウンド マップの設定が必要になることがあります。マップをロードするステップは、次のとおりです。

ステップ 1　メニュー バーで、[Map] > [Open Map...] を選択します。

または

Ctrl+M を押します。

ステップ 2　[Load Map] ウィンドウで必要な選択を行います。

ウィンドウの右側部分には、小さいコントロール パネルがあり、マップを表示する投影法を選択できます。マップの投影では、平面に球体がマップされます。一般的な投影法には、メルカトル、ランベルト、およびステレオ投影があります。

投影法の詳細については、次の場所にある、Eric Weisstein による「World of Mathematics」の「Map Projections」の項を参照してください。

http://mathworld.wolfram.com/topics/MapProjections.html

それぞれの投影について、表示されるマップのリージョンを選択することもできます。多くの場合、あらかじめ定義されている値で十分です。

必要に応じて、[Longitude Range] フィールドと [Latitude Range] フィールドの設定を変更します。

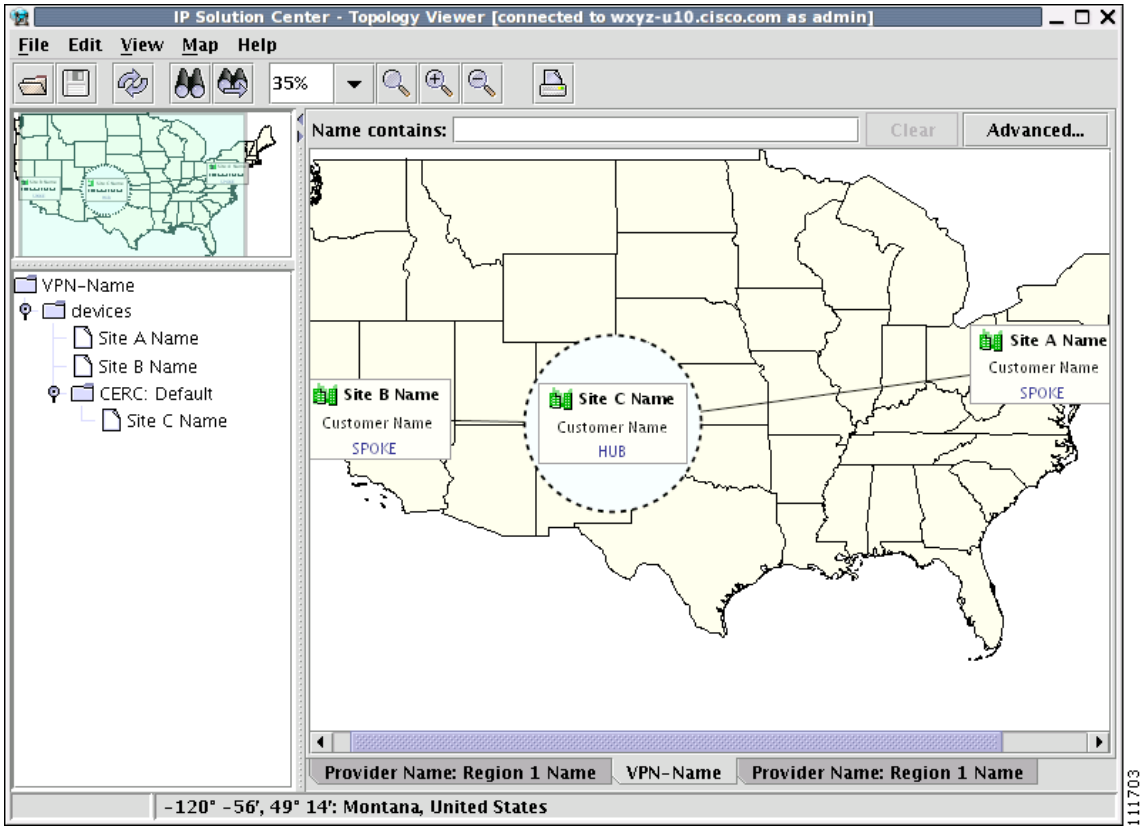
ステップ 3　マップ ファイルを選択し、[Open] をクリックして、マップをロードします。

マップ ファイルを選択し、[Open] ボタンをクリックすると、ファイルのロードが開始されます。マップは複数のコンポーネントから構成されることもあるため、進捗ウィンドウが開き、マップ ファイルのどの部分がロードされているかという情報が表示されます。

レイヤ

1 つのマップに複数のレイヤが含まれることがあります。たとえば、国土マップの大半には、図 12-17 に示すように、国レイヤ、地域レイヤ、市区町村レイヤがあります。

図 12-17　マップ レイヤ



マップのロード後、[Map] メニューの [View] サブメニューに自動的に項目が入力されます。使用可能な各レイヤの名前が、そのレイヤの可視性を示すチェックボックスとともに表示されます。特定のマップに現れる詳細が多すぎる場合は、レイヤのチェックボックスをオフにして、レイヤの一部またはすべてが表示されないようにできます。同じサブメニューを使って、レイヤを再表示できます。

誤ったマップがロードされた場合、またはマップがロードされているときのトポロジ ツールのパフォーマンスに満足できない場合は、マップ全体をクリアします。そのためには、[Map] メニューから [Clear Map] を選択します。このマップは、別のマップをロードすると自動的にクリアされます。

したがって、単に別のマップをロードするだけの場合は、既存のマップをクリアする必要はありません。新しいマップをロードすれば同じ結果が得られます。

マップ データ

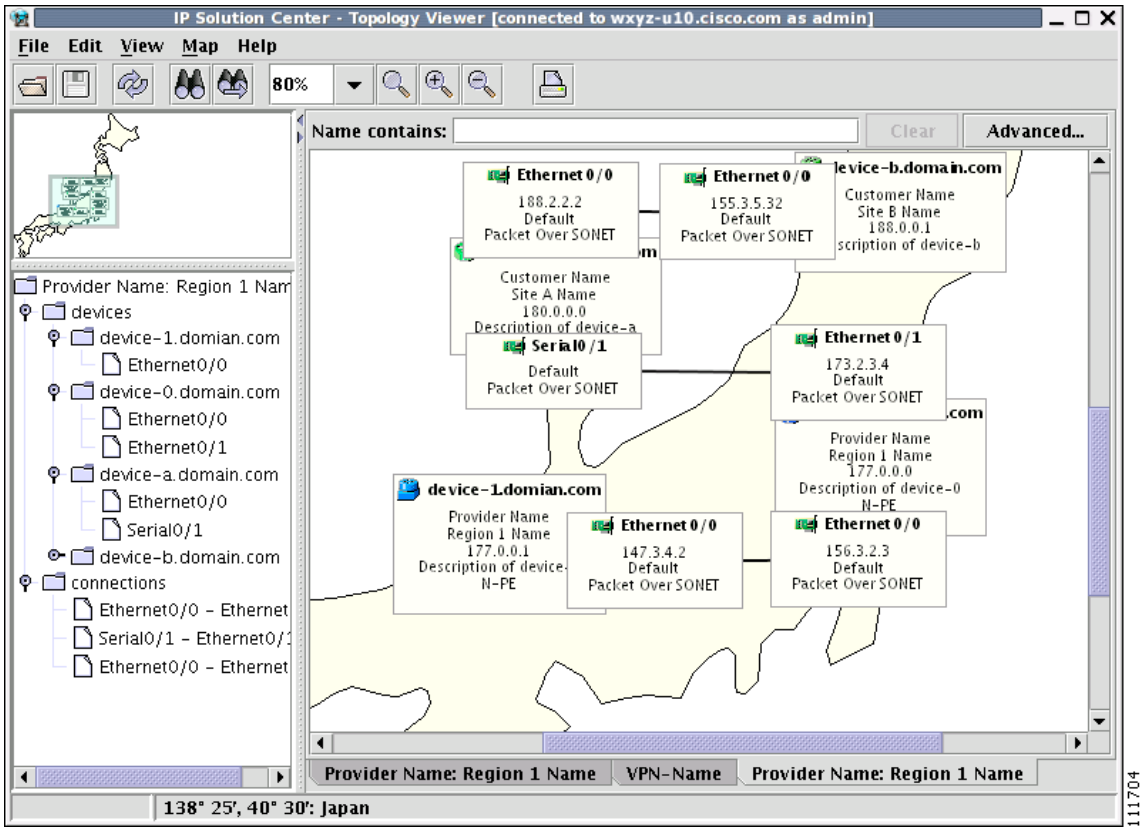
マップとともに、マップ データ ファイルのロードが正常に終了すると、ステータス バーの右側のフィールドに、マップ上でカーソルがある位置の緯度と経度が表示されます。都市、湖などのマップ オブジェクトにデータが関連付けられている場合、緯度と経度の座標に続けて、その名前が表示されます。

ノードの位置

マップのロードが正常終了すると、図 12-18 に示すとおり、マップ全体が表示されるように、ビューエリアが調整されます。ウィンドウに表示されるノードに緯度および経度の情報が関連付けられている場合、ノードは、マップ上でその地理的な場所に対応する位置に移動します。関連付けられていない場合、位置は変わりません。

ただし、目的の位置に手動で移動して、将来参照するために、この位置を保存できます。次にこのネットワークのイメージをロードしたときには、ノードの位置が復元され、マップ ファイルがロードされます。

図 12-18　日本のマップが表示された物理ビュー



新規マップの追加

マップの選択肢に独自のマップを追加して、トポロジ アプリケーションで使用することもできます。このためには、root ディレクトリにマップを保存します。この例を分かりやすく説明するために、クイーンズランド州の州都ブリスベンの郊外にあるトゥーウォンのマップを追加するとします。最初のステップとして、マップ ベンダーからマップを入手します。すべてのマップは ESRI シェープ ファイル形式でなければなりません（詳細は、Web サイト http://www.esri.com で説明されています）。また、各シェープ ファイルにデータ ファイルが付属することもあります。データ ファイルには、シェープ ファイルに含まれているシェープを持つオブジェクトに関する情報が含まれます。ベンダーが次の 4 つのファイルを提供しているとします。

- toowong_city.shp
- toowong_city.dbf
- toowong_street.shp
- toowong_street.dbf

ここで、トポロジ アプリケーションにマップのレイヤに関する情報を伝えるマップ ファイルを作成するとします。この例では、City と Street という 2 つのレイヤがあります。マップ ファイル（たとえば、Toowong.map）は、次のような内容になります。

```
toowong_city
toowong_street
```

このファイルには、トゥーウォンのマップを構成するレイヤがすべてリストされます。最初のファイルがバックグラウンド レイヤになり、他のレイヤは先行するレイヤの上に配置されるため、順序が重要です。

シェープ ファイルとデータ ファイルを取得し、マップ ファイルを書き込んだら、その位置を決定します。前述のとおり、トゥーウォンはオーストラリアのクイーンズランド州にあるブリスベンの郊外にある都市です。マップ ファイルはすべて、**$PRIMEP_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** ディレクトリの中、またはこの下になければなりません。デフォルトでは、このディレクトリはその地域のマップすべてを対象とした **Oceania** というディレクトリに含まれていますから、**Oceania** ディレクトリの下に **Australia/Queensland/Brisbane** パスを作成します。次に、この場所に 5 つのファイルをすべて配置します。これが終了すると、自動的にトポロジ ビューアからこのマップにアクセスできるようになります。

CHAPTER 13

インベントリ マネージャの使用

この章では、インベントリ マネージャを使用して、Prime Provisioning プロビジョニング プロセスでインベントリおよびサービス モデル データへの多数の変更を管理する方法について説明します。このプロセスでは、インベントリ マネージャにより、オペレータはネットワーク固有のデータを Prime Provisioning リポジトリ（以降、リポジトリといいます）にバルク モードでインポートできます。Prime Provisioning では、Prime Network からのインベントリのインポートがサポートされるようになりました。インポートできるインベントリは、デバイス クレデンシャル、ソフトウェア バージョン、および SNMP の詳細です。他のすべての物理的および論理的インベントリは、収集設定を使用してデバイスから取得されます。次の事項について説明します。

- 「[Inventory] - [Device Console]」（P.13-1）
- 「Prime Network デバイスのインポート」（P.13-12）

[Inventory] - [Device Console]

[Inventory] - [Device Console] は多数の操作の開始ポイントです。インベントリ マネージャは、主に次の 3 つの機能を実行します。

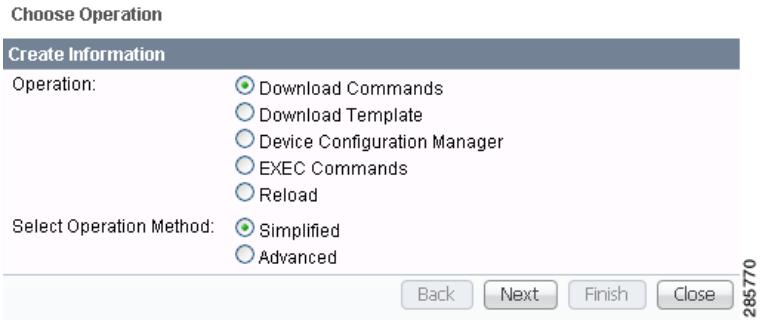
- コンフィギュレーション ファイルからデバイスをインポートし、カスタマーまたはプロバイダーのデバイスにアクセスすることで CPE および PE を設定します。
- Prime Provisioning リポジトリに保存されているデバイス、CPE、または PE を編集します。
- デバイスをプロバイダーまたはカスタマーに割り当てます。

デバイス コンソールに移動するには、次のステップを実行します。

ステップ 1 [Inventory] > [Device Tools] > [Device Console] を選択します。図 13-1 の例に示されているウィンドウが表示されます。

（注） 図 13-1 では、直前に選択されたオプション ボタンが示されています。

図 13-1　[Device Console] ウィンドウ



ステップ 2　いずれかの操作を選択するには、次の選択肢のいずれかに対応するオプション ボタンをクリックし、[Next] をクリックします。

（注）　すべての操作は、ECHO モード *ではなく*、Live モードのみに適用されます。

- 「Download Commands」（P.13-2）：操作コマンドおよびコンフィグレットをダウンロードします。[Simplified] と [Advanced (via wizard)] が含まれる [Select Operation Method] 選択肢は、[Download Commands] に対してのみ使用できます。これらについては、該当する項で説明します。
- 「テンプレートのダウンロード」（P.13-3）：テンプレート コンフィグレットを指定したデバイスにダウンロードします。
- 「Device Configuration Manager」（P.13-6）：タイムスタンプごとにリポジトリに作成されたコンフィギュレーション ファイルの各バージョンを表示し、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションに書き込みを行います。
- 「EXEC コマンド」（P.13-8）：イネーブル モードで実行できる任意の Cisco IOS コマンドをターゲット デバイスに送信できます。
- 「Reload」（P.13-10）：リモートでデバイスをリロードします。

Download Commands

コマンドをダウンロードするには、次の手順を実行します。

ステップ 1　[Inventory] > [Device Tools] > [Device Console] > [Download Commands] を選択します。

ステップ 2　[Select Operation Method] のデフォルトは [Simplified] で、この場合、単一のウィンドウ内に、デバイス、デバイス グループ、および操作コマンドを選択するためのオプションが表示されます。複数回クリックする必要はありません。単一のウィンドウ内で、必要なパラメータを送信してタスクを完了できます。[Advanced (via wizard)] では、複数のウィンドウに移動してタスクを実行する必要があります。この方法では、デバイスを選択し、[Next] をクリックし、デバイス グループを選択し、[Next] をクリックし、操作コマンドを選択します。これにより概要が示されます。

ステップ 3　[Next] をクリックします。

図 13-2 に示されているウィンドウが表示されます。

図 13-2　[Device Console] — [Download Commands] : [Select Devices]

ステップ 4　[Devices] 行で、[Select/Deselect] をクリックします。新しいウィンドウで、目的の各デバイスのチェックボックスをオンにします。対象デバイスが目的のデバイスではない場合は、チェックボックスをオフにします。次に、[Select] をクリックします。図 13-2 が再表示され、選択したデバイスが [Devices] 行に表示されます。

ステップ 5　[Groups] 行で、[Select/Deselect] をクリックします。次のウィンドウで、目的の各グループのチェックボックスをオンにします。対象グループが目的のグループではない場合は、チェックボックスをオフにします。次に、[Select] をクリックします。選択したグループが [Groups] 列に表示されます。

ステップ 6　[Operation Commands] フィールドに、ダウンロードするコマンドを入力するか、[Load File] をクリックして、[Operation Commands] フィールドに入力するコマンドのセットを選択します。

[Upload Config After Download] チェックボックスがオフのままの場合、ダウンロード後にコンフィギュレーション ファイルはアップロード*されません*。

[Retrieve device attributes] チェックボックスがオフのままの場合、デバイス属性は取得されません。[Retrieve device attributes] チェックボックスをオンにすると、テンプレートがダウンロードされた後に、SNMP を使用してインターフェイス情報を取得し、**show version** などの追加 **show** コマンドを発行します。

ステップ 7　[OK] をクリックしてダウンロードをサブミットすると、[Device Console Operation Result] と、左下の隅に [Status] が表示されたウィンドウが表示されます。[Download] または [Done] をクリックできます。

ステップ 8　[Download] をクリックすると、ステップ 6 に戻り、選択したデバイスに追加コマンドがダウンロードされます。

ステップ 9　[Done] をクリックし、図 13-1 に戻ります。

テンプレートのダウンロード

（注）　異なるテンプレートに属する複数のデータ ファイルをデバイス コンソールを介してダウンロードすることはできません。

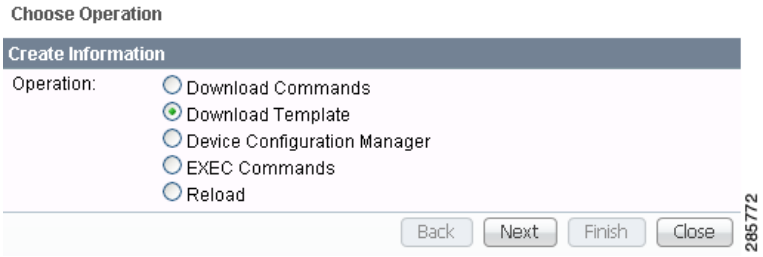
テンプレートをダウンロードするには、次の手順を実行します。

ステップ 1　[Inventory] > [Device Tools] > [Device Console] を選択します。

ステップ 2　[Download Template] を選択し、[Next] をクリックします。

図 13-3 に示されているウィンドウが表示されます。

図 13-3　デバイス コンソール — [Download Template]：デバイスの選択



ステップ 3　デバイスを追加する場合は、引き続きステップ 4 を実行します。デバイスを削除する場合は、ステップ 9 に進みます。または、[Next] をクリックして ステップ 11 の「**3. Select Device Groups**」に進みます。

ステップ 4　図 13-3 に示されているように [Add] をクリックして、「**2. Select Devices**」に進みます。

ステップ 5　表示される [Device Selection] ウィンドウで、選択する各デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 6　デバイスが追加された状態で、図 13-3 に戻ります。

ステップ 7　各デバイスに対して、追加された [Clear] ボタンをクリックして [Upload to Customer/Site] 列をクリアし、[none selected] を反映するか、追加された [Select] ボタンをクリックして新しいウィンドウを使用し、[Create Customer]、[Create Site]、[Select]、または [Cancel] を行えます。この新しいウィンドウの [Select] をクリックすると、カスタマーまたはサイトが追加された状態で 図 13-3 に戻ります。

ステップ 8　ステップ 4 からステップ 7 を繰り返して、さらにデバイスを**追加**したり、ステップ 9 に説明されているようにデバイスを削除したり、ステップ 10 に進んで続行したりすることができます。

ステップ 9　デバイスを削除するには、削除するデバイスのチェックボックスを 1 つ以上オンにし、[Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 10　必要なすべてのデバイスを選択した後、[Next] をクリックします。ステップ 11 から始まる「**3. Select Device Groups**」に進みます。

ステップ 11　デバイス グループを追加する場合は、引き続きステップ 12 を実行します。デバイス グループを削除する場合は、ステップ 14 に進みます。または、[Next] をクリックして ステップ 16 の「**4. Enter Download Commands**」に進みます。

ステップ 12　図 13-4 に示されているように [Add] をクリックして、「**3. Select Device Groups**」に進みます。デバイス グループの追加は任意です。

図 13-4　デバイス グループの選択

ステップ 13　表示されるウィンドウで、選択する各デバイス グループのチェックボックスをオンにします。次に、[Select] をクリックします。

デバイス グループが追加された状態で、図 13-4 に戻ります。ステップ 12 からステップ 13 を繰り返してその他のデバイス グループを**追加**すること、ステップ 14 の説明に従いデバイス グループを削除すること、またはステップ 15 に進んで続行できます。

ステップ 14　デバイス グループを削除するには、削除するデバイスのチェックボックスを 1 つ以上オンにし、[Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 15　必要なすべてのデバイス グループを選択した後、[Next] をクリックします。ステップ 16 から始まる「**4. Select Download Template**」に進みます。

ステップ 16　「**4. Select Download Template**」の結果ウィンドウを図 13-5 に示します。

図 13-5　ダウンロード テンプレートの選択

ステップ 17　図 13-5 で、[Select] ボタンをクリックできます。

図 13-6 に示されているウィンドウが表示されます。

ステップ 18　[Add] をクリックしてテンプレートを追加するか、[Remove] をクリックしてテンプレートを削除します。必要なテンプレートを選択した後、[OK] をクリックします。

[Add] をクリックすると、ツリー形式のテンプレート選択肢を含む [Template Datafile Chooser] ウィンドウが表示されます。選択するプロパティが表示されるまで、+ をクリックしてツリー内のフォルダとサブフォルダを開きます。目的のプロパティをクリックすると、リストに追加されます。必要なテンプレートがすべてリストに追加されるまで、この操作を繰り返します。追加された各プロパティで、[View] をクリックしてそのデータ ファイルのコンフィグレットを受け取ることができます。戻るには、[OK] をクリックします。図 13-6 で、必要なテンプレートのチェックボックスをオンにします。各テンプレートの行で、[Action] ドロップダウン リストをクリックして、[APPEND] または [PREPEND] を選択し、後ろまたは後に情報を追加します。次に、[Active] チェックボックスをオンまたはオフにして [OK] をクリックします。

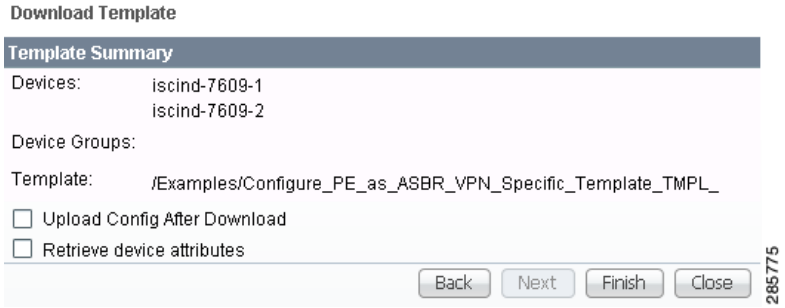
図 13-6　テンプレートの追加または削除

ステップ 19　情報が更新された状態で、図 13-5 に戻ります。

ステップ 20　[Next] をクリックすると、ステップ 21 に説明されているように、「**5. Download Template Summary**」に進みます。

ステップ 21　「**5. Download Commands Summary**」では、図 13-7 に示されているウィンドウが表示されます。

図 13-7　　ダウンロード テンプレートの概要



ステップ 22　図 13-7 で、[Upload Config After Download] チェックボックスがオフのままの場合、ダウンロード後にコンフィギュレーション ファイルはアップロード*されません*。[Upload Config After Download] チェックボックスをオンにすると、でテンプレートをダウンロードした後に、新しいコンフィギュレーション ファイルをアップロードします。[Retrieve device attributes] チェックボックスがオフのままの場合、デバイス属性は取得されません。[Retrieve device attributes] チェックボックスをオンにすると、テンプレートがダウンロードされた後に、SNMP を使用してインターフェイス情報を取得し、**show version** などの追加 **show** コマンドを発行します。

ステップ 23　変更する情報がすべて修正されるまで [Back] をクリックするか、[Finish] をクリックしてダウンロードをサブミットすると、[Download Template Results] と、左下の隅に [Succeeded] を示す緑色のチェックマークが付いた [Status] が表示されたウィンドウが表示されます。

ステップ 24　[Done] をクリックし、図 13-1 に戻ります。

Device Configuration Manager

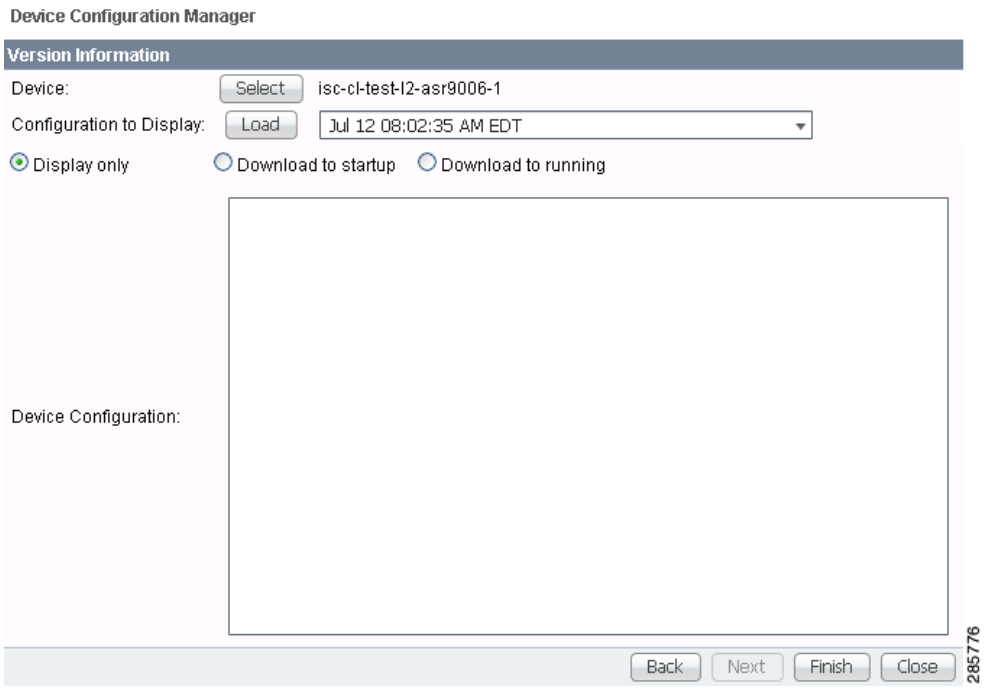
コンフィギュレーションを表示するために、デバイスのスタートアップ コンフィギュレーションにコンフィギュレーションをダウンロードするか、デバイスの実行中のコンフィギュレーションにコンフィギュレーションをダウンロードするには、次の手順を実行します。

ステップ 1　[Inventory] > [Device Tools] > [Device Console] を選択します。

ステップ 2　[Device Configuration Manager] を選択し、[Next] をクリックします。

図 13-8 に示されているウィンドウが表示されます。

図 13-8　Device Configuration Manager



ステップ 3　[Device] 行で、[Select] をクリックします。

ステップ 4　リストされたデバイスから、選択するデバイスのオプション ボタンをクリックします。次に、[Select] をクリックします。

ステップ 5　デバイスが追加された状態で、図 13-8 に戻ります。ステップ 3 からステップ 4 を繰り返して、デバイスを変更できます。

ステップ 6　必要なデバイスを選択したら、[Configuration to Display] 行に移動して、[Select a Version...] ドロップダウン リストをクリックします。必要なバージョンをクリックしてから、[Load] をクリックしてそのコンフィギュレーション ファイルをロードします。

ステップ 7　次のいずれかのオプション ボタンをクリックするか、またはデフォルトをそのまま使用します。

- [Display only]：コンフィギュレーション ファイルの表示のみ可能です。
- [Download to startup]：コンフィギュレーション ファイルは選択したルータのスタートアップ コンフィギュレーションにダウンロードされます。

（注）　[Download to startup] では、（デバイス作成で定義される）デバイス アクセス プロトコルは **ftp** または **tftp** である必要があります。これら以外の場合、[Device Configuration Manager Results] ウィンドウが表示され、**ftp** または **tftp** を設定する必要があることが示されます。Appendix B, “Property Settings” で、FTP と TFTP の両方について DCS の Dynamic Component Properties Library（DCPL）プロパティを指定します。

- [Download to running]：コンフィギュレーション ファイルはルータの実行中のコンフィギュレーション ファイルにダウンロードされます。

（注）　**GTL/ios** フォルダ内の DCPL プロパティ **copy-running-to-startup** が **true** に設定されている場合、ルータの実行中のコンフィギュレーション ファイルもスタートアップ コンフィギュレーションにコピーされます。

ステップ 8　[Finish] をクリックします。ステップ 7 で [Display only] を選択した場合、図 13-1 に自動的に戻ります。ステップ 7 で、[Download to startup] または [Download to running] をクリックすると、[Device Configuration Manager Results] ウィンドウが表示されます。[Status] ボックスで、[Succeeded] を示す緑色のチェックマークまたは赤色の [Failed] ステータスを受け取り、[Done] をクリックして図 13-1 に戻る必要があります。

EXEC コマンド

[EXEC Commands] を使用すると、イネーブル モードで実行できる任意の Cisco IOS コマンドをターゲット デバイスに送信できます。ルータ情報のみを表示できます。情報を編集または削除することはできません。

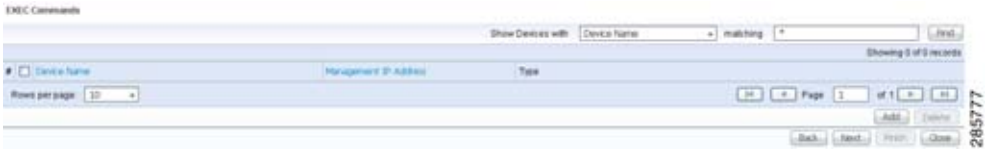
EXEC コマンドを実行するには、次の手順を実行します。

ステップ 1　[Inventory] > [Device Tools] > [Device Console] を選択します。

ステップ 2　[EXEC Commands] を選択し、[Next] をクリックします。

図 13-9 に示されているウィンドウが表示されます。

図 13-9　[Device Console] — [EXEC Commands]:[Select Devices]



ステップ 3　デバイスを追加する場合は、引き続きステップ 4 を実行します。デバイスを削除する場合は、ステップ 7 に進みます。または、[Next] をクリックして ステップ 9 の「**3. Select Device Groups**」に進みます。

ステップ 4　図 13-9 に示されているように [Add] をクリックして、「**2. Select Devices**」に進みます。

ステップ 5　表示されるウィンドウで、選択する各デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 6　デバイスが追加された状態で、図 13-9 に戻ります。ステップ 4 からステップ 5 を繰り返して、さらにデバイスを**追加**したり、ステップ 7 に説明されているようにデバイスを削除したり、ステップ 8 に進んで続行したりすることができます。

ステップ 7　デバイス グループを削除するには、削除するデバイスのチェックボックスを 1 つ以上オンにし、図 13-9 の [Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 8　必要なすべてのデバイスを選択した後、[Next] をクリックします。

ステップ 9 から始まる「**3. Select Device Groups**」に進みます。

ステップ 9　デバイス グループを追加する場合は、引き続きステップ 10 を実行します。デバイス グループを削除する場合は、ステップ 13 に進みます。または、[Next] をクリックして ステップ 15 の「**4. Enter EXEC Commands**」に進みます。

ステップ 10　図 13-10 に示されているように [Add] をクリックして、「**3. Select Device Groups**」に進みます。

図 13-10　　デバイス グループの選択

ステップ 11　表示されるウィンドウで、選択する各デバイス グループのチェックボックスをオンにします。次に、[Select] をクリックします。

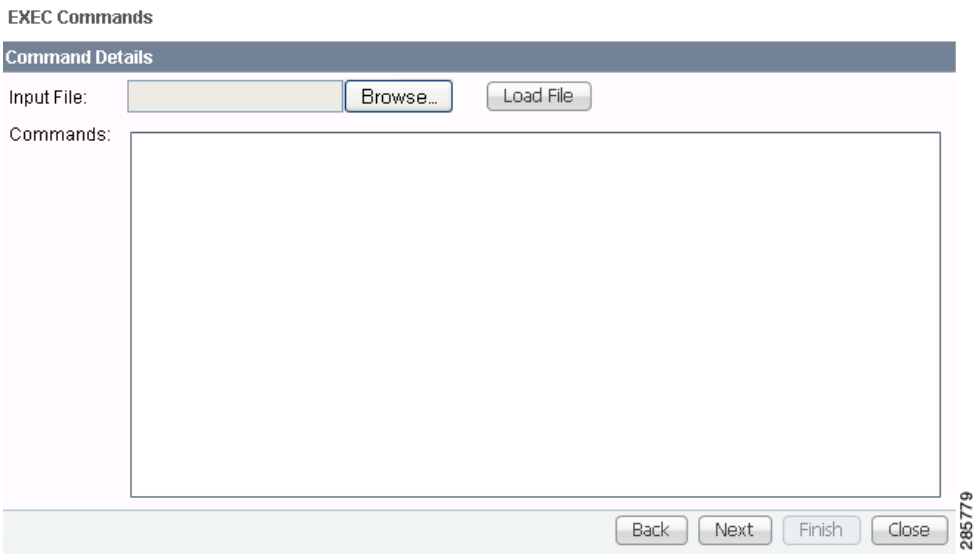
ステップ 12　デバイス グループが追加された状態で、図 13-10 に戻ります。ステップ 10 からステップ 11 を繰り返してその他のデバイス グループを**追加**すること、ステップ 13 の説明に従いデバイス グループを削除すること、またはステップ 14 に進んで続行できます。

ステップ 13　デバイス グループを削除するには、削除するデバイスのチェックボックスを 1 つ以上オンにし、[Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 14　必要なすべてのデバイス グループを選択した後、[Next] をクリックします。ステップ 15 から始まる「**4. Enter EXEC Commands**」に進みます。

ステップ 15　「**4. Enter EXEC Commands**」の結果ウィンドウを図 13-11 に示します。

図 13-11　　操作コマンド



ステップ 16　図 13-11 では、[Browse] ボタンをクリックして、Cisco IOS コンフィギュレーション コマンドとともに既存のファイルを入力できます。次に [Load File] ボタンをクリックして、ファイルの情報を [Commands] フィールドに入力します。または、Cisco IOS コンフィギュレーション コマンドを [Commands] フィールドに直接入力できます。

ステップ 17　[Next] をクリックすると、ステップ 18 に説明されているように、「**5. EXEC Commands Summary**」に進みます。

ステップ 18　「**5. EXEC Commands Summary**」では、図 13-12 に示されているウィンドウが表示されます。

図 13-12　EXEC コマンドの概要

ステップ 19　変更する情報がすべて修正されるまで [Back] をクリックするか、[Finish] をクリックしてルータから情報を取得します。その後、[EXEC Commands Results] と、[Succeeded] を示す緑色のチェックマークが付いた [Status] が含まれたウィンドウが表示されます。[EXEC] または [Done] をクリックできます。

ステップ 20　[EXEC] をクリックすると、ステップ 15 に戻り、選択したデバイスに追加コマンドが入力されます。

ステップ 21　[Done] をクリックし、図 13-1 に戻ります。

Reload

ルータをリロード（再起動）するには、次の手順を実行します。

ステップ 1　[Inventory] > [Device Tools] > [Device Console] を選択します。

ステップ 2　[Reload] を選択し、[Next] をクリックします。

図 13-13 に示されているウィンドウが表示されます。

図 13-13　[Device Console] — [Reload]:[Select Devices]

ステップ 3　デバイスを追加する場合は、引き続きステップ 4 を実行します。デバイスを削除する場合は、ステップ 7 に進みます。または、[Next] をクリックして ステップ 9 の「**3. Select Device Groups**」に進みます。

ステップ 4　図 13-13 に示されているように [Add] をクリックして、「**2. Select Devices**」に進みます。

ステップ 5　表示されるウィンドウで、選択する各デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 6　デバイスが追加された状態で、図 13-13 に戻ります。ステップ 4 からステップ 5 を繰り返して、さらにデバイスを**追加**したり、ステップ 7 に説明されているようにデバイスを削除したり、ステップ 8 に進んで続行したりします。

ステップ 7　デバイスを削除するには、削除するデバイスのチェックボックスを 1 つ以上オンにし、[Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 8　必要なすべてのデバイスを選択した後、[Next] をクリックします。ステップ 9 から始まる「**3. Select Device Groups**」に進みます。

ステップ 9　デバイス グループを追加する場合は、引き続きステップ 10 を実行します。デバイス グループを削除する場合は、ステップ 13 に進みます。または、[Next] をクリックして ステップ 15 の「**4. Reload Devices Summary**」に進みます。

ステップ 10　図 13-14 に示されているように [Add] をクリックして、「**3. Select Device Groups**」に進みます。

図 13-14　　デバイス グループの選択

ステップ 11　表示されるウィンドウで、選択する各デバイス グループのチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 12　デバイス グループが追加された状態で、図 13-14 に戻ります。ステップ 10 からステップ 11 を繰り返して、さらにデバイス グループを**追加**したり、ステップ 13 に説明されているようにデバイス グループを削除したり、ステップ 15 に進んで続行したりします。

ステップ 13　デバイス グループを削除するには、図 13-14 で削除するデバイスのチェックボックスを 1 つ以上オンにし、[Delete] をクリックします。この削除を確認する機会はないため、慎重に選択してください。

ステップ 14　必要なすべてのデバイス グループを選択した後、[Next] をクリックします。ステップ 15 から始まる「**4. Reload Devices Summary**」に進みます。

ステップ 15　「**4. Reload Devices Summary**」では、図 13-15 に示されているウィンドウが表示されます。

図 13-15　　リロードの概要

ステップ 16　変更する情報がすべて修正されるまで [Back] をクリックするか、[Finish] をクリックしてリロードをサブミットすると、[Reload Results] と、[Succeeded] を示す緑色のチェックマークが付いた [Status] が表示されたウィンドウが表示されます。

ステップ 17　[Finish] をクリックして、図 13-1 に戻ります。

Prime Network デバイスのインポート

Prime Provisioning では、Prime Network からのインベントリのインポートがサポートされるようになりました。インポートできるインベントリは、デバイス クレデンシャル、ソフトウェア バージョン、および SNMP の詳細です。他のすべての物理的および論理的インベントリは、収集設定を使用してデバイスから取得されます。Prime Network デバイスをインポートする前に、**InventoryImport** から DCPL プロパティを設定します。DCPL プロパティの設定の詳細については、*『Cisco Prime Provisioning Administrator’s Guide 6.3』* を参照してください。

（注）　この設定は、ネットワークに新たに追加されたデバイスごとに必要です。

この機能を使用して次の作業を実行できます。

- Prime Network からのデバイスのインポート
- 自動化されたリング検出プロセス
- 統合された単一の画面でのカスタマー デバイスの挿入
- Prime Network からの一括インポートの拡張インベントリ マネージャ

N-PE、U-PE、または PE-AGG として機能する Cisco IOS ルータは、Prime Provisioning が情報を収集するデバイスとして定義されます。Prime Provisioning が管理するすべてのネットワーク要素は、システム内でデバイスとして定義されます。

次の 2 通りの方法で、Prime Network からデバイスをインポートできます。

- 「デバイスの作成中の単一デバイスのインポート」（P.13-12）
- 「インベントリ マネージャを使用したバルク インポート」（P.13-13）
- 「Prime Provisioning トラスト ストアへの Prime Network 証明書のインポート」（P.13-14）

デバイスの作成中の単一デバイスのインポート

[Devices] 内をナビゲーションし、手動でデバイスをインポートするには、次の手順を実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device List] ウィンドウが表示されます。[Create] ボタンをクリックします。

ステップ 2　ドロップダウン メニューから [Cisco Device] を選択します。

[Create Cisco Device] ウィンドウが表示されます。

フィールドの説明については、次の項を参照してください。

- 「一般属性」（P.2-7）
- 「ログインとパスワードの属性」（P.2-9）
- 「[Device and Configuration Access Information] の属性」（P.2-9）
- 「[SNMP v1/v2c] の属性」（P.2-10）

ステップ 3　[Roles] セクションの下にあるドロップダウン メニューから、デバイス タイプとして [Customer Device] または [Provider Device] を選択します。

作成しているプロバイダーのリージョン名を入力します。プロバイダーのリージョン名を入力するには、次の手順を実行します。

a. [Provider Region Name] の横にある [Select] ボタンをクリックします。

プロバイダー リージョン名のリストが表示されます。

b. プロバイダー リージョン名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

[Role Type] ドロップダウン メニューからデバイス ロールを選択します。

（注）　[Provider Region Name] と [PE Role Type] オプションは、デバイス タイプとして [Provider Device] を選択した場合にのみイネーブルになります。

ステップ 4　[Config Collect] の横にあるチェックボックスをオンにして、デバイスの保存中にコンフィギュレーションの収集を行います。

コンフィギュレーションの収集は、デバイスの作成およびデバイスのインポートの段階で行われます。または、[Operate] > [Task Manager] > [Task] とナビゲートして、コンフィギュレーション タスクを作成し、作成したデバイスを選択します。

ステップ 5　[Ring Discovery] の横にあるチェックボックスをオンにして、デバイスの保存中にリング収集を行います。REP リングに関連付けられたデバイスは Active Network Abstration（ANA）から検出され、Prime Provisioning にインポートされます。リングの検出タスクは、次から実行できます。

- [Device Creation] ウィンドウ
- [Inventory Manager] ウィンドウ

ステップ 6　[MPLS-TP Discovery] および [MPLS Label Sync] の横にあるチェックボックスをオンにして、これらの詳細にアクセスします。

ステップ 7　[Create Cisco Device] の [Additional Properties] セクションにアクセスするには、[Show] をクリックします。

[Additional Properties] ウィンドウが表示されます。

[Additional Properties] フィールドの説明については、次の項を参照してください。

- 「SNMP v3 属性」（P.2-10）
- 「[Terminal Server] オプションの属性」（P.2-11）
- 「[Device Platform Information] の属性」（P.2-11）

ステップ 8　作成しているターミナル サーバ デバイスに関する、必要な追加プロパティ情報を入力します。

ステップ 9　[Save] をクリックします。

ステップ 10　新たにインポートされたデバイスがリストされて、[Devices] ウィンドウが再表示されます。

インベントリ マネージャを使用したバルク インポート

[Inventory Manager] ウィンドウで使用可能なオプションを使用して、ANA にすでにあるデバイスを Prime Provisioning に直接インポートできます。

シスコ デバイスの一括インポートを実行するには、次の手順を実行します。

ステップ 1　[Inventory] > [Physical Inventory] > [Inventory Manager] を選択します。

[Device List] ウィンドウが表示されます。

ステップ 2　[Import Devices] ボタンをクリックします。[ANA] を選択します。

ステップ 3　[Inventory Import Filter] ウィンドウが表示されます。

a. Prime Provisioning にインポートする前に、ANA からのデバイスのインポートをフィルタリングできます。

- ANA で利用可能なデバイスは、[Device Host Name]、[Management IP Address]、[Element Management Key] および [Software Version] に基づいてフィルタリングできます。
- フィルタリングが完了すると、成功メッセージにフィルタ基準と一致するデバイスの検出数が表示されます。
- 基準と一致する、検出されたデバイスは [Inventory Manager] ウィンドウに表示されます。[Assign CE/PE] ボタンをクリックして、ロール割り当てなどの追加設定を行うことができます。
- デバイスを保存する前に、デバイスを選択し、[Edit] ボタンをクリックしてデバイス パラメータを変更します。
- [Save] ボタンをクリックして、デバイスを Prime Provisioning にインポートおよび保存します。

b. ANA で使用可能なすべてのデバイスをインポートする場合は、フィルタ画面でフィルタリング基準を何も指定せずに、[OK] ボタンをクリックします。

ステップ 4　[Device List] ウィンドウが表示されます。

ステップ 5　デバイスのインポート中に、[Config Collect] と [Ring Discovery] をスケジュールできます。[Action] ボタンをクリックして、次をスケジュールします。

- コンフィギュレーションの収集
- コンフィギュレーションの収集およびリングの検出
- リングの検出

ステップ 6　[Save] をクリックします。

新しいデバイスが追加された状態で、[Devices] ウィンドウが再表示されます。

Prime Provisioning トラスト ストアへの Prime Network 証明書のインポート

Prime Network 証明書のインポートを実行するには、次の手順を実行します。

ステップ 1　Prime Network サーバの詳細を Prime Provisioning に追加し、Prime Network サーバにログインします。

ステップ 2　`<Installation-Path>/ Main/resourcebundle/com/sheer` ディレクトリにナビゲートし、(`ls -alrt`) リスト コマンドを指定します。

（注）　ファイル .keystore & security.properties を使用できることを確認します。

ステップ 3　次のコマンドを使用して、サーバのキー ストア（.keystore）からサーバ証明書をエクスポートします。

```
keytool -export -alias ana -file <certificate-name>.cer -keystore <keystore-name>
```

```
<certificate-name> can be - sheer.cer (must end with .cer)
<keystore-name> must be - .keystore
Example: keytool -export -alias ana -file sheer.cer -keystore .keystore
```

ステップ 4　証明書（sheer.cer）を Prime Provisioning サーバのインストール ディレクトリ（<PRIMEP_INSTALLATTION-DIR>/etc/）などのディレクトリに転送（FTP）します。

ステップ 5　<PRIMEP_INSTALLATTION-DIR> ディレクトリから次のコマンドを実行して、環境設定情報を取得します。

```
./prime.sh shell
```

ステップ 6　キーツールによって、パスワードを求めるプロンプトが出されます。etc ディレクトリの security.properties ファイルに、パスワード <PRIMEP_INSTALLATTION-DIR>/etc/security.properties がないか、確認してください。

ステップ 7　<PRIMEP_INSTALLATTION-DIR>/etc/ ディレクトリから次のコマンドを実行して、証明書を Prime Provisioning キーストアにインポートします。

```
keytool -import -file <certificate-name>.cer -keystore <keystore-name> -alias
<alias-name>
<certificate-name> - must be the name of the Prime  Network certificate.
<keystore-name>  - must be prime.keystore
<alias-name> - unique name to identify the certificate.
Example: keytool -import -file sheer.cer -keystore prime.keystore -alias anacer
```

（注）　パスワードを確認するために、セキュリティをチェックにします。properties ファイルは <PRIMEP_INSTALLATTION-DIR>, etc ディレクトリにあります。

ステップ 8　コマンドの実行中に、証明書をインポートするためのキーツールの確認が行われます。

インポートするには、**Yes** を入力します。「Certificate was imported successfully」というメッセージが表示されます。

ステップ 9　証明書がインポートされたことを確認するには、キーストアに追加された信頼できる証明書をリストする次のコマンドを実行します。

```
keytool -list -v -keystore prime.keystore
```

サーバを再起動して、変更を反映させます。

APPENDIX A

Cisco Configuration Engine サーバ

（注） Cisco Configuration Engine サーバは、Prime Provisioning ユーザ インターフェイス全体を通して IE2100 と呼ばれています。Prime Provisioning 内で参照されている IE2100 アプライアンスは、Cisco Configuration Engine ソフトウェアを実行するように設定されているすべてのサーバを表します。このサーバは、2.0 以前のサポートされるすべてのソフトウェア バージョンの場合は IE2100 自体にし、2.0 以降のサポートされるすべてのソフトウェア バージョンの場合は Solaris ワークステーションにすることができます。

Prime Provisioning はデバイスからのコンフィギュレーション ファイルのアップロード、デバイスへのコンフィグレットのダウンロード、またはデバイスでのコマンドの実行と結果の取得など、何らかの Cisco IOS デバイスとの通信を行うために、Cisco CNS IE2100 Device Access Protocol をサポートします。Prime Provisioning は CNS Plug-and-Play もサポートします。

Prime Provisioning で Cisco CNS IE2100 の機能を使用するには、まず、Cisco CNS IE2100 アプライアンスと Prime Provisioning ワークステーションを、*『Cisco Prime Provisioning 6.3 Installation Guide』* の付録で説明されているようにセットアップする必要があります。

この付録は、次の項で構成されています。これらの項を順番に実装します。

（注） 「Plug-and-Play の使用」（P.A-4）は、オプションです。

1. 「Cisco CNS IE2100 アプライアンスの作成」（P.A-1）
2. 「Cisco CNS デバイス アクセス プロトコルを使用した Cisco IOS デバイスの作成」（P.A-2）
3. 「Plug-and-Play の使用」（P.A-4）

Cisco CNS IE2100 アプライアンスの作成

Prime Provisioning は、複数の Cisco CNS IE2100 アプライアンスをサポートします。Cisco CNS IE2100 アプライアンスを作成するには、次の手順を実行します。

（注） 詳細については、「デバイス」（P.2-1）を参照してください。第 2 章「Prime Provisioning を設定する前に」

ステップ 1 [Inventory] > [Physical Inventory] > [Devices] を選択します。

[Device] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

ステップ 3　[Create] メニューから、[IE2100] をクリックします。

[Create IE2100 Device] ウィンドウが表示されます。

ステップ 4　[Device Host Name] にデバイス ホスト名を入力し、該当する場合は IE2100 の [Device Domain Name] にデバイス ドメイン名を入力します。[Description] フィールドはオプションです。Cisco CNS IE2100 アプライアンスが DNS に登録されていない場合、Cisco CNS IE2100 アプライアンスの **IP アドレス**を入力する*必要があります*。[Save] をクリックします。

IE2100 がデバイスとしてリストされて、[Device] ウィンドウが再表示されます。

Cisco CNS デバイス アクセス プロトコルを使用した Cisco IOS デバイスの作成

各 Cisco CNS IE2100 アプライアンスは、複数の Cisco IOS デバイスを処理できます。1 台の Cisco IOS デバイスを処理できるのは 1 台の Cisco CNS IE2100 アプライアンスのみです。Cisco CNS デバイス アクセス プロトコルを使用して Cisco IOS デバイスを作成するには、次の手順を実行します。

（注）　詳細については、「デバイス」（P.2-1）を参照してください。第 2 章「Prime Provisioning を設定する前に」

ステップ 1　[Inventory] > [Physical Inventory] > [Devices] を選択すると、[Device] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

ステップ 3　[Create] メニューから、[Cisco Device] をクリックします。

[Create Cisco Device] ウィンドウが表示されます。

ステップ 4　[General] セクションに、[Device Host Name] と [Device Domain Name] を入力します。

CNS Device Access Protocol では、[Login User] セクションと [Login Password] セクションでパラメータを定義する必要はありません。

[Device and Configuration Access Information] セクションでは、[Terminal Session Protocol] に [CNS] を選択する必要があります。

[Device and Configuration Access Information] セクションでは、唯一の有効な [OS] の選択肢は [IOS] です。[IOS XR] は、Prime Provisioning が動作する Cisco CNS IE2100 アプライアンスでサポートされていません。

ステップ 5　ウィンドウの下部にある [Additional Properties] の [Show] ボタンをクリックするとウィンドウが展開され、追加情報が追加されます。

次の手順は、[Terminal Server] と [CNS Options] のセクション**に関連します。**

ステップ 6　デバイスを完全な管理対象デバイスにする場合は、[Fully Managed] チェックボックスをオンにします。完全な管理対象デバイスの場合、Prime Provisioning の外部から行われたデバイス設定変更を受信すると、Prime Provisioning は電子メール通知を送信し、侵入の可能性を検出すると、強制監査タスクをスケジュールします。

（注）　『*Cisco Prime Provisioning Administrator’s Guide 6.3*』で説明されているように、電子メールと [Fully Managed] に DCPL パラメータを設定してください。[Administration] > [Control Center] > [Hosts] を選択します。ホストを選択し、[Config] をクリックします。次に左のカラムの TOC で、次のフィールドに該当する情報を入力してください。[SYSTEM] > [email] > [from]、[SYSTEM] > [email] > [smtpHost]、[SYSTEM] > [fullyManaged] > [auditableCommandsFileLocation]（ここで情報が指定されない場合、すべてのコマンドが監査されます）、[SYSTEM] > [fullyManaged] > [enforcementAuditScript]、および [SYSTEM] > [fullyManaged] > [externalEventsEmailRecipients]。

（注）　**cns config notify** コマンドが IOS デバイスに対して設定されていることを確認します。このコマンドによって、完全管理機能の基盤となる設定変更イベントがイベント バスに送信されるようになります。このコマンドがデバイスに設定されていない場合、Prime Provisioning に到達する設定変更イベントがないため、完全管理機能は機能しません。

ステップ 7　次のように、[Device State] を指定します。

- [ACTIVE] を選択（デフォルト）：ルータがネットワークに物理的に存在する場合。
- [INACTIVE] を選択：ルータがネットワークにまだ物理的に存在しない場合。

ステップ 8　次のように、[Device Event Identification] を指定します。

- [HOST_NAME] を選択：ステップ 4 で定義されているように、[Device Host Name] をこのデバイスの [CNS Identification] として使用する場合。
- [CNS_ID] を選択：デバイスの CNS ID ストリングが [Device Host Name] 以外である場合。
- [CNS_ID] を [Device Event Identification] として選択した場合、[CNS Identification] パラメータを [CNS Identification] というラベルのフィールドに入力する必要があります。これは一意の引数にする必要があります。これは、対応する Cisco CNS IE2100 リポジトリでデバイスを作成し、このデバイスに関連するイベントをリッスンするために使用されます。

（注）　**cns id string {CNS_ID} event** コマンドが IOS デバイスに設定されていることを確認します。このコマンドがデバイス上に存在しない場合、IE2100 はこの CNS ID を使用してバス上でイベントを送出しないため、デバイスとの通信が障害になります。

ステップ 9　この Cisco IOS デバイスを動作させる Cisco CNS **IE2100** アプライアンスを選択します。リポジトリにすでに定義されている IE2100 デバイスのドロップダウン リストからエントリを 1 つ選択します。

ステップ 10　[CNS Software Version] のドロップダウン リストを使用して、IOS デバイスを管理する Cisco CNS Configuration Engine のバージョンを選択します（1.3、1.3.1、1.3.2、1.4、1.5、2.0、3.0、または 3.5）。

ステップ 11　[CNS Device Transport] のドロップダウン リストを使用して、Prime Provisioning によって使用される転送メカニズムとして HTTP または HTTP を選択し、IE2100 リポジトリでデバイスの作成、削除、または編集を行います。[HTTPS] を使用する場合、Cisco CNS Configuration Engine をセキュア モードで実行する必要があります。

ステップ 12　[Save] をクリックします。Cisco IOS デバイスがリストされて、[Devices] ウィンドウが再表示されます。

Plug-and-Play の使用

Prime Provisioning は、Cisco CNS IE2100 アプライアンスを介した Plug-and-Play デバイス設定をサポートします。Prime Provisioning は、ネットワーク上に物理的に存在しないデバイスをサポートしています。

Cisco IOS デバイスがネットワーク上に物理的に存在しない場合に Plug-and-Play を使用するための手順は、デバイス用の初期コンフィギュレーション ファイルがあるかどうかによって異なります。

Cisco IOS デバイスに初期コンフィギュレーション ファイルが*ない*場合は、次の手順を実行します。

ステップ 1 「Cisco CNS デバイス アクセス プロトコルを使用した Cisco IOS デバイスの作成」（P.A-2）の項で説明されているように、Cisco IOS デバイスを作成します。

ステップ 2 Cisco IOS デバイスのプロパティを定義します。

デバイスが物理的にネットワークにないため、[Device State] は [INACTIVE] として指定してください。

ステップ 3 [Save] をクリックします。

Cisco IOS デバイスのエントリが Prime Provisioning リポジトリと、対応する Cisco CNS IE2100 アプライアンス リポジトリに作成されます。

Cisco IOS デバイスに初期コンフィギュレーション ファイルが*ある*場合、このマニュアルの第 13 章「インベントリ マネージャの使用」で説明されている [Inventory Manager] 機能を使用して、初期コンフィギュレーション ファイルを Prime Provisioning にインポートします。

デバイスが物理的にネットワークにないため、[Device State] は [INACTIVE] として指定してください。

インベントリ マネージャは Cisco IOS デバイスのエントリを Prime Provisioning リポジトリに作成します。また、対応する Cisco CNS IE2100 リポジトリ内にエントリを作成し、Cisco CNS IE2100 リポジトリで、指定された初期設定ファイルをこの新しいデバイスに関連付けます。

さまざまなサービス用に新しく作成された非アクティブ Cisco IOS デバイスをプロビジョニングできます。デバイスがネットワークに物理的に存在しないため、Prime Provisioning はこれらのサービスに関連付けられたコンフィグレットをそのリポジトリに保存し、デバイスが起動した後にのみ、それらをデバイスにダウンロードしようとします。デバイスがネットワークに物理的に存在するようになるまで、サービス要求は **WAIT_DEPLOY** 状態になります。サービス要求は、サービスごとにユーザ ガイドに記載されています。

デバイスが起動し、対応する Cisco CNS IE2100 アプライアンスに接続されると、Cisco CNS IE2100 リポジトリに初期コンフィギュレーションを待機しているものがある場合、デバイスは初期コンフィギュレーションを取得して、適用します。

Prime Provisioning はデバイスがネットワークに接続されたことを検出すると、次のアクションを実行します。

- Cisco IOS デバイスの状態を [INACTIVE] から [ACTIVE] に変更します。

  Prime Provisioning は、IOS デバイスのコンフィギュレーション収集を実行し、Prime Provisioning リポジトリにそれを保存します。
- いずれかの Prime Provisioning サービスがこのデバイスの起動を待機しているかどうかを確認し、対応するコンフィグレットをデバイスにダウンロードして、サービス要求を完了しようとします。

APPENDIX B

Prime Provisioning XML リファレンス

この付録では、Prime Provisioning ディスカバリで使用される XML ファイルで使用される XML ルール、タグ、および属性を示します（アルファベット順）。

XML ファイルと XML の例の詳しい説明については、付録 E「インベントリ - ディスカバリ」を参照してください。

表 B-1　Prime Provisioning の XML ルール、タグ、および属性

タグ	説明
<as-number>	プロバイダーの自律システム（AS）番号を指定します。AS 番号は、1 ～ 65535 の範囲の整数です。
<CDP>	**<CDP>** タグを開始します。**<CDP>** タグは、シード IP アドレスとホップ カウントを指定します。 **<CDP>** タグには、次の属性を含める必要があります。 • **ipaddress** • **hop**
<connection>	**<connection>** タグを開始します。**<connection>** タグでは、次の属性を指定する必要があります。 • **discovery-protocol** • **fromDevice** • **FromIP** • **FromInterface** • **toDevice** • **toIP** • **toIF**

表 B-1　Prime Provisioning の XML ルール、タグ、および属性 （続き）

タグ	説明
<create-customer>	**create-customer** ルールを開始します。**create-customer** ルールは、リージョン オブジェクトを作成します。create-customer ルールには、次のタグを含める必要があります。 • **<customer-name>** • **<create-site>**
<create-provider>	**create-provider** ルールを開始します。create-provider ルールは、サービス プロバイダー オブジェクトを作成します。 **create-provider** ルールには次のタグを含める必要があります。 • **<provider-name>** • **<as-number>** • **<create-region>**
<create-region>	**create-region** ルールを開始します。**create-region** ルールはリージョン オブジェクトを作成します。**create-region** ルールには **region-name** タグを含める必要があります。
<create-site>	**create-site** ルールを開始します。create-site ルールには **<site-name>** タグを含める必要があります。
<customer-name>	カスタマー名を指定します。**create-customer** ルール内で必須です。
<device>	**<device>** タグを開始します。**<device>** タグには、次のタグを含める必要があります。 • **<device-name>** • **<ip-address>** 次のタグは、**<device>** タグ内で使用する任意のタグです。 • **<system-object-id>** • **<snmp-info>**
<device-name>	デバイス名を指定します。**<device>** タグ内で必須です。
<DISCOVERY_METHOD>	**<DISCOVERY_METHOD>** タグを開始します。**<DISCOVERY_METHOD>** タグには **<CDP>** タグを含める必要があります。
discovery-protocol	ネットワーク トポロジを検出する際に使用する検出プロトコルを指定します。通常は「CDP」です。
fromDevice	名前付き物理回線の開始元のデバイス名を指定します。**<connection>** タグの必須属性です。

表 B-1　Prime Provisioning の XML ルール、タグ、および属性 （続き）

タグ	説明
FromInterface	名前付き物理回線の開始元のデバイス インターフェイス名を指定します。**<connection>** タグの必須属性です。
FromIP	名前付き物理回線の開始元デバイスの管理 IP アドレスを指定します。**<connection>** タグの必須属性です。
hop	デバイスを検出するときに、**ipaddress** 属性によって指定されたデバイスから何ホップまでを対象とするかを指定します。**<CDP>** タグの必須属性です。
ipaddress	シード デバイスの IP アドレスを指定します。**<CDP>** タグの必須属性です。
<ip-address>	デバイスの IP アドレスを指定します。**<device>** タグ内で必須です。
<provider-name>	プロバイダーの名前を指定します。
<region-name>	リージョン名を指定します。
<ro-community>	デバイスの SNMP アクセスのレベルを指定します。通常は「public」にします。**<snmp-info>** タグ内で必須です。
<site-name>	サイト名を指定します。
<snmp-info>	デバイスの SNMP 情報を指定します。**<snmp-info>** タグには **<ro-community>** タグを含める必要があります。**<device>** タグ内では任意です。
<system-object-id>	（任意）使用するとデバイスに SNMP Object ID（OID; オブジェクト ID）を指定できます。これを指定すると、**<device>** タグ内に指定されます。
toDevice	名前付き物理回線の接続先デバイス名を指定します。**<connection>** タグの必須属性です。
toIF	名前付き物理回線の接続先デバイス上で、デバイス インターフェイスを指定します。**<connection>** タグの必須属性です。
toIP	名前付き物理回線が **<connection>** タグ必須属性に接続する際の接続先デバイスの管理 IP アドレスを指定します。

APPENDIX C

2 台の N-PE 上でのアクセス リングの終端

この付録では、アクセス リンクがダウンした場合に備えた冗長性のために、2 台の N-PE 上でアクセス リングを終端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。

概要

Prime Provisioning は、サービス トポロジでデバイス レベルの冗長性をサポートします。これにより、1 つのアクセス リンクがドロップした場合でも、サービスはアクティブな状態を維持できます。これは、2 台の異なる N-PE に対するアクセス リンクの終端のプロビジョニングをサポートすることによって達成されます。2 台の異なる N-PE 上でアクセス リングを終端できるようにすることで実現されます。これは、「デュアルホーム接続されたアクセス リング」と表現することもできます。N-PE は、N-PE 上のループバック インターフェイスを使用した論理リンクによって接続されます。冗長リンクは、U-PE デバイスから開始して、任意で PE-AGG デバイスを含めることができます。一方の接続リンクがプライマリとなり、他方がセカンダリとなります。選択は、Named Physical Circuit（NPC; 名前付き物理回線）を作成するときに行われます。NPC 上の終端デバイスはプライマリ N-PE として動作し、同じリング上の他方の N-PE はセカンダリ N-PE として動作します。

下位互換性を得るために、Prime Provisioning は以前のリリースと同様に冗長リンクなしのプロビジョニング サービスを引き続きサポートします。

N-PE 冗長性は、FlexUNI/EVC および MPLS サービスでサポートされます。両方のサービスで基本概念の多くが共有されているため、この付録で両方のサービスについて説明します。

図 C-1 と図 C-2 は、冗長性を説明するための、U-PE アクセス ノードで開始される 2 つのネットワーク トポロジを示しています。どちらのトポロジも、各アップリンクに対して、U-PE で開始され N-PE デバイスで終端するオープンなセグメントを提供しています。N-PE はループバック インターフェイスによって論理的に接続されています。サービスは、U-PE で開始され 2 台の異なる N-PE への、これら両方のイーサネット アクセス リンク上で設定されます。

図 C-1　U-PE で開始される N-PE の冗長性

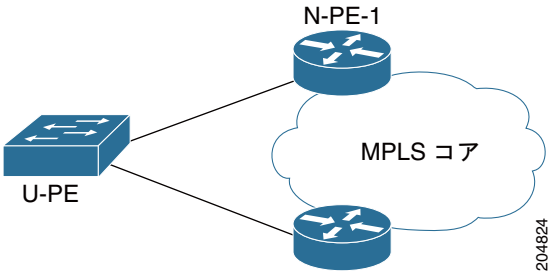
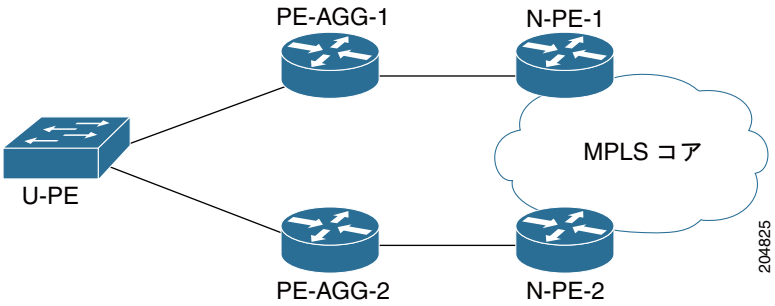


図 C-2　U-PE で開始される N-PE と PE-AGG の冗長性



最初のトポロジ（図 C-1 に示す、U-PE で開始される N-PE の冗長性）は、N-PE デバイスのディザスタ リカバリのモデルを提供します。図に示すように、U-PE デバイスで開始される 2 つの異なる発信インターフェイスがあります。各インターフェイスは異なる N-PE で終端します。

第 2 のトポロジ（図 C-2 に示す、U-PE で開始される N-PE と PE-AGG の冗長性）は、PE-AGG デバイスと N-PE デバイスの両方に対してディザスタ リカバリ機能を提供します。サービスは、プライマリ リンクの PE-AGG と N-PE のいずれかが障害になった場合に、プライマリ リンクからセカンダリ リンクにスイッチオーバーします。

より複雑なトポロジを表す他のネットワーク シナリオについては、「追加のネットワーク構成とサンプル コンフィグレット」（P.C-5）を参照してください。

次のリストに、実装の詳細を示します。

- 1 台の U-PE と 2 台の N-PE を使用することで、1 つの Access Link（AL; アクセス リンク）が消費されます。
- U-PE 上でサービスを作成する場合、ユーザは使用する NPC を指定します。トポロジに 2 台の N-PE を使用したアクセス リングが含まれる場合、サービスは両方の N-PE で設定されます。
- Ethernet over MPLS（EoMPLS）の疑似回線（PW）サービスでは、サービス プロバイダー ネットワークの両側に N-PE の冗長性がある場合、2 個の疑似回線が作成されます。疑似回線の接続方法を決定するために、1 台の N-PE がプライマリとして定義され、他方がセカンダリとして定義されます。ユーザが [PW Redundancy] オプションをイネーブルにした場合、両方の端のプライマリとセカンダリも疑似回線冗長性が有効な状態で接続されます。
- Point-to-Point（P2P; ポイントツーポイント）構成の場合、2 台の N-PE が 2 個の異なる疑似回線を使用します。
- Prime Provisioning のサポートは、サービスが両方の N-PE で同様に設定される場合（アクセス インターフェイスを除き）に行われます。サービス要求ワークフロー内のリンク属性は、接続回線の一部になっている両方の N-PE で共通であるため、ユーザはデータを 2 回入力する必要がありません。

- この機能は、Cisco 7600 プラットフォームと Cisco ASR 9000 プラットフォームの両方でサポートされています。ただし、1 つのサービスに 7600 プラットフォームと ASR 9000 プラットフォームの両方を含めることはできません。
- Cisco ASR 9000 プラットフォームでは、IOS XR バージョン 3.7.3 および 3.9.0 がサポートされています。

（注）　本ガイドの発行以降にアップデートが行われる可能性があるため、デバイスおよびプラットフォームのサポートの最新情報について、*『Cisco Prime Provisioning 6.3 Release Notes』*のオンライン版を参照してください。

この機能の実装については、次の項で詳しく説明します。

2 台の N-PE を使用した NPC アクセス リングの設定

2 つの N-PE での NPC アクセス リングの終端は、Prime Provisioning で NPC リングを設定する標準的な方法を使用して実現できます。これを行うための基本的な手順については、「論理的インベントリの設定」（P.2-56）を参照してください。その他の情報については、このマニュアルの「名前付き物理回線の作成」（P.3-13）の項を参照してください。

通常、リングは物理インターフェイスを通じてデバイスを接続することで閉じられます。2 台の異なる N-PE 上でアクセス リングを終端させる場合、N-PE 間に物理接続は必要ありません。しかし、Prime Provisioning では、リングを閉じるには N-PE 間に仮想リンクを作成する必要があります。仮想リンクは、ループバック インターフェイスを使用して設定されます。

リング内でこのようにしてループバック インターフェイスを使用するには、DCPL プロパティ allowLoopbackIntfInNPC をイネーブルにする必要があります。このプロパティには、[Host Configuration] ウィンドウのフォルダ /repository/mlshare でアクセスします。この DCPL プロパティを true に設定すると、Prime Provisioning で、リング内のループバック インターフェイスを使用できます。

（注）　Prime Provisioning はサービス要求の展開時にループバック インターフェイスに対してコンフィグレットを生成しないことに注意してください。

FlexUNI/EVC サービス要求での N-PE 冗長性の使用

FlexUNI/EVC サービス要求でデュアルホーム接続のアクセス リングを使用するために、Prime Provisioning GUI の通常のワークフローを変更する必要はありません。FlexUNI/EVC サービス要求の作成中、2 つの N-PE 上で終端された NPC アクセス リングに関連付けられている NPC を選択します。

使用方法に関する注釈：

- サービスはアクセス リングの両方の N-PE 上で設定します。
- 2 台の異なる N-PE がありますが、1 つのアクセス リンクのみが消費されます。
- サービス要求を展開する前または展開した後に、構成が冗長な N-PE を変更できます。変更したコンフィグレットは、サービス要求で行った変更に従って生成されます。

- サービス要求で使用される NPC 上の宛先の N-PE デバイスは、プライマリ N-PE として扱われます。同じリング上の他方の N-PE はセカンダリ N-PE として扱われます。プライマリおよびセカンダリ N-PE を変更するには、サービス要求で接続回線を変更する必要があります。
- サービス要求で指定した設定に従ってコンフィグレットが生成されます。Prime Provisioning は、接続回線（AC）の両方の N-PE 上で同一のコンフィグレットを生成します。Link Attributes セクションは両方の N-PE に共通です。
- FlexUNI/EVC サービスの場合、N-PE の冗長性はコア接続タイプ PSEUDOWIRE および VPLS についてサポートされます。
- VPLS コア接続の場合、NPC リング内のすべての N-PE がレイヤ 2 Virtual Forwarding Interface（VFI; 仮想転送インターフェイス）を持つように設定され、同じ VPLS VPN 上のすべての N-PE が同時に VPLS サービスに参加します。
- PSEUDOWIRE コア接続の場合、次の注記が適用されます。
  - 両側に N-PE の冗長性がある場合、NPC の作成時に終端 N-PE デバイスとして指定された N-PE 間（プライマリ N-PE 間）に、ポイントツーポイント疑似回線（PW）が設定されます。もう 1 つのポイントツーポイント PW が、NPC の作成時に終端 N-PE デバイスとして指定されなかった N-PE 間に設定されます。これらの疑似回線の VC ID は共通です。
  - 片側のみに N-PE の冗長性がある場合、GUI で [Pseudowire Redundancy] オプションをオンにする必要があります（[FlexUNI(EVC) Service Editor] ウィンドウの [Service Request Details] セクション）。プライマリ PW はシングルホーム リングの N-PE でデュアルホーム接続のリングのプライマリ N-PE を接続し、セカンダリ PW はシングルホーム リングの N-PE でデュアルホーム接続のリングのセカンダリ N-PE を接続します。Prime Provisioning では、[Pseudowire Redundancy] オプションをイネーブルにせずにサービス要求を保存しようとすると、警告メッセージが表示されます。

MPLS サービス要求での N-PE 冗長性の使用

2 つの N-PE 上のアクセス リングの終端は、標準 PE-CE ポリシー タイプの MPLS/L3 サービスでサポートされています。NPC リングを作成し、MPLS サービスに関連付けるための手順は、「FlexUNI/EVC サービス要求での N-PE 冗長性の使用」（P.C-3）で説明されている手順に似ています。標準の MPLS サービス要求ワークフローの変更はありません。

使用方法に関する注釈：

- PE_NO_PE の場合、サービスはアクセス リングの両方の N-PE 上で設定されます。ただし、PE_CE の場合、サービス要求はアクセス リングのプライマリ N-PE で設定されます。
- 2 台の異なる N-PE がありますが、1 つのアクセス リンクのみが消費されます。
- サービス要求を展開する前または展開した後に、構成が冗長な N-PE を変更できます。変更したコンフィグレットは、サービス要求で行った変更に従って生成されます。
- サービス要求で使用される NPC 上の宛先の N-PE デバイスは、プライマリ N-PE として扱われます。同じリング上の他方の N-PE はセカンダリ N-PE として扱われます。
- NPC がサービス要求に関連付けられていない場合、プライマリ N-PE を変更するには、NPC を削除してから、再作成します。セカンダリ N-PE を変更するには、レベル リングでセカンダリ N-PE を変更する必要があります。
- PE_NO_CE ポリシーを使用した MPLS サービス要求の作成中に、セカンダリ NPE デバイスを 2 つめのリンクで設定できます。VLAN ID の PE インターフェイスなどの個別のリンク属性
- アドレス/マスク、VPN および RD などは、プライマリとセカンダリの両方の N-PE 用に個別に設定できます。このようにすることで、異なる IP アドレスをプライマリ N-PE とセカンダリ N-PE に手動で追加できます。UNI デバイス情報はプライマリ N-PE のリンクでのみ使用できます。

- 選択した NPC に 2 台の N-PE がある場合でも、PE-CE ポリシーを使用した MPLS サービス要求の作成時に、1 つの MPLS VPN リンクのみが作成されます。サービスはプライマリ N-PE にのみ関連付けることができます。セカンダリ N-PE に追加リンクは提供されません。コンフィグレットはセカンダリ N-PE を除くリング上のすべてのデバイスに生成され、転送されます。
- VPN オブジェクトと VRF オブジェクトは、2 台の N-PE 上のアクセス リングの終端を使用した MPLS サービス要求についてサポートされます。

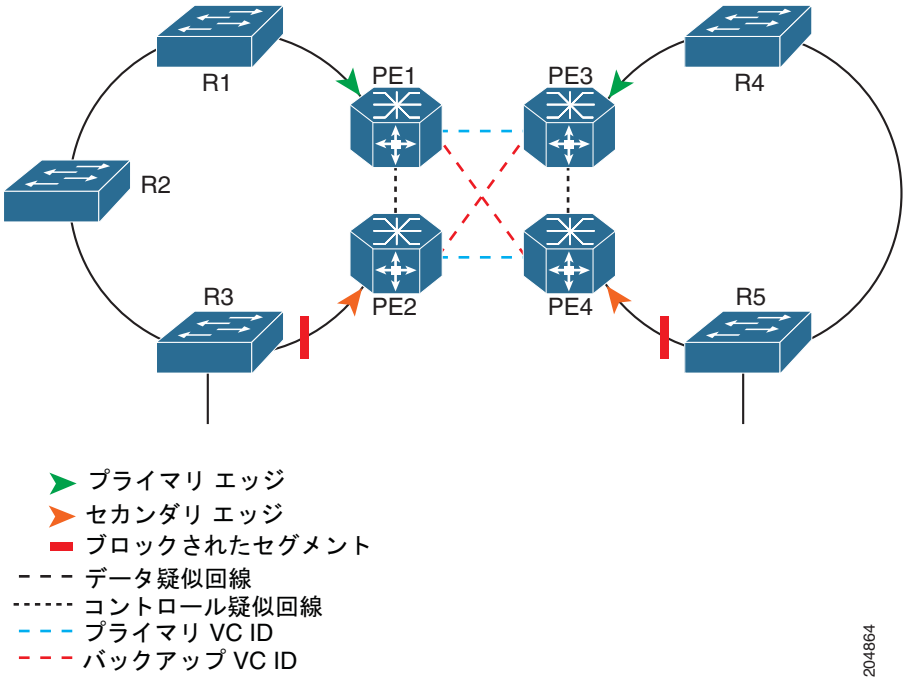
追加のネットワーク構成とサンプル コンフィグレット

ここでは、参照用の追加のネットワーク シナリオと、関連付けられたネットワーク デバイス用のサンプル コンフィグレットを示します。

例 1：疑似回線接続（A）

図 C-3 に、ネットワークの両側にデュアルホーム接続された N-PE との疑似回線接続があり、疑似回線の冗長性を使用したネットワーク構成を示します。

図 C-3　疑似回線接続、ネットワークの両側にデュアルホーム接続された N-PE、疑似回線冗長性を使用



デバイスのサンプル コンフィグレットを次に示します。

PE1

```
vlan <S-Vlan>
!
interface <UNI-to-R1>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE3 loopback> <PrimaryVcId> encapsulation mpls
    backup peer <PE4 loopback> <BackupVcId>
```

PE2

```
vlan <S-Vlan>
!
interface <UNI-to-R3>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE4 loopback> <PrimaryVcId> encapsulation mpls
    backup peer <PE3 loopback> <BackupVcId>
```

PE3

```
vlan <S-Vlan>
!
interface <UNI-to-R4>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE1 loopback> <PrimaryVcId> encapsulation mpls
    backup peer <PE2 loopback> <BackupVcId>
```

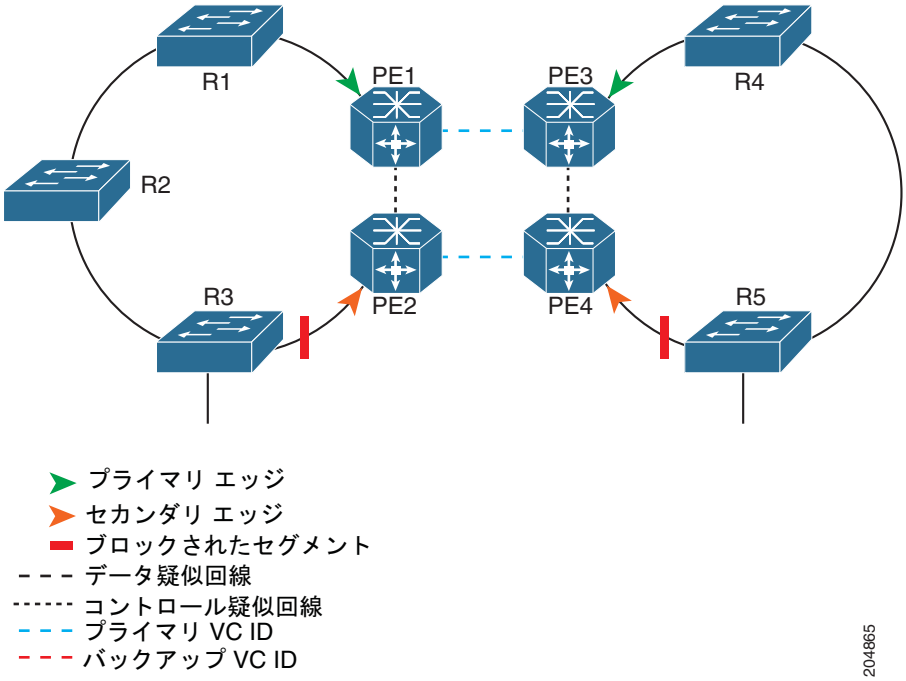
PE4

```
vlan <S-Vlan>
!
interface <UNI-to-R5>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE2 loopback> <PrimaryVcId> encapsulation mpls
    backup peer <PE1 loopback> <BackupVcId>
```

例 2：疑似回線接続（B）

図 C-4 に、ネットワークの両側にデュアルホーム接続された N-PE との疑似回線接続があり、疑似回線の冗長性を使用しないネットワーク構成を示します。

図 C-4　疑似回線接続、ネットワークの両側にデュアルホーム接続された N-PE、疑似回線冗長性なし



デバイスのサンプル コンフィグレットを次に示します。

PE1

```
vlan <S-Vlan>
!
interface <UNI-to-R1>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE3 loopback> <PrimaryVcId> encapsulation mpls
```

PE2

```
vlan <S-Vlan>
!
interface <UNI-to-R3>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE4 loopback> <PrimaryVcId> encapsulation mpls
```

PE3

```
vlan <S-Vlan>
!
interface <UNI-to-R4>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE1 loopback> <PrimaryVcId> encapsulation mpls
```

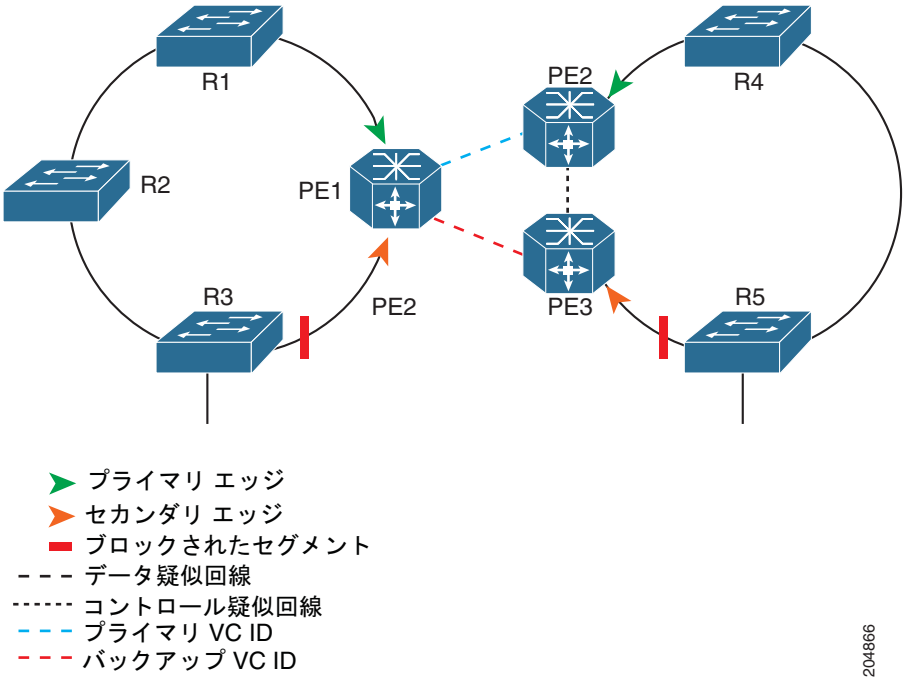
PE4

```
vlan <S-Vlan>
!
interface <UNI-to-R5>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE2 loopback> <PrimaryVcId> encapsulation mpls
```

例 3：疑似回線接続（C）

図 C-5 に、ネットワークの片側にデュアルホーム接続された N-PE との疑似回線接続があり、疑似回線の冗長性を使用したネットワーク構成を示します。

図 C-5　疑似回線接続、ネットワークの片側にデュアルホーム接続された N-PE、疑似回線冗長性を使用



デバイスのサンプル コンフィグレットを次に示します。

PE1

```
vlan <S-Vlan>
!
interface <UNI-to-R1>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE2 loopback> <PrimaryVcId> encapsulation mpls
    backup peer <PE3 loopback> <BackupVcId>
```

PE2

```
vlan <S-Vlan>
!
interface <UNI-to-R4>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE1 loopback> <PrimaryVcId> encapsulation mpls
```

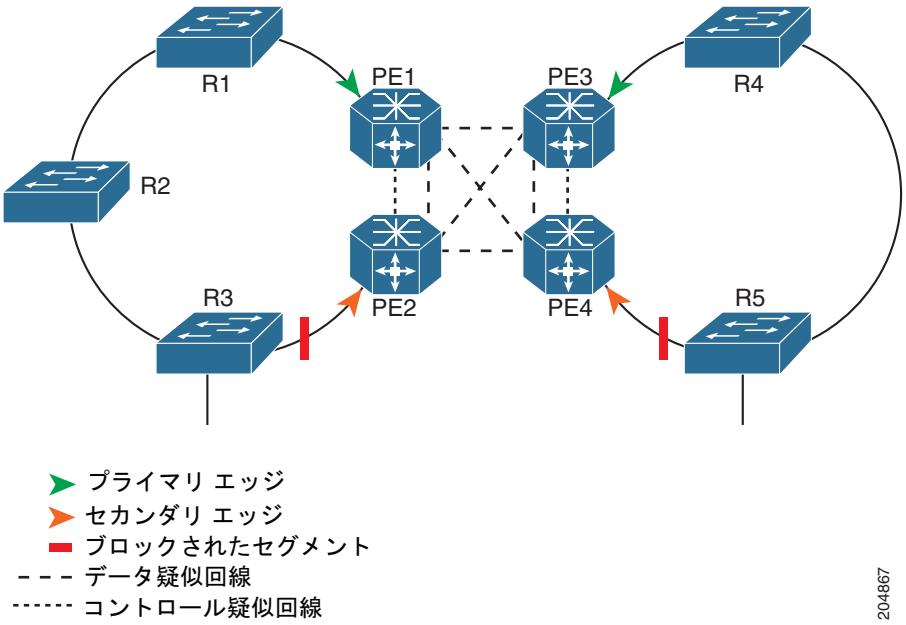
PE3

```
vlan <S-Vlan>
!
interface <UNI-to-R5>
    switchport
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport trunk allowed vlan add <S-Vlan>
!
interface vlan <S-Vlan>
    xconnect <PE1 loopback> <BackupVcId> encapsulation mpls
```

例 4：VPLS 接続

図 C-6 に、ネットワークの両側にデュアルホーム接続された N-PE との VPLS 接続があるネットワーク構成を示します。

図 C-6　VPLS 接続、ネットワークの両側にデュアルホーム接続された N-PE



デバイスのサンプル コンフィグレットを次に示します。

PE1

```
vlan <S-Vlan>
!
l2 vfi <VFI-ID> manual
    vpn id <S-Vlan>
    neighbor <PE2> encapsulation mpls
    neighbor <PE3> encapsulation mpls
    neighbor <PE4> encapsulation mpls
!
interface vlan <S-Vlan>
    xconnect vfi <VFI-ID>
!
interface <NNI-to-R1>
    switchport trunk allowed vlan add <S-Vlan>
```

PE2

```
vlan <S-Vlan>
!
l2 vfi <VFI-ID> manual
    vpn id <S-Vlan>
    neighbor <PE1> encapsulation mpls
    neighbor <PE3> encapsulation mpls
    neighbor <PE4> encapsulation mpls
!
interface vlan <S-Vlan>
    xconnect vfi <VFI-ID>
!
interface <NNI-to-R3>
    switchport trunk allowed vlan add <S-Vlan>
```

PE3

```
vlan <S-Vlan>
!
l2 vfi <VFI-ID> manual
    vpn id <S-Vlan>
    neighbor <PE1> encapsulation mpls
    neighbor <PE2> encapsulation mpls
    neighbor <PE4> encapsulation mpls
!
interface vlan <S-Vlan>
    xconnect vfi <VFI-ID>
!
interface <NNI-to-R5>
    switchport trunk allowed vlan add <S-Vlan>
```

PE4

```
vlan <S-Vlan>
!
l2 vfi <VFI-ID> manual
    vpn id <S-Vlan>
    neighbor <PE1> encapsulation mpls
    neighbor <PE2> encapsulation mpls
    neighbor <PE3> encapsulation mpls
!
interface vlan <S-Vlan>
    xconnect vfi <VFI-ID>
!
interface <NNI-to-R4>
    switchport trunk allowed vlan add <S-Vlan>
```

APPENDIX D

リポジトリ ビュー

ビューは、クエリーの結果セットからなる仮想的なテーブルとしてアクセス可能なストアド クエリーです。ビューは、リレーショナル データベースの通常のテーブル（ベース テーブル）と異なり、物理的なスキーマの一部を構成せず、データベース中のデータから計算または照合された、動的で仮想的なテーブルです。テーブル内のデータを変更すると、それ以降にビューを実行したときに表示されるデータが変化します。

リポジトリ ビューの利点は次のとおりです。

- データのセキュリティ：テーブルのあらかじめ決められた行または列のセットあるいはその両方にアクセスを制限することで、テーブルのセキュリティ レベルがさらに高まります。
- 1 つのテーブルなど、さまざまなデータ ソースからデータを簡単にクエリーできます。
- 複数のテーブルに基づく複雑なレポートを作成するときに便利です。

この付録の内容は、次のとおりです。

リポジトリ ビューの作成

この項では、Sybase リポジトリおよび Oracle リポジトリでのビューの作成方法について説明します。

Sybase リポジトリでのビューの作成

新規およびアップグレード インストール

Prime Provisioning で使用可能なすべてのビュー（「Prime Provisioning でのビューの使用」（P.D-2）を参照）は、Prime Provisioning 6.3 の新規インストールおよびアップグレード インストールの一部として作成されます。

Oracle リポジトリでのビューの作成

新規およびアップグレード インストール

Prime Provisioning 6.3 の新規インストールおよびアップグレード インストールでリポジトリ ビューを作成するには（「Prime Provisioning でのビューの使用」（P.D-2）を参照）、次の手順を実行します。

ステップ 1　**schema.tar** ファイルを Oracle サーバにコピーし、すべてのファイルをディレクトリに展開します。

（注）　スキーマ情報は、ソフトウェア パッケージの schema.tar ファイルに格納されています。正しいパッケージを入手し（スキーマはパッケージごとに異なる場合があります）、**schema.tar** ファイルをパッケージから展開します。

ステップ 2　展開したスキーマが格納されているディレクトリを参照し、**ddl/6.0** サブディレクトリに移動します。

ステップ 3　コマンド **sqlplus** を実行します。

ステップ 4　sysdba としてログインし、次のコマンドを使用して Prime Provisioning ユーザに DBA 特権を付与します。
GRANT DBA, CONNECT, RESOURCE TO <isc_user>;

ステップ 5　前に作成したユーザ名とパスワードでログインします。

ステップ 6　SQL コマンド **start DBViews.sql;** を入力します。

これで、Oracle リポジトリ内のすべてのビューが作成されます。

Prime Provisioning でのビューの使用

Prime Provisioning で使用できる各種ビューは次のとおりです。

- 「サマリー ビュー」（P.D-2）
- 「サイト ビュー」（P.D-4）
- 「カスタマー ビュー」（P.D-5）
- 「リージョン ビュー」（P.D-5）

サマリー ビュー

サマリー ビューのカラム名を使用してクエリーを実行できます。表 D-1 には、カラム名とタイプ名が説明されています。

表 D-1　サマリー ビューの列名

カラム名	型名
SR_Number	整数型
SR_STATE	整数型

表 D-1　サマリー ビューの列名 （続き）

カラム名	型名
SR_Last_Modified_Time	Varchar
PE_Name	Varchar
PE_Interface	Varchar
PE_Interface_IPAddress	Varchar
CE_Name	Varchar
CE_Interface	Varchar
CE_Interface_IPAddress	Varchar
CE_Type	整数型
CE_Site_ID	整数型
CE_Site_Name	Varchar
VPN_Name	Varchar
VRF_Name	Varchar
Customer_ID	整数型
Customer_Name	Varchar
JOB_DESCRIPTION	Varchar

列名の説明を次に示します。

- SR_Number：サービス要求番号。Prime Provisioning GUI の [Service Request] ページで使用可能なサービス要求の JOB ID を表します。
- SR_STATE：サービス要求の状態。次の表に、データベース中の値と関連付けられている状態のマッピングを示します。

データベース値	関連付けられている状態
-1	UNKNOWN
0	All States
1	Requested
2	Pending
3	Failed Deploy
4	InValid
5	Deployed
6	Broken
7	Functional
8	Lost
9	Closed
10	Failed Audit
11	Wait Deploy
12	In Progress

- SR_Last_Modified_Time：SR の現在の状態に基づく SR の最終変更時間
- PE_Name：PE のホスト名
- PE_Interface：SR に関連付けられた PE インターフェイス名
- PE_Interface_IPAddress：PE インターフェイスの IP アドレス
- CE_Name：CE ホスト名
- CE_Interface：SR に関連付けられた CE インターフェイス名
- CE_Interface_IPAddress：CE インターフェイスの IP アドレス
- CE_Type：CE デバイスの管理タイプ。次の表に、データベース中の値と CE 管理タイプのマッピングを示します。

データベース値	CE 管理タイプ
-1	UNKNOWN
0	Managed
1	UnManaged
2	Managed - Management LAN
3	UnManaged - Management LAN
4	Directly Connected
5	Directly Connected Management Host
6	Multi-VRF
7	Un Managed Multi-VRF

- CE_Site_ID：CE のサイト ID
- CE_Site_Name：CE のサイト名
- VPN_Name：SR に関連付けられている VPN 名
- VRF_Name：SR に関連付けられている VRF 名
- Customer_ID：カスタマー ID
- Customer_Name：カスタマー名
- JOB_DESCRIPTION：MPLS SR のジョブの説明

サマリー ビュー クエリーの例を次に示します。

```
select SR_Number, PE_Name, CE_Name, VPN_Name from Summary_View;
```

サイト ビュー

サイト ビューのカラム名を使用してクエリーを実行できます。表 D-2 には、カラム名とタイプ名が説明されています。

表 D-2　サイト ビューのカラム名

カラム名	型名
SITE_ID	整数型
SITE_NAME	Varchar
CPE_Name	Varchar
LINK_ID	整数型

列名の説明を次に示します。

- SITE_ID：サイト ID
- SITE_NAME：サイト名
- CPE_Name：サイトに関連付けられている CPE 名
- LINK_ID：SR に関連付けられた CPE リンクの ID

サイト ビュー クエリーの例を次に示します。

```
select Site_Id, Site_Name, CPE_Name, Link_ID from Site_View;
```

カスタマー ビュー

カスタマー ビューのカラム名を使用してクエリーを実行できます。表 D-3 には、カラム名とタイプ名が説明されています。

表 D-3　カスタマー ビューの列名

カラム名	型名
CUSTOMER_ID	整数型
CUSTOMER_CONTACT	Varchar

列名の説明を次に示します。

- CUSTOMER_ID：カスタマー ID
- CUSTOMER_CONTACT：カスタマーに関する情報

カスタマー ビュー クエリーの例を次に示します。

```
select * from Customer_View;
```

リージョン ビュー

リージョン ビューに使用できるカラム名を使用してクエリーを実行できます。表 D-4 には、カラム名とタイプ名が説明されています。

表 D-4　[Region] ビューのカラム名

カラム名	型名
PROVIDER_ID	整数型
REGION_ID	整数型
PE_NAME	Varchar

列名の説明を次に示します。

- PROVIDER_ID：プロバイダー ID
- REGION_ID：プロバイダーのリージョン ID
- PE_NAME：このリージョンに関連付けられている PE のホスト名

リージョン ビュー クエリーの例を次に示します。

```
select Region_Id, PE_Name from Region_View;
```

APPENDIX E

インベントリ - ディスカバリ

この付録では、ディスカバリ機能を使用して Prime Provisioning プロビジョニング プロセスのためにデバイス、接続、サービスを検出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。

Prime Provisioning ディスカバリの概要

Prime Provisioning ディスカバリ機能は、既存のネットワーク（Prime Provisioning の導入より先に存在していたサービスを持つネットワーク）での Prime Provisioning のインストールに役立つよう設計されています。Prime Provisioning ディスカバリは、サービスの検出とデータベースとの同期とを繰り返し実行するメカニズムではありません。初回のディスカバリが完了した後のプロビジョニングは、すべて Prime Provisioning を使用して実行する必要があります。Prime Provisioning を使用せずにサービスを直接プロビジョニングすると、サービスは Prime Provisioning から認識されず、Prime Provisioning によってこれらのサービスに上書きや競合が発生する可能性があります。このため、Prime Provisioning 以外でプロビジョニングされたサービスはすべて、グラフィカル ユーザ インターフェイス（GUI）またはアプリケーション プログラム インターフェイス（API）によって

Prime Provisioning にプロビジョニングすることで Prime Provisioning に展開する必要があります。これをエコー モードで実行することで、ネットワークと Prime Provisioning データベースとの同期が後続のコンフィギュレーション監査によって確認されます。

通常、Prime Provisioning でプロビジョニング可能なサブセットだけが検出されます。
Prime Provisioning でプロビジョニングできないタイプのサービスは検出できません。

Prime Provisioning によって、ご使用の MPLS VPN または L2VPN メトロ イーサネット ネットワークを構成するデバイス、接続、サービスを検出してネットワーク デバイスのインベントリを作成するプロセスを効率良く進められます。

（注） サービス ディスカバリは、ネットワーク内のさまざまな要素の影響を受ける、複雑な操作です。元のネットワーク コンフィギュレーションは、サービスのプロビジョニング時に Prime Provisioning が使用したルールに従って実行されたものである必要があります。そうでない場合、ディスカバリ中にエラーが発生することがあります。特定のネットワークでは多数の設定が可能であるため、サービス ディスカバリ プロセスをコミットする前に、シスコのアカウント チームまたはシスコ アドバンスド サービスに連絡して、サポートを受けることを強く推奨します。

サービス ディスカバリを実行するユーザは、全体的なネットワーク トポロジを十分把握し、PE、N-PE、U-PE、PE-AGG、CE といったネットワーク用語についての知識があり、Prime Provisioning での NPC やメトロ イーサネット /MPLS サービスの定義について理解している必要があります。

Prime Provisioning は、管理ユーザだけに対してディスカバリ プロセスをサポートします。

Prime Provisioning ディスカバリ機能は、Prime Provisioning アプリケーション スイートに含まれる次の 3 つのアプリケーションのリポジトリ読み込みに使用できます。

- Prime Provisioning MPLS VPN Management
- Prime Provisioning L2VPN Management
- Prime Provisioning Prime Diagnostics

（注） サービス ディスカバリは、Secure Shell version 2（SSHv2; セキュア シェル バージョン 2）をターミナル セッション プロトコルとしてサポートしていません。MPLS および L2VPN のサービス ディスカバリは、IOS XR が稼働中のデバイスをサポートしていません。

Prime Provisioning のデバイスにホスト名だけが割り当てられている場合、Prime Provisioning デバイスでは、IP 管理アドレスまたはドメイン名が設定されていません。ディスカバリでは、同じホスト名のデバイスが IP 管理アドレスで検出された場合やデバイス エディタで手動作成された場合、そのデバイスによる Prime Provisioning リポジトリへのコミットが失敗することがあります。この失敗の原因は、両方のデバイスにドメイン名が設定されていないため、既存の Prime Provisioning デバイスで一致判定がなされてしまうことにあります。

回避策として、次の 1. または 2. のいずれかを実行します。

1. ディスカバリの前に既存の Prime Provisioning 内デバイスを編集し、管理 IP アドレスを追加しておく。これにより、ディスカバリはそのデバイスを重複として扱い、デバイス エディタでは読み取り専用としてマークします。

   または

2. ディスカバリ中に、検出されたデバイスにデバイス エディタを使用してドメイン名を入力する。これにより、ディスカバリはそのデバイスを新しいデバイスとして扱うようになります。

Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ インターフェイスおよびプロセスがあります。この点については、*『Cisco Prime Provisioning 6.3 User Guide』*の TE ネットワーク検出で説明されています。

複数のサービス ディスカバリ プロセスがサポートされており、前のステップの任意の場所から再開できます。複数のサービス ディスカバリ プロセスのサポートによって、ネットワークの増分ディスカバリが可能になります。前のステップから再開する機能は、選択した以前のステップまでディスカバリ プロセスをロールバックするために役立ちます。これにより、ディスカバリ プロセス全体を最初から再開する代わりに、そのステップから検出を再開できます。ディスカバリ データ収集から再開すると、データ収集が必要なデバイスを選択するよう求められます。

既存の VPN リンクでは増分ディスカバリが発生します。既存の VPN はディスカバリ GUI では編集できません。既存の VPN リンクは、コミット中バイパスされます。

MPLS および L2VPN サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning へのコミットは、各ステップの後ではなく、ディスカバリ フェーズの終了時だけに発生します。検出ワークフローの中で、ディスカバリ プロセスが Prime Provisioning の状態を変更することはありません。ユーザが検出されたデバイスとサービスを Prime Provisioning にコミットできるのは、ワークフローの最後だけです。

ディスカバリ プロセスは、ネットワーク トポロジの検出方法に関して、複数の選択肢を提供します。

3. Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management をプロビジョニングするためにディスカバリを実行している場合は、次の 3 つのディスカバリ方式から選択できます。

   a. CDP ディスカバリ

      Cisco Discovery Protocol（CDP）を使用して、**policy.xml** ファイルで指定する IP アドレスを持つ、最初のデバイスに接続されているデバイスを検出できます。

   b. デバイス / トポロジ・ベースのディスカバリ

      デバイス / トポロジ ベースの方式を使用できます。この方式では、デバイスおよび NPC トポロジの情報を指定する XML ファイルを使用します。

   c. インポート コンフィギュレーション ファイル ベース

      インポート コンフィギュレーション ファイル ベースの方式を使用できます。この方式は、検出するデバイスのコンフィギュレーション ファイルが格納されているサーバのディレクトリと、NPC を自動作成するために使用されるデバイス接続情報を含む XML ファイルを使用します。

4. MPLS VPN トポロジ、L2VPN（Metro Ethernet）トポロジ、またはその両方を検出するために、ネットワーク トポロジを選択できます。

   L2VPN（Metro Ethernet）ディスカバリを選択した場合は、MPLS コアの Metro Ethernet、イーサネット コアの Metro Ethernet、または混合コアの両方の組み合わせのいずれかを検出できます。混合コアでは、L2VPN サービスは、MPLS コア全体を対象とすることも、ローカル イーサネット ドメインだけに制限することもできます（ローカル スイッチド サービス）。イーサネット ドメインにわたって N-PE デバイスを通過しないローカル スイッチド サービスも検出できます。図 E-1 には、混合コアを示します。

図 E-1　混合コア

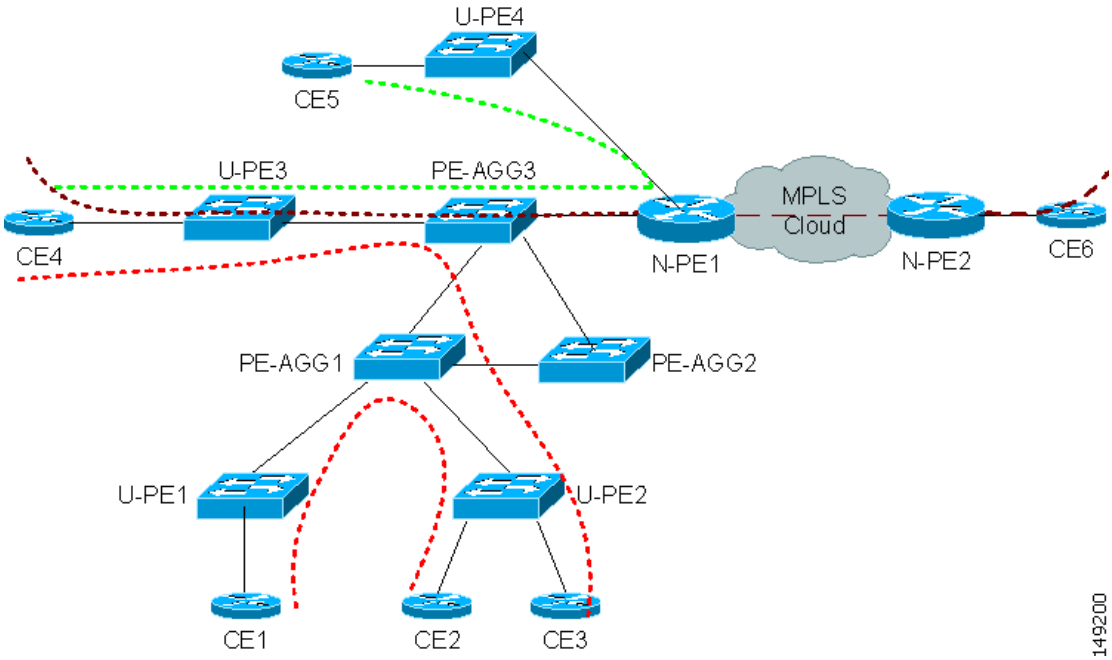


図 E-2 に、ディスカバリ プロセスの各フェーズを示します。

図 E-2　Prime Provisioning のディスカバリ ステップ

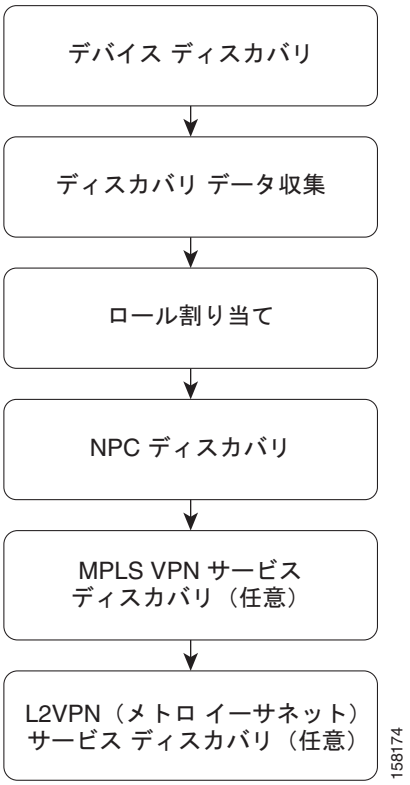


表 E-1 では、ディスカバリ プロセスのフェーズについて説明します。

表 E-1　ディスカバリ プロセスのステップ

ステップ	説明
デバイス ディスカバリ	MPLS VPN またはメトロ イーサネット トポロジあるいはその両方でデバイスを検出します。
ディスカバリ データ収集	検出されたデバイスの IOS コンフィギュレーションを収集します。
ロール割り当て	rules.xml に基づいて検出されたデバイスのロール割り当てが実行され、N-PE、U-PE、または CE として、デバイスのロールを編集するよう求められます。 **（注）** サンプルは $PRIMEP_HOME/resources/discovery/data/ にあります。rules.xml（ここに rules.xml ファイルが保持されている必要がある）。
NPC ディスカバリ	検出された NPC を表示し、NPC の追加または削除を許可します。
MPLS VPN ディスカバリ	MPLS VPN ネットワークのトポロジを検出し、必要に応じてその変更を許可します。 **（注）** Prime Provisioning Discovery with Prime Diagnostics を使用している場合、MPLS VPN ディスカバリ ステップは必要ありません。
L2VPN（Metro Ethernet）ディスカバリ	Metro Ethernet ネットワークのトポロジを検出し、必要に応じてその変更を許可します。 **（注）** Prime Provisioning Discovery with Prime Diagnostics を使用している場合、（L2VPN）Metro Ethernet ディスカバリ ステップは必要ありません。

次のディスカバリ操作は、Prime Provisioning でサポートされていません。

- IOS XR が動作しているデバイスでの MPLS VPN サービスの初回ディスカバリ
- MPLS VPN サービスへのイーサネット アクセス（U-PE、PE-AGG）の初回ディスカバリ
- VRF lite/MVRF の初回ディスカバリ
- マルチキャスト設定の VRF の初回ディスカバリ
- 固有ルート識別子を持つ MPLS VPN サービスの初回ディスカバリ
- インターフェイスに関連付けられていない VRF の初回ディスカバリ
- 1 つのインターフェイスに関連付けられ、検出されるデバイス間で他の VRF が稼働していない VRF の初回ディスカバリ。
- 検出されたエクストラネット（ユーザが手動で VPN を分割する場合を除く）
- ループバック インターフェイスに接続されている MPLS VPN/MLS VRF のディスカバリ

- Cisco 7600 シリーズ ルータの 12.2(33) SRB で導入された新しいイーサネット サービス インスタンス（EVC）の構文を使用しているサービスの初回ディスカバリ
- IOS XR が動作しているデバイスでの L2VPN サービスの初回ディスカバリ
- アクセス ポートを備えた ERS および ERMS サービスのディスカバリ（VLAN アクセスによるディスカバリだけをサポート）
- ATM やフレームリレー サービスのディスカバリ（イーサネット サービスのディスカバリだけをサポート）
- 段階的な NPC 同期
- 不一致の管理を含む再同期

Prime Provisioning ディスカバリのテクニカル ノート

ここでは、Prime Provisioning ディスカバリ プロセスに関する技術的なヒント、一般情報、および制約事項を示します。

Prime Provisioning ディスカバリ機能は、Prime Provisioning アプリケーション スイートに含まれる次の 3 つのアプリケーションのリポジトリ読み込みに使用できます。

- Prime Provisioning MPLS VPN Management
- Prime Provisioning L2VPN Management
- Prime Provisioning Prime Diagnostics

ステップは全体としてよく似ていますが、ディスカバリのタイプによってワークフローにいくつかの違いがあります。これらについては、各 Prime Provisioning アプリケーションに関する項で説明します。

- 「Prime Provisioning ディスカバリの Prime Provisioning MPLS VPN Management との使用」（P.E-7）
- 「Prime Provisioning ディスカバリの Prime Provisioning L2VPN Management との使用」（P.E-8）
- 「Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用」（P.E-8）
- 「Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用」（P.E-9）

（注） Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ インターフェイスおよびプロセスがあります。

この点については、*『Cisco Prime Provisioning 6.3 User Guide』* の TE ネットワーク検出で説明されています。

Prime Provisioning トラフィック エンジニアリング管理と Prime Provisioning MPLS VPN Management の両方を含むインストール環境での Prime Provisioning ディスカバリの使用に関するテクニカル ノートについては、「Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用」（P.E-9）を参照してください。

一般的な注意点

Prime Provisioning ディスカバリを実行する前に、次の点に注意してください。

- ディスカバリを実行する前に、Prime Provisioning GUI を使用して、プロバイダー、カスタマー、およびリソース プールを作成できます。
- 検出ワークフロー インターフェイスを制御できるのは、一度に 1 ユーザだけです。
- この章の手順には、「汎用」な手順を示します。特定のアプリケーションのライセンスがない場合は、Prime Provisioning ディスカバリのスタート画面に、そのアプリケーションの選択肢が表示されません。
- ディスカバリの終了後に、「手動」のデバイスの収集を実行します。
- ディスカバリ プロセスを開始した後、[Discovery Workflow] ウィンドウに [Restart] ボタンが表示されます。[Restart] ボタンをクリックすると、完了したステップのドロップダウン リストがポップ アップ表示されます。ステップを選択し、そのステップから再開できます。
- 初期化から再開すると、現在のディスカバリ プロセスが中止されます。
- Role Based Access Control（RBAC）を使用したディスカバリは、サポートされていません。

ディスカバリのログ ファイルの使用

ログ ファイルは、ディスカバリ プロセスの各フェーズに対して書き込まれます。[Discovery Workflow] ウィンドウの各ディスカバリ フェーズの概要の横にある [Log] 列で、[View] をクリックして、ログ ファイルを表示できます。

ログ ファイルは、ディスカバリ ステップが失敗したイベントに関して役立つ情報を提供します。

Prime Provisioning ディスカバリの Prime Provisioning MPLS VPN Management との使用

ディスカバリ プロセスを実行して、Prime Provisioning MPLS VPN Management で使用するために MPLS VPN ネットワークを検出する場合は、次の点に注意してください。

- ディスカバリ プロセスの主要なすべてのステップを実行する必要があります。
- CDP ディスカバリ、デバイス/トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス/トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- Prime Provisioning はパーシャル メッシュ VPN トポロジをサポートしていません。ディスカバリ プロセスがパーシャル メッシュ VPN を検出した場合、より小さな単位（通常は完全メッシュ VPN とハブ アンド スポーク VPN の組み合わせ）にパーシャル メッシュ VPN を分割する必要があります。
- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Operate] > [Tasks] > [Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

（注） MPLS サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning ディスカバリの Prime Provisioning L2VPN Management との使用

ディスカバリ プロセスを実行して、Prime Provisioning L2VPN Management を使用してプロビジョニングおよび管理される L2VPN ネットワークを検出する場合は、次の点に注意してください。

- ディスカバリ プロセスの主要なすべてのステップを実行する必要があります。
- CDP ディスカバリ、デバイス/トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス/トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- 新しい L2VPN サービスは、Prime Provisioning にあるサービスと比較して、次のいずれかが見つかった場合に検出されます。
  - イーサネット コア（イーサネット アクセス ドメイン）内の新しい仮想 LAN ID（VLAN ID）
  - MPLS コアの Virtual Private Wire Services（VPWS）サービスに対する新しい Virtual Circuit Identifier（VC ID）。
  - MPLS コアの Virtual Private LAN Service（VPLS）サービスに対する新しい VPLS Forwarding Instance Identifier（VFI ID）。
- Prime Provisioning L2VPN Management のディスカバリ プロセスは、MPLS コア、イーサネット コア、またはその両方の Metro Ethernet を検出できます。
- Prime Provisioning L2VPN Management のために NPC ディスカバリ ステップを実行する前に、N-PE デバイスのアクセス ドメインを指定する必要があります。
- Existing Modified または Conflicting としてマークされた NPC で設定済みの新しいリンクは、検出されません。
- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

（注） L2VPN サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用

ディスカバリ プロセスを実行して、Prime Diagnostics で使用するために MPLS VPN ネットワークを検出する場合は、次の点に注意してください。

- CDP ディスカバリ、デバイス/トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス/トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- Prime Provisioning Prime Diagnostics では、デバイスの検出、ディスカバリ データ収集、およびロールの割り当てのステップだけを実行する必要があります。NPC ディスカバリ ステップまたはサービス ディスカバリ ステップを実行する必要はありません。ただし、NPC ディスカバリ プロセスを実行させることはできます。

  Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用に必要なステップのフローチャートについては、図 E-5 を参照してください。

- Prime Provisioning Prime Diagnostics を使用している場合は、通常、P および PE デバイスだけを検出する必要があります。したがって、検出したデバイスに対してロール割り当てのステップを実行する場合は、P および PE デバイスだけにロールを割り当てる必要があります。

（注）　CE デバイスを検出する場合は、CE ロールを割り当てる必要があります。

- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用

通常、Prime Provisioning トラフィック エンジニアリング管理を使用している場合、Prime Provisioning ディスカバリ プロセスを実行する必要はありません。Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ プロセスがあります。このプロセスは、*『Cisco Prime Provisioning 6.3 User Guide』* の TE ネットワーク検出で説明されています。

ただし、Prime Provisioning Traffic Engineering Management（TEM）と Cisco IP solution Center MPLS VPN Management の*両方*を稼働させている場合、Prime Provisioning MPLS VPN Management のためにディスカバリ プロセスを実行する必要があります。

次の点に注意してください。

- 1 つのリージョン（デフォルト リージョン）が TEM のために使用されます。
- また、MPLS VPN Management のために Prime Provisioning ディスカバリを実行している場合は、この章で説明したディスカバリ ワークフローを*先に*実行し、Prime Provisioning トラフィック エンジニアリング管理プロセスを後で実行します。

ディスカバリのタスクの概要（Prime Provisioning MPLS VPN Management および L2VPN Management）

図 E-3 には、Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management アプリケーションで使用されるディスカバリ プロセスの一般的なワークフロー図を示します。

（注）　図 E-5 には、Prime Diagnostics アプリケーションで使用されるディスカバリ プロセスの一般的なワークフロー図を示します。

図 E-3　Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management でのディスカバリの基本ワークフロー

表 E-2 では、Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management のためのディスカバリ ワークフローの各タスクについて説明します。

表 E-2　MPLS VPN および L2VPN Management のディスカバリ ステップの説明

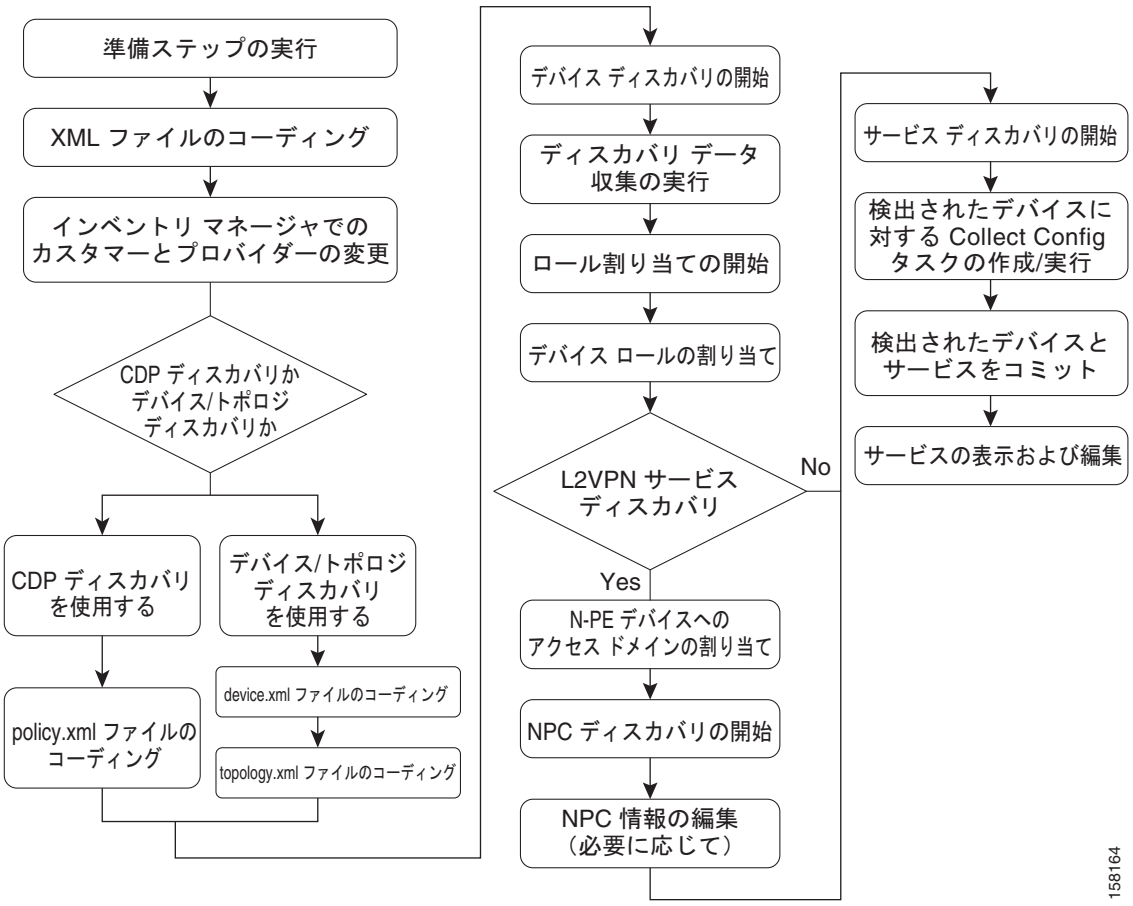
ステップ	説明
ステップ 1：準備ステップの実行	Prime Provisioning ディスカバリに必要な準備ステップを実行します。「ステップ 1：予備ステップの実行」（P.E-16）を参照してください。 • システム要件の確認 「システム要件の確認」（P.E-17）を参照してください。 • ライセンスのインストール 「ライセンスのインストール」（P.E-18）を参照してください。 • （CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認 「（CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認」（P.E-18）を参照してください。 • （CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認 「（CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認」（P.E-19）を参照してください。 • ディスカバリに必要な XML ファイルのコーディング 「ディスカバリに必要な XML ファイルのコーディング」（P.E-20）を参照してください。
ステップ 2：デバイス ディスカバリの実行	• デバイス ディスカバリの開始 「デバイス ディスカバリの開始」（P.E-27）を参照してください。 • デバイス ディスカバリの完了後に、デバイスのパスワードを入力します。 デバイスのパスワードの入力については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。 • 必要に応じて、他のデバイス情報を入力します。 「一般デバイス属性の設定」（P.E-32）および「Cisco CNS 属性の設定」（P.E-33）を参照してください。
ステップ 3：ディスカバリ データ収集の実行	コンフィギュレーションの収集を開始します。このステップに必要な入力はありません。「ステップ 3：ディスカバリ データ収集の実行」（P.E-33）を参照してください。
ステップ 4：ロール割り当ての実行	各デバイスにデバイス ロールを割り当てます。「ステップ 4：ロール割り当ての実行」（P.E-34）を参照してください。

表 E-2　MPLS VPN および L2VPN Management のディスカバリ ステップの説明 （続き）

ステップ	説明
ステップ 5：NPC ディスカバリの実行	イーサネット コアの Metro Ethernet ネットワークを検出する場合は、必要な準備ステップを実行します。「メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ」（P.E-43）を参照してください。 • NPC ディスカバリの実行 「ステップ 5：NPC ディスカバリの実行」（P.E-43）を参照してください。 • 必要に応じて、NPC を変更または追加します。 「NPC へのデバイスの追加」（P.E-46）、「リングの追加」（P.E-46）、「デバイスの挿入」（P.E-46）、「リングの挿入」（P.E-47）、または「デバイスやリングの削除」（P.E-47）を参照してください。
ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）	MPLS VPN サービス ディスカバリを開始します。「ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）」（P.E-47）を参照してください。 このステップは、Prime Provisioning MPLS VPN Management アプリケーションで必要です。 **（注）** Prime Provisioning L2VPN Management アプリケーションや Prime Provisioning Prime Diagnostics アプリケーションの場合、このステップは必要ありません。
ステップ 7：L2VPN サービス ディスカバリの実行（任意）	L2VPN サービス ディスカバリを開始します。「ステップ 7：L2VPN（メトロ イーサネット）サービス ディスカバリの実行（任意）」（P.E-53）を参照してください。 このステップは、Prime Provisioning L2VPN Management アプリケーションで必要です。 **（注）** Prime Provisioning MPLS VPN Management アプリケーションや Prime Provisioning Prime Diagnostics アプリケーションの場合、このステップは必要ありません。
ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット	検出されたデバイスとサービスを Prime Provisioning リポジトリにコミットします。このステップの前に、検出ワークフローは検出されたデバイスとサービスを、検出ワークフローの最後のステップでだけ Prime Provisioning にコミットされる一時リポジトリに格納します。
ステップ 9：検出されたデバイスのコンフィギュレーション収集タスクの作成および実行	[Prime Provisioning Start] ページから、[Operate] > [Tasks] > [Task Manager] と選択します。[Collect Config] タスクを選択し、デバイス ディスカバリ ステップで検出されたデバイスすべてを選択してから、タスクを送信します。 「ステップ 9：検出されたデバイスへのコンフィギュレーション収集タスクの作成と実行」（P.E-60）を参照してください。
ステップ 10：サービスの表示と編集	検出されたサービスは保留状態になり、[Deployed] 状態に移行するにはコンフィギュレーション監査を実行する必要があります。「ステップ 10：サービスの表示と編集」（P.E-61）を参照してください。

各ステップで、追加のタスクを実行し、選択を行う必要があります。図 E-4 には、ディスカバリ ワークフローのすべてのステップを説明する詳細フローチャートを示します。

図 E-4　ディスカバリ ステップの詳細図（Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management）



Prime Diagnostics の Prime Provisioning ディスカバリ ステップの概要

図 E-5 では、Prime Diagnostics アプリケーションでの Prime Provisioning に対する基本ディスカバリ ステップを示します。Prime Diagnostics では、Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management で必要ないくつかのステップは必要ありません。

図 E-5　Prime Diagnostics アプリケーションのディスカバリ ワークフロー

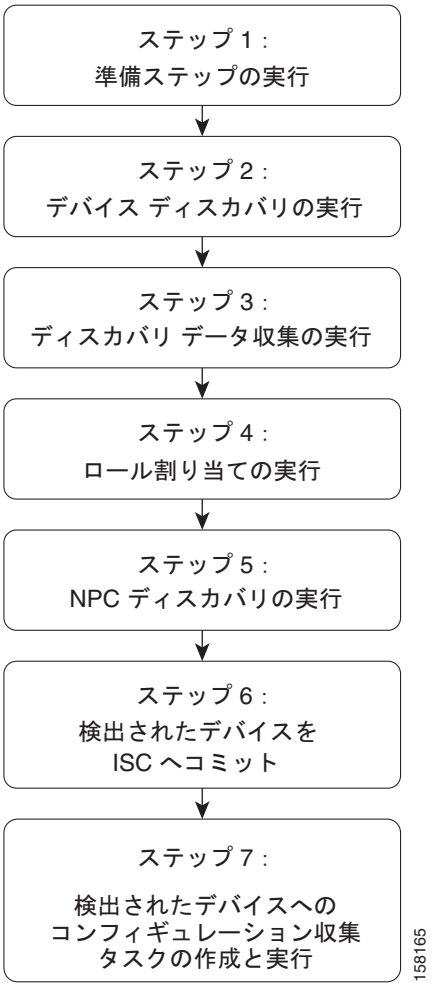


表 E-3　Prime Diagnostics のディスカバリ ステップの説明

ステップ	説明
ステップ 1：準備ステップの実行	Prime Provisioning ディスカバリに必要な準備ステップを実行します。 • システム要件の確認 「システム要件の確認」（P.E-17）を参照してください。 • ライセンスのインストール 「ライセンスのインストール」（P.E-18）を参照してください。 • ディスカバリに必要な XML ファイルのコーディング 具体的な手順については、次の項を参照してください。 – 「ディスカバリに必要な XML ファイルのコーディング」（P.E-20）。
ステップ 2：デバイス ディスカバリの実行	• デバイス ディスカバリの開始 「デバイス ディスカバリの開始」（P.E-27）を参照してください。 • デバイス ディスカバリの完了後に、デバイスのパスワードを入力します。 デバイスのパスワードの入力については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。 • 必要に応じて、他のデバイス情報を入力します。 「一般デバイス属性の設定」（P.E-32）および「Cisco CNS 属性の設定」（P.E-33）を参照してください。
ステップ 3：ディスカバリ データ収集の実行	コンフィギュレーションの収集を開始します。このステップに必要な入力はありません。「ステップ 3：ディスカバリ データ収集の実行」（P.E-33）を参照してください。

表 E-3　Prime Diagnostics のディスカバリ ステップの説明 （続き）

ステップ	説明
ステップ 4：ロール割り当ての実行	各デバイスにデバイス ロールを割り当てます。「ステップ 4：ロール割り当ての実行」（P.E-34）を参照してください。 Prime Diagnostics の場合、検出されるのは通常 P および PE だけで、割り当てるのも P および PE ロールだけです。しかし、CE が検出された場合、CE デバイスには CE ロールを割り当てます。 **（注）** Prime Diagnostics の NPC を編集する必要はありませんが、ロール割り当てを実行した後に、このステップを完了する必要があります。
ステップ 5：検出されたデバイスのコンフィギュレーション収集タスクの作成および実行	[Prime Provisioning Start] ページから、[Operate] > [Tasks] > [Task Manager] と選択します。[Collect Config] タスクを選択し、デバイス ディスカバリ ステップで検出されたデバイスすべてを選択してから、タスクを送信します。 「ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット」（P.E-60）を参照してください。

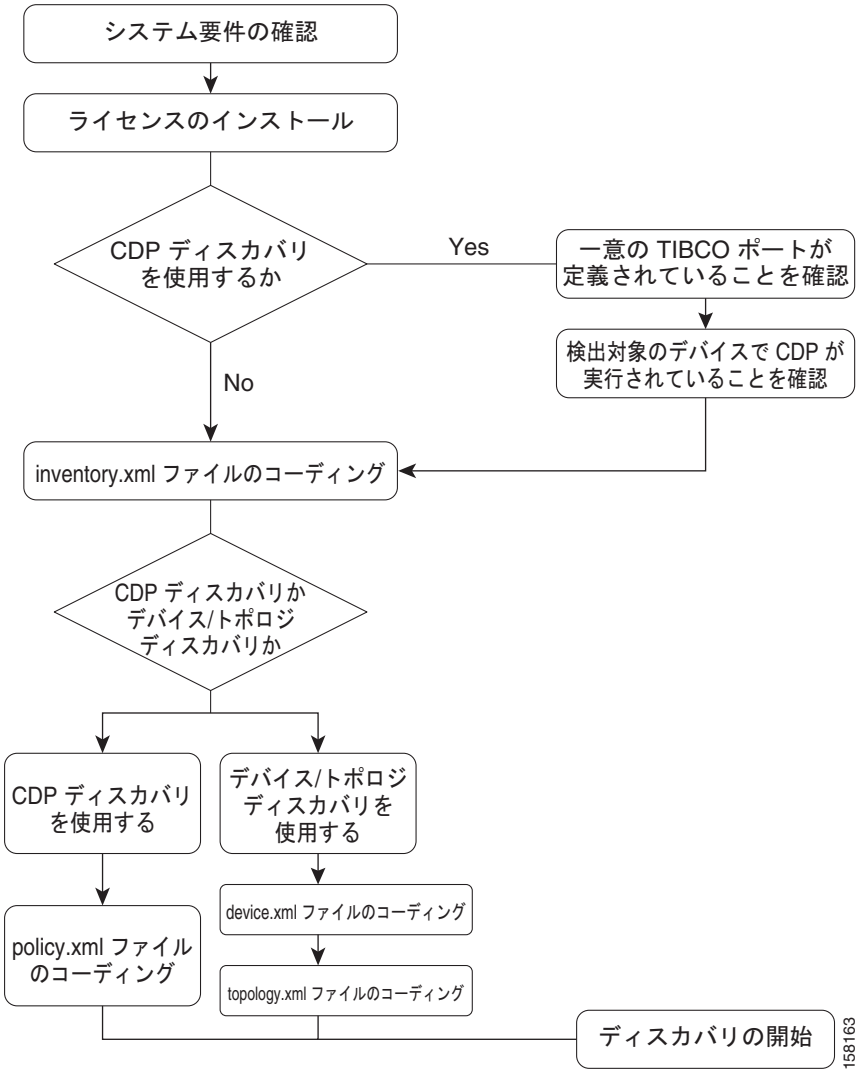
ステップ 1：予備ステップの実行

Prime Provisioningディスカバリ プロセスを開始する前に、次の準備ステップを完了します。

- システム要件の確認
- ライセンスのインストール
- 大規模ネットワークでのディスカバリ
- （CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認
- （CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認
- ディスカバリに必要な XML ファイルのコーディング

図 E-6 に、Prime Provisioning ディスカバリの準備ステップの概要を示します。

図 E-6　ディスカバリの準備ステップの概要



システム要件の確認

インストールの計画前に Prime Provisioning のシステム要件を十分に確認し、インストールを成功させるために必要なハードウェアとソフトウェアがすべて揃っていることを確認することを推奨します。

Prime Provisioning に対するシステムの推奨事項および要件は、*『Cisco Prime Provisioning 6.3 Installation Guide』*の第 1 章「System Recommendations」と、*『Cisco Prime Provisioning 6.3 Release Notes』* に示されています。

ライセンスのインストール

検出を開始する前に、適切なライセンス（アクティベーションと VPN ライセンスの両方）をインストールする必要があります。また、各ライセンスは、すべての検出されうるオブジェクトを処理するために、十分な規模にする必要があります。ライセンスのインストールの詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』* の第 2 章の「Installing License Keys」項、「Installing and Logging In to Prime Provisioning」を参照してください。

大規模ネットワークでのディスカバリ

トポロジが複雑な大規模なネットワークを検出するには、次のように 2 つの DCPL プロパティをリセットすることを推奨します。

ステップ 1　Dynamic Component Properties Library（DCPL）プロパティに移動する方法については、Appendix B, “Property Settings” を参照してください。

ステップ 2　プロパティ **watchdog\server\discovery\heartbeat\timeout** に移動し、このプロパティを **180000 milliseconds**（3 分）に設定します。

ステップ 3　プロパティ **watchdog\server\discovery\java\flags** に移動し、このプロパティを **-Xmx3072m -XX:PermSize=256m -XX:MaxPermSize=512m** に設定します。

ステップ 4　Prime Provisioning サーバを再起動します。

ヒープとは、L2VPN と Metro Ethernet、レイヤ 3 MPLS VPN、および TEM コンポーネントに対するメモリ セグメントのブロックです。これは、Java Virtual Machine（JVM）プロセスによる使用のために実行時に割り当てられます。これは、大規模な展開では、増大させる必要が生じることがあります。**httpd** プロセスが再起動する場合、次のようにヒープのサイズを大きくします。

ステップ 1　**cd $PRIMEP_HOME/bin**

ステップ 2　**vi tomcat.sh**

ステップ 3　**-Xmx** がある行を検索し、より高い値を指定します。

ステップ 4　**-Xmx512m** を **-Xmx1024m** または **-Xmx2048m** に置き換えて、ヒープ サイズを 1GB または 2GB に設定します。

ステップ 5　**tomcat.sh** ファイルを保存します。

ステップ 6　**stopall** と入力して Prime Provisioning サーバを停止します。

ステップ 7　Prime Provisioning サーバを起動するために **startwd** と入力します。

（CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認

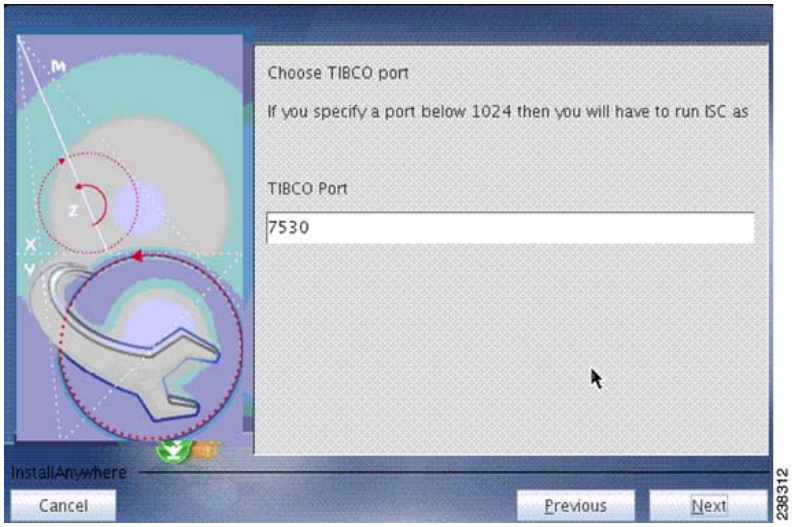
ネットワーク トポロジのディスカバリに CDP ディスカバリを使用している場合、TIBCO ポートが一意であることを確認します。一意でない場合、CDP ディスカバリは失敗します。

インストール プロセスの開始時に「カスタム」インストール タイプを選択した場合は、インストール中に、TIBCO ポートを指定できます。それ以外の場合、インストールされるデフォルト ポートは 7530 です。[Choose TIBCO Port] ダイアログで TIBCO ポートを指定します。

指定するポート番号は、ネットワーク全体で一意である必要があり、その他の Prime Provisioning インストールで同じポートを使用することはできません。

図 E-7 には、[Choose TIBCO Port] ダイアログを示します。

図 E-7　Choose TIBCO Port



Tibco ポートは、インストールの後に、Appendix B, “Property Settings” で指定する Dynamic Component Properties Library エントリの /SYSTEM/tibco/port を修正することにより、インストール後に変更できます。

（CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認

CDP ディスカバリを使用する場合は、**show cdp** コマンドを使用して、ディスカバリの対象となるすべてのデバイスで CDP が実行されていることを確認します。

例 E-1 に示すように、デバイスごとに、**show cdp** コマンドを入力します。

例 E-1　show cdp コマンド：

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
Router#
```

（注）　複数の IP アドレスが設定されているデバイスに対して CDP ディスカバリを実行する場合は、CDP ディスカバリによって、管理 IP アドレス以外の IP アドレスが検出される場合があります。検出された IP アドレスが Prime Provisioning サーバからアクセスできない場合、CDP ディスカバリを使用して、そのデバイスを検出することはできません。

ディスカバリに必要な XML ファイルのコーディング

Prime Provisioning ディスカバリの実行前に、ディスカバリ プロセスに必要な XML ファイルをコーディングしておく必要があります。CDP ディスカバリまたはデバイス / トポロジ ベースのディスカバリのいずれを使用するかに応じて、異なるファイルのセットが必要です。

表 E-4 では、XML ファイルについて説明し、各タイプのディスカバリ方式に対して必要なファイルを示します。

表 E-4　Prime Provisioning ディスカバリで使用される XML ファイル

XML ファイル	説明	CDP ディスカバリに必要	デバイス / トポロジ ベースのディスカバリに必要
policy.xml	指定シード デバイスから到達可能な 1 つ以上のシード IP アドレスおよびデバイス ディスカバリ プロセスの最大ホップ カウントを指定します。	Yes	No
device.xml	デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。	No	Yes
topology.xml	MPLS VPN またはメトロ イーサネット トポロジあるいはその両方で使用される NPC の構築に使用する情報を指定します。	No	Yes

（注）　XML ファイルのコーディングが正しいことを確認します。ファイルにエラーがある場合、ディスカバリ プロセスを再実行する必要が生じる場合があります。

サンプル XML ファイル

Prime Provisioning の初回インストールでは、独自の XML ファイルのコーディングで開始点として使用できるサンプル XML ファイルが提供されます。サンプル XML ファイルは、次のディレクトリにあります。

<*install_directory*>/resources/discovery/sample

ここで、<*install_directory*> は、Prime Provisioning インストール プログラムによって要求されたときに指定したインストール ディレクトリです。

policy.xml ファイルのコーディング

policy.xml ファイル：

- CDP ディスカバリに必要です。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics で必要です。
- デバイス / トポロジ ベースのディスカバリでは必要ありません。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- シード デバイスの近くのデバイスを検出するために CDP プロトコルが使用するシード IP アドレスを提供します。

例 E-2 は、Prime Provisioning インストール時に準備されているサンプル **policy.xml** ファイルです。

例 E-2　　サンプル policy.xml ファイル

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.232" hop="1"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

ネットワークのコア セグメントのエッジで、PE ルータの反対側に追加のルータがある場合、これらのデバイスを検出するために複数のシード IP アドレスを指定できます。

例 E-3 は、2 つのシード IP アドレスを持つ **policy.xml** ファイルです。

例 E-3　　2 つの IP アドレスを持つ Policy.xml ファイル

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.241" hop="8"/>
  </DISCOVERY_METHOD>
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.244" hop="8"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

表 E-5 で、**policy.xml** ファイルで使用する XML タグについて説明します。

表 E-5　policy.xml ファイルで使用する XML タグと属性

タグ	説明
<DISCOVERY_METHOD>	**<DISCOVERY_METHOD>** タグを開始します。 **<DISCOVERY_METHOD>** タグには **<CDP>** タグを含める必要があります。
<CDP>	**<CDP>** タグを開始します。**<CDP>** タグは、シード IP アドレスとホップ カウントを指定します。 **<CDP>** タグには、次の属性を含める必要があります。 • **ipaddress** • **hop**
ipaddress	シード デバイスの IP アドレスを指定します。**<CDP>** タグの必須属性です。
hop	デバイスを検出するときに、ipaddress 属性によって指定されたデバイスから何ホップまでを対象とするかを指定します。**<CDP>** タグの必須属性です。

サンプル **policy.xml** ファイルの編集は、次のステップを実行します。

ステップ 1　サンプル ファイルを編集し、**ipaddress** XML 属性で指定された IP アドレスを、ご使用のネットワークの適切な IP アドレスに置き換えます。

この IP アドレスは、Prime Provisioning ホストから到達可能なデバイスです。それぞれのシード デバイスについて、出発点でアクセス可能なインターフェイスが設定されます。管理インターフェイスが必要なためです。管理インターフェイスは、Prime Provisioning ホストがデバイスに到達するために使用する、デバイス上のアドレスです。

（注）　複数の IP アドレスを指定できます。これは、1 つのネットワーク ドメインが、ネットワークのコア セグメントのエッジで、PE ルータの反対側にある場合に便利です。

ステップ 2　**hop** 属性で指定されたホップ カウントを編集し、ディスカバリ プロセスが初期化されるときに使用されるホップ カウントを指定します。

シード デバイスとホップ カウントを選択する場合は、ネットワークの大規模なセクションに到達できるシード デバイスを選択します。これらのデバイスによって、管理対象ネットワーク全体にアクセスすることができると考えられるまで、1 つ以上のシード デバイスを選択します。

通常、Point Of Presence（POP）ルータを選択できます。シード デバイスの集合としてネットワークのすべての POP を選択し、適切な数のハブを配置した場合、管理対象ネットワーク全体が検出されます。

ホップ カウント数を選ぶには、関連付けられた POP から最も遠い CE まで移動するときに、その間にあるデバイスの数を数えます。シードとして POP を選択している場合、この値が N であれば、ハブの数は N+1 です。

ステップ 3　シード デバイスに IP アドレスを追加する必要がある場合は、追加の **<DISCOVERY_METHOD>** タグをコーディングします。

追加の **<DISCOVERY_METHOD>** タグには、**<CDP>** タグを含めます。

各 **<CDP>** タグでは、**ipaddress** 属性で IP アドレスを指定し、**hops** 属性でホップ カウントを指定します。

ステップ 4　**policy.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

ディスカバリ プロセスの実行中、プロセスは出発点デバイスを CDP テーブルに問い合わせます。このテーブルから、すべてのデバイスの CDP 情報が問い合わせされます。このプロセスは、開始点から最大ホップ カウントに達するまで続きます。CDP ベースの方法で検出されるのは CDP が稼働中のデバイスだけであることに注意してください。

device.xml ファイルのコーディング

device.xml ファイル：

- デバイス / トポロジ ベースのディスカバリで必要です。
- CDP ベースのディスカバリでは必要ありません。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics で必要です。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。

例 E-4 に **device.xml** ファイルの例を示します。サンプル ファイルを例として使用し、編集したファイルを適切なディレクトリに保存します。

例 E-4　サンプル device.xml ファイル

```
<network>
<device>
<device-name>mlpe8</device-name>
<ip-address>209.168.133.244</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.509</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw11</device-name>
<ip-address>209.168.133.170</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw16</device-name>
<ip-address>209.168.133.175</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw17</device-name>
<ip-address>209.168.133.176</ip-address>
```

```
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

</network>
```

表 E-6 で、**device.xml** ファイルで使用する XML タグについて説明します。

表 E-6　device.xml ファイルで使用する XML タグ

タグ	説明
<device>	**<device>** タグを開始します。**<device>** タグには、次のタグを含める必要があります。 • **<device-name>** • **<ip-address>** 次のタグは、**<device>** タグ内で使用する任意のタグです。 • **<system-object-id>** • **<snmp-info>**
<device-name>	デバイス名を指定します。**<device>** タグ内で必須です。
<ip-address>	デバイスの IP アドレスを指定します。**<device>** タグ内で必須です。
<system-object-id>	（任意）使用するとデバイスに SNMP Object ID（OID; オブジェクト ID）を指定できます。これを指定すると、**<device>** タグ内に指定されます。
<snmp-info>	デバイスの SNMP 情報を指定します。**<snmp-info>** タグには、**<ro-community>** タグを含める必要があります。**<device>** タグ内では任意です。
<ro-community>	デバイスの SNMP アクセスのレベルを指定します。通常は「public」とします。**<snmp-info>** タグ内で必須です。
注：SNMPv3 はサポートされていません。	

次のステップに従って、**device.xml** ファイルをコーディングします。

ステップ 1　インストール時に準備されている **device.xml** ファイルを編集します。

ステップ 2　Prime Provisioning で検出するデバイスのそれぞれに、**<device>** エントリをコーディングします。

各 **<device>** エントリには、次のタグを含める必要があります。

- デバイス名を指定する **<device-name>** タグ。
- デバイスの IP アドレスを指定する **<ip-address>** タグ。
- デバイスの OID を指定する **<system-object-id>** タグ（任意）。
- **<ro-community>** 情報を指定する **<snmp-info>** タグ。

ステップ 3　**device.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

topology.xml ファイルのコーディング

topology.xml ファイルについて：

- デバイス / トポロジ ベースのディスカバリで必要です。
- CDP ベースのディスカバリでは必要ありません。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics の Prime Provisioning ディスカバリ実行に必要です。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。

topology.xml ファイルは、ディスカバリ プロセスで使用するディスカバリ プロトコルを指定し、各接続に対して、開始 IP アドレス、開始インターフェイス、エンド デバイス、および最後のインターフェイスを指定します。

例 E-5 には、サンプル **topology.xml** ファイルを示します。サンプル ファイルを例として使用し、編集したファイルを適切なディレクトリに保存します。

例 E-5　サンプル topology.xml ファイル

```
<topology>
<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="GigabitEthernet1/1/2"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="GigabitEthernet1/1/1" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/23"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="FastEthernet1/0/24" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet
1/0/24"   toDevice="mlsw18"  toIP="209.168.133.177"  toIF="FastEthernet1/0/23" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/22"   toDevice="mlsw22"  toIP="209.168.133.221"
toIF="FastEthernet1/0/24" >
</connection>

</topology>
```

表 E-7 で、**topology.xml** ファイルで使用する XML タグについて説明します。

表 E-7　topology.xml ファイルで使用する XML タグと属性

タグ	説明
<connection>	**<connection>** タグを開始します。**<connection>** タグでは、次の属性を指定する必要があります。 • **discovery-protocol** • **fromDevice** • **FromIP** • **FromInterface** • **toDevice** • **toIP** • **toIF**
discovery-protocol	ネットワーク トポロジを検出する際に使用する検出プロトコルを指定します。通常は「CDP」です。
fromDevice	名前付き物理回線の開始元のデバイス名を指定します。**<connection>** タグの必須属性です。
FromIP	名前付き物理回線の開始元デバイスの管理 IP アドレスを指定します。**<connection>** タグの必須属性です。
FromInterface	名前付き物理回線の開始元のデバイス インターフェイス名を指定します。**<connection>** タグの必須属性です。
toDevice	名前付き物理回線の接続先デバイス名を指定します。**<connection>** タグの必須属性です。
toIP	名前付き物理回線の接続先デバイスの管理 IP アドレスを指定します。**<connection>** タグの必須属性です。
toIF	名前付き物理回線の接続先デバイス上で、デバイス インターフェイスを指定します。**<connection>** タグの必須属性です。

次のステップに従って、**topology.xml** ファイルをコーディングします。

ステップ 1　インストール時に準備されている **topology.xml** ファイルを編集します。

ステップ 2　Prime Provisioning で検出する NPC 接続のそれぞれに、**<connection>** エントリをコーディングします。

各 **<connection>** エントリには、次のタグを含める必要があります。

- CDP プロトコルを指定する **discovery-protocol** 属性。
- NPC の開始元のデバイスを指定する **fromDevice** 属性。
- NPC の開始元の管理 IP アドレスを指定する **FromIP** 属性。
- NPC の開始元のデバイス インターフェイスを指定する **FromInterface** 属性。
- NPC の接続先デバイスの名前を指定する **toDevice** 属性。

- NPC の接続先デバイスの管理 IP アドレスを指定する **toIP** 属性。
- NPC の接続先デバイス上のインターフェイス名を指定する **toIF** 属性。

ステップ 3　**topology.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

ステップ 2：デバイス ディスカバリの実行

この項では、デバイス ディスカバリ プロセスの開始方法と、デバイス コンフィギュレーションの編集方法について説明します。

デバイス ディスカバリの開始

ディスカバリを開始するには、次のステップを実行します。

ステップ 1　Prime Provisioning にログインします。

ステップ 2　[Inventory] > [Physical Inventory] > [Discovery] とクリックします。

[Device Discovery — CDP Fields] ウィンドウが表示されます。

初期状態では、ディスカバリ方式として [CDP] が選択され、この方式に必要な入力内容がウィンドウに表示されています。

編集可能な [Output Device File] フィールドはオプションで、検出されたデバイスの XML ファイルにデフォルトで設定されています。このファイルは、[Device/Topology] オプション ボタンを選択してデバイス / トポロジ オプションを使用したディスカバリの再実行を行う場合の入力 [Devices File] となります。

編集可能な **Output Connection File** は任意であり、CDP デバイス ディスカバリ中に書き込まれるデバイス接続情報を含む XML ファイルにデフォルト設定されます。このファイルは、[Device/Topology] オプション ボタンを選択してデバイス / トポロジ オプションを使用したディスカバリの再実行を行う場合の入力 [NPC Topology File] となります。

ステップ 3　ディスカバリ方式を選択します。

- Cisco Discovery Protocol（CDP）方式を使用するには、[CDP] オプション ボタンをクリックします。
- デバイス / トポロジ方式を使用するには、[Device/Topology] ボタンをクリックします。
- インポート コンフィギュレーション ファイル方式を使用するには、[Import Configuration Files] ボタンをクリックします。

必須の [Directory] フィールドは、検出するデバイスのコンフィギュレーション ファイルが格納された、サーバ上のディレクトリです。これらのファイルの形式は、*必ず* <*filename*>**.cfg** である必要があります。

[NPC Topology File] フィールドの内容は、NPC を自動作成するために使用するデバイス接続情報が含まれている XML ファイルです。

（注）　サービス ディスカバリ中、プロバイダー、リージョン、カスタマー、サイトは自動作成されません。そのため、サービス ディスカバリの実行前に手動で作成しておく必要があります。Prime Provisioning のプロビジョニングでリソース プールが使用される場合、アクセス ドメインとリソース プールはサービス ディスカバリの実行前に手動で作成しておく必要があります。

ステップ 4　[Discovery] ウィンドウで、表 E-8 に示す設定を指定します。

表 E-8　ディスカバリ設定

設定	説明
Name	このフィールドには、ワークフロー名に対して選択した一意の名前を入力します。このフィールドに名前を入力しない場合、システムが一意の名前を生成します。
CDP	このオプション ボタンをクリックして、Cisco Discovery Protocol（CDP）をディスカバリ方式として選択します。
Policy File	[CDP] ボタンをクリックした場合、**policy.xml** ファイルのパスをここで指定します。このファイルは、ディスカバリ プロセスで出発点として使用する 1 つ以上のデバイスの IP アドレスを指示する XML ファイルです。 **policy.xml** ファイルの詳細については、「policy.xml ファイルのコーディング」（P.E-20）を参照してください。
Output Device File	この編集可能なフィールドの設定は任意で、検出されたデバイスの XML ファイルにデフォルト設定されています。このファイルは、[Device/Topology] オプションを使用したディスカバリの再実行を行う場合の入力 [Devices File] にできます。
Output Connection File	この編集可能なフィールドの設定は任意で、CDP デバイス ディスカバリの間に書き込まれたデバイス接続情報を含む XML ファイルにデフォルト設定されています。このファイルは、[Device/Topology] オプションを使用したディスカバリの再実行を行う場合の入力 [NPC Topology File] にできます。
Device/Topology	このオプション ボタンをクリックして、ディスカバリ方式としてデバイス / トポロジを選択します。

表 E-8　ディスカバリ設定 （続き）

設定	説明
Devices File	[Device/Topology] ボタンをクリックした場合、**device.xml** ファイルのパスをここで指定します。このファイルには、IP アドレスや OID など、ネットワーク内でデバイスを位置づけるための情報が含まれています。 **device.xml** ファイルの詳細については、「device.xml ファイルのコーディング」（P.E-23）を参照してください。
NPC Topology File	オプションのこの [Device/Topology] ボタンをクリックした場合、**topology.xml** ファイルのパスをここで指定します。このファイルには、ネットワークの NPC トポロジを判定するために使用される情報が含まれます。 **topology.xml** ファイルの詳細については、「topology.xml ファイルのコーディング」（P.E-25）を参照してください。
Import Configuration Files	このオプション ボタンをクリックして、ディスカバリ方式としてインポート コンフィギュレーション ファイルを選択します。
Directory	この必須フィールドは、検出するデバイスのコンフィギュレーション ファイルが格納された、サーバ上のディレクトリです。これらのファイルの形式は、*必ず* <*filename*>**.cfg** である必要があります。
NPC Topology File	このフィールドには、NPC を自動作成するために使用するデバイス接続情報の XML ファイルが含まれます。
MPLS VPN	MPLS VPN サービスでデバイスを検出するには、[MPLS VPN] オプション ボタンをクリックします。
L2VPN (Metro Ethernet) Discovery	メトロ イーサネット サービスで使用されるレイヤ 2 デバイスを検出するには、[L2VPN (Metro Ethernet) Discovery] オプション ボタンをクリックします。

ステップ 5　[Start] ボタンをクリックします。

ディスカバリ プロセスが開始され、[Discovery Workflow] ウィンドウが表示されます。

データ ペインの [Workflow] カテゴリに、現在のディスカバリ要求や検出ワークフローについての名前情報が表示されます。

[Restart] ボタンをクリックすると、完了したステップのドロップダウン リストが表示されます。ステップを選択すると、そのステップから再開します。

左側の列で、[Current Request] には現在実行中のディスカバリ要求や検出ワークフローが表示されます。現在実行中のディスカバリ要求やワークフローがない場合、初期化ウィンドウが開いて新規のディスカバリ要求やワークフローを作成できます。

左側の列で、[Previous Requests] には検出された要求やワークフローがすべてリストされます。ディスカバリ要求や検出ワークフローそれぞれについて、ステータスやログを参照できます。

[Discovery Workflow] ウィンドウには、デバイス ディスカバリの各フェーズの進行状況が表示されます。

- このウィンドウが最初に開いたとき、ステータス インジケータは黄色で、デバイス ディスカバリ プロセスが初期化中（[Initializing]）であることを示します。
- その後、ステータス インジケータはプロセスが進行中（[In Progress]）であることを示します。
- ディスカバリ プロセスが完了すると、ディスプレイには検出されたデバイス数が表示され、ステータス インジケータはオレンジに変わり、入力待ち（[Pending Input]）であることを示します。

ウィンドウ下部の [Progress] エリアには、検出されたデバイス数が表示されます。

ウィンドウの右下には、[Restart] ボタンがあります。このボタンをクリックすると、ディスカバリ プロセス全体を再起動できます。ただし、ディスカバリ プロセスを再起動すると、ディスカバリの再起動前の作業内容はすべて失われます。

（注）　ディスカバリ プロセスの各フェーズ後に、プロセスにエラーがないことを確認するためにログ ファイルをチェックします。具体的な手順については、「ディスカバリのログ ファイルの使用」（P.E-7）を参照してください。

デバイス コンフィギュレーションの編集

ネットワークのデバイスの初回ディスカバリ終了後、Prime Provisioning のデバイスについての情報を編集する必要があります。こうすることで、ディスカバリ プロセスはネットワーク トポロジを判定し、サービス要求を生成するために必要となる、デバイスについてのコンフィギュレーション情報を収集できます。

デバイス コンフィギュレーションの編集には、次のようなステップがあります。

- パスワード属性の設定（必須ステップ）
- 一般デバイス属性の設定
- Cisco CNS 属性の設定

デバイス コンフィギュレーションを編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリが [Pending Input] であると [Discovery Workflow] ウィンドウに表示されたら、[Continue] ボタンをクリックします。

[General Attributes - Devices] ウィンドウが表示されます。

[General Attributes - Devices] ウィンドウでは、次の作業が実行できます。

1. デバイスを削除する。

   デバイスのリストに設定対象でないデバイスがある場合、ステップ 4 の説明に従って削除できます。

2. 各デバイスに次のグループの属性を設定する。

   – [General Attributes] : 一般属性には、デバイスのホスト名、デバイス タイプ、管理 IP アドレスやその他の設定が含まれます。

[General Attributes - Devices] ウィンドウに表示されたデフォルトの属性を使用することも、必要に応じて変更することも可能です。

一般属性のリストについては、「一般デバイス属性の設定」（P.E-32）を参照してください。

- [Password Attributes]：パスワード 属性には、デバイスのユーザ名とパスワード、およびデバイスのイネーブル ユーザ名とイネーブル パスワードが含まれます。これらの属性の設定は*必須*です。
- [CNS Attributes]：デバイスが CNS デバイスの場合、CNS 属性を設定します。

ステップ 2　ウィンドウに表示されたデバイスのフィルタリングを行うには、表示させるデバイス名の一部をアスタリスク（*）を前か後に付けて入力し、[Find] ボタンをクリックします。

[Find] フィールドにアスタリスクが表示されている場合、すべてのデバイスが表示されます。

[Find] フィールドの設定は、すべての属性ウィンドウに適用されます。

ステップ 3　属性エリアの 1 つを表示するよう変更するには、ウィンドウ下部の [Attributes] ボタンをクリックし、プルダウン リストで表示する属性エリアを選択します。

- デバイスを設定するために使用するプロトコル（コンフィギュレーション アクセス プロトコル）といった、デバイスの一般属性を変更する必要がある場合、最初に表示されるウィンドウでこの操作を実行できます。

  [General Attributes - Devices] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [General Attributes] を選択します。

  一般属性の設定については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。

- パスワード属性を設定するには、[Attributes] ボタンをクリックし、プルダウン リストから [Password Attributes] を選択します。

  パスワード属性の設定については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。

（注）　この手順は必須です。コンフィギュレーション収集をイネーブルにするには、パスワード属性の設定が*必須*です。

- CNS 属性の変更が必要な場合、「Cisco CNS 属性の設定」（P.E-33）を参照してください。

ステップ 4　1 つ以上のデバイスを削除するには、次のステップを実行します。

a. 削除する各デバイスの横にあるチェックボックスをオンにします。

複数のデバイスを削除する必要がある場合、デバイスのリストの見出し横にあるチェックボックスをオンにします。リストのすべてのデバイスが選択されます。その後、削除しないデバイスのチェックを外します。

b. デバイスを削除するには、[Delete] ボタンをクリックします。

パスワード属性の設定（必須ステップ）

コンフィギュレーション収集フェーズを正しく完了させるには、各デバイスへのパスワード属性の設定が*必須*です。パスワード属性を設定するには、次のステップを実行します。

ステップ 1　[Password Attributes] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [Password Attributes] を選択します。

[Password Attributes] ウィンドウが表示されます。

ステップ 2　設定対象のデバイスとパスワード属性を選択するには、次のステップを実行します。

a. 設定対象のパスワード属性を持つデバイス横のチェックボックスをオンにします。

いくつかのデバイスが同じパスワード属性を持つ場合、複数のチェックボックスをオンにできます。すべてのデバイスが同じパスワード属性を持つ場合、見出し行の左にあるチェックボックスをオンにして、リスト内のすべてのデバイスを選択できます。このチェックボックスがオンになっている場合、オフにすることですべてのデバイスの選択を解除できます。

b. 設定するパスワード属性を選択するには、見出し行の属性名の横にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Edit] ボタンをクリックします。

ステップ 4　デバイスについて、次の情報を入力します。

- [Login Password] : デバイスのログイン パスワードを入力します。
- [Login User] : デバイスのユーザ名を入力します。
- [Enable User] : イネーブル権限を持つユーザ名を入力します。
- [Enable Password] : イネーブル ユーザのイネーブル パスワードを入力します。

ステップ 5　[Save] をクリックします。

入力した情報が [Password Attributes] ウィンドウに表示されます。

一般デバイス属性の設定

デバイス ディスカバリ プロセスが完了すると、[General Attributes - Devices] ウィンドウに各デバイスの現在の一般属性設定が表示されます。

デバイスの一般属性を変更するには、次のステップを実行します。

ステップ 1　変更する属性をクリックします。

選択した属性の [Edit Attributes] ダイアログボックスが開きます。

ステップ 2　ダイアログボックスに、属性の新しい設定を指定します。

一般デバイス属性には、次の内容が含まれます。

- [Host Name] : 先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Device Type] : デバイス タイプは [Cisco Router] です。
- [Device Description]（このウィンドウでは編集不可）: デバイスのタイプ、位置やその他サービス プロバイダーのオペレータに役立つ情報など、デバイスに関係する情報を何でも含められます。80 文字に制限されています。
- [Management Address] : Prime Provisioning がターゲット ルータ デバイスの設定に使用する、デバイスの有効な IP アドレス。この IP アドレスは、Prime Provisioning ホストから到達可能である必要があります。

- [Domain Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。名前は、ターゲット ルータ デバイスのドメイン名と一致させる必要があります。
- [Config Access Protocol]：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用のアクセス プロトコルを管理します。[Telnet]、[Terminal]、[TFTP]、[RCP] から選択できます。

Cisco CNS 属性の設定

デバイスの 1 つが Cisco CNS デバイスの場合、次のステップに従って CNS 属性を設定します。

ステップ 1　[CNS Attributes] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [CNS Attributes] を選択します。

[CNS Attributes] ウィンドウが表示されます。

[Terminal Server] 列はエッジ ルータのプロビジョニングに使用可能なワークステーションを表すデバイスを指定し、[Port Number] 列はターミナル サーバが使用するポート番号を指定します。

ステップ 2　既存の [Event Identification] 項目をクリックします。

イベント識別の [Edit Attributes] ダイアログボックスが開きます。

ステップ 3　[Event Identification] 属性のドロップダウン リストから、イベント識別を選択できます。これは [CNS Identification] フィールドの内容が HOST NAME か CNS ID かを示します。デフォルト：[HOST NAME]。

。

デバイス コンフィギュレーションの保存

デバイス コンフィギュレーションを変更した後、[Continue] ボタンをクリックします。

[Device Discovery] インジケータがグリーンに変わり、デバイス ディスカバリの完了（[Complete]）を示します。

ディスカバリ データ収集フェーズが自動的に始まります。

ステップ 3：ディスカバリ データ収集の実行

デバイス コンフィギュレーション設定を保存すると、デバイス ディスカバリのディスカバリ データ収集フェーズが自動的に始まります。

Cisco Prime Provisioning がデバイス コンフィギュレーションを収集している間、ディスカバリ データ収集インジケータはイエローになり、プロセスが進行中（[In Progress]）であることを示します。

ディスカバリ データ収集フェーズが完了すると、インジケータはグリーンに変わり、プロセスの完了（[Complete]）を示します。これでデバイス ロールの割り当ての準備ができました。

ステップ 4：ロール割り当ての実行

デバイス ディスカバリのディスカバリ データ収集フェーズ完了後、[Discovery Workflow] ウィンドウは、ロール割り当てフェーズが入力待ち（[Pending Input]）であることを示します。

ディスカバリ データ収集から再開すると、ディスカバリ データ収集対象デバイスを選択するよう求められます。

デバイス ロールを割り当てるには、次のステップを実行します。

- デバイス ロール割り当ての開始
- デバイス割り当て表示の変更
- デバイス割り当ての変更
- デバイス ロールの決定
- CE デバイス ロールの割り当て
- PE デバイス ロールの割り当て

ここでは、これらのステップについて説明します。

デバイス ロール割り当ての開始

次のステップを実行して、デバイス ロール割り当てを開始します。

ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[Role Assignment - Un-assigned Devices] ウィンドウが表示されます。

[Role Assignment - Un-assigned Devices] ウィンドウでは、単一のデバイスを選択した場合、直接デバイス ロールを割り当てるよう求められます。複数のデバイスを選択した場合は、[Role Assignment - CEs] ウィンドウと [Role Assignment - PEs] ウィンドウのいずれかが表示されます。これらのウィンドウで、必要なデバイス ロールを指定できます。

ステップ 2　デバイスの表示方法を変更するには、次の項「デバイス割り当て表示の変更」（P.E-34）を参照してください。

デバイス割り当て表示の変更

次の方法で、[Role Assignment] ウィンドウのデバイス表示方法を変更できます。

- [Role Assignment] ウィンドウ下部のプルダウン リストを使って、未割り当てデバイス、PE デバイス、CE デバイスの表示を切り替えられます。
- ウィンドウ上部にある [Show devices with] の選択と [matching] フィールドを使用して、表示されるデバイスの範囲を変更できます。

表示されるデバイスのカテゴリを変更するには、次のステップを実行します。

ステップ 1　表示されるデバイスのカテゴリを変更するには、[Role Assignment] ウィンドウ下部のプルダウン リストから値を選択します。

- PE デバイスを表示するには、[PEs] を選択します。

- CE デバイスを表示するには、[CEs] を選択します。
- 未割り当てデバイスを表示するには、[Un-assigned Devices] を選択します。

ステップ 2　表示されるデバイスの範囲を変更するには、ウィンドウ上部にある [Show devices with] の選択と [matching] フィールドを組み合わせて使用します。

- ホスト名順にデバイスをリストするには、[Device Host Name] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。
- ドメイン名順にデバイスをリストするには、[Device Domain Name] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。
- 管理 IP アドレス順にデバイスをリストするには、[Management IP Address] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。

[matching] フィールドの値は、表示されるデバイスを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのデバイスを指定します。アスタリスクが後に付いた文字列を指定すると、その文字列で始まるホスト名、ドメイン名、管理 IP アドレスを持つすべてのデバイスを表示します。アスタリスクが前に付いた文字列を指定すると、その文字列で終わるホスト名、ドメイン名、管理 IP アドレスを持つすべてのデバイスを表示します。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、ホスト名の一部に「ce」を含むデバイスすべてを表示するには、[matching] フィールドに「*ce*」と入力します。

表示内容は、選択によって変わります。たとえば、2 台のデバイスに CE ロールが割り当てられている場合は、[Role Assignment - CEs] ウィンドウが表示されます。

デバイス割り当ての変更

デバイス ディスカバリ プロセスで、誤ったデバイス ロールがデバイスのグループに割り当てられる場合があります。たとえば、PE となるはずのデバイスに CE が割り当てられることがあります。

この場合、次のステップを実行します。

- PE と表示されるはずのデバイスの一部が [Role Assignment - PEs] ウィンドウにリストされない場合、[Role Assignment - Unassigned Devices] ウィンドウと [Role Assignment - CEs] ウィンドウを確認し、デバイスを PE デバイスとして割り当てます。
  - [Role Assignment - CEs] ウィンドウに移動し、PE デバイスとなるはずのデバイスをすべて選択します。
  - [Assign as PEs] ボタンをクリックします。

    [Role Assignment - PEs] ウィンドウが表示され、PE として割り当てたデバイスがリストされるようになります。
- 希望どおりに割り当てられていない他のデバイスがあれば、必要に応じて基本デバイス割り当てを変更します。

個別および一括でのデバイス割り当て

ロール割り当て用のウィンドウでは、単一のデバイスにデバイス ロールを割り当てることも、一括割り当てを使用する（複数のデバイスを選択してすべてに同じロールを割り当てる）こともできます。

単一のデバイスにデバイス ロールを割り当てる場合、[Site] や [Region] といった他のデバイス属性も割り当てられます。ただし、一括でデバイス ロールを割り当てる場合は、同時に他の属性を割り当てられません。他の属性は、後から [PEs] または [CEs] ウィンドウに移動して割り当てることになります。

デバイス ロールの決定

デバイス割り当ての目的は、プロバイダーのネットワークで検出されたデバイスを、2 つの一般的なグループに区分することです。

- プロバイダー関連デバイス：プロバイダー エッジ（PE）デバイス

  PE ロールの割り当て（U-PE、N-PE、P、PE-AGG）については、「PE ロールの割り当て」（P.E-36）を参照してください。

- カスタマー関連デバイス：カスタマー エッジ（CE）デバイス

  CE ロールの割り当てについては、「CE ロールの割り当て」（P.E-39）を参照してください。

PE デバイスでは、次の注意事項に従ってデバイス ロールを決定します。

- コア ドメインの中央に位置するデバイスを P デバイスとして割り当てます。
- VPN サービスのユーザとインターフェイスが設定されているデバイスは、すべて U-PE デバイスとして割り当てます。これらのデバイスが、ドメインのカスタマー方向エッジにあるデバイスです。
- MPLS コア ドメインまたは L2VPN コア ドメインのエッジにあるデバイスすべてを、N-PE デバイスとして割り当てます。
- デバイス リング内のデバイス、または複数の U-PE デバイスに接続するデバイスを、PE-AGG デバイスとして割り当てます。

  CE デバイスでは、CE ロールの割り当てについての項にある CE ロールの説明（「CE ロールの割り当て」（P.E-39））の特定情報を参照してください。

PE ロールの割り当て

あるデバイスを PE デバイスとして割り当てるには、次のステップを実行します。

ステップ 1　[Role Assignment - Un-assigned Devices] ウィンドウで、PE として割り当てるデバイスを選択します。

- デバイスを選択するには、デバイス名の横のチェックボックスをオンにします。
- デバイスの選択を解除するには、デバイス名の横のチェックボックスをオフにします。

ステップ 2　[Assign as PE(s)] ボタンをクリックします。

ステップ 3　[Assign as PE] ウィンドウで、PE に必要な情報を割り当てます。

a. PE リージョン名を割り当てるには、[Select] ボタンをクリックします。

[PE Region Name] ウィンドウが表示されます。

b. [PE Region Name] ウィンドウで、割り当てるリージョン名の横のオプション ボタンをクリックし、[Select] をクリックします。

[PE Region] フィールドにリージョン名が表示された状態で [Assign as PE] ウィンドウが表示されます。

c. PE ロールを割り当てるには、プルダウン リストから [PE Role] フィールドの値を選択します。

PE ロールは、PE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて PE ロールを割り当てます。

次の PE ロールを選択できます。

- [N-PE]：ドメインのエッジにある（エッジ レイヤ内）デバイスを、ネットワーク側プロバイダー エッジ（N-PE）デバイスとして割り当てます。
- [U-PE]：ユーザ方向のプロバイダー エッジ内のデバイスを、U-PE デバイスとして割り当てます。
- [P]：コア ドメインの中央に位置するデバイスをプロバイダー コア（P）デバイスとして割り当てます。
- [PE-AGG]：集約レイヤ内のデバイスを Provider Edge Aggregation（PE-AGG）デバイスとして割り当てます。

d. [OK] をクリックします。

指定した値が表示された状態で [Role Assignment - PEs] ウィンドウが表示されます。

PE ロールの編集

1 つ以上のデバイスが PE デバイスとして割り当てられ、[Role Assignment - PEs] ウィンドウに表示された後、PE ロールを編集できます。[Assign as PE] ウィンドウで値が割り当てられなかった場合でも、PE ロールを編集できます。

（注） PE ロールの割り当ては必須ではありません。ただし、予期しない動作の防止のために推奨されています。

PE デバイスのロール割り当ての値を編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリのロール割り当てフェーズがアクティブな間に、[Role Assignment - PEs] ウィンドウを選択します。

[Role Assignment - Un-assigned Devices] または [Role Assignment - CEs] ウィンドウがアクティブの場合、ウィンドウ下部のプルダウンリストから [Role-Assignment - PEs] を選択します。

[Role Assignment - PEs] ウィンドウが表示されます（図 E-8 を参照）。

図 E-8　[Role Assignment - PEs] ウィンドウ

このウィンドウでは、次の列によるソートが無効なことに注意してください。

- PE Device Host Name
- PE Provider Name
- PE Region Name

図 E-8 のウィンドウ例では、PE の 1 つにロール情報が割り当てられています。他の 2 つの PE は、PE として割り当てられていますが、ロール情報は割り当てられていません。PE の情報はすべて、情報が入力されているかどうかにかかわらず編集可能です。

ステップ 2　編集する 1 つ以上の PE を選択します。

- 特定の PE を選択するには、デバイス名の横のチェックボックスをオンにします。
- ウィンドウ内のすべての PE を選択するには、見出し行のチェックボックスをオンにします。

ステップ 3　PE ロールを編集するには、次のステップを実行します。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [PE Role] を選択します。

PE ロールを選択するよう求められます。

b. プルダウン リストから [PE Role] フィールドの値を選択し、PE ロールを割り当てます。

次の PE ロールを選択できます。

- [N-PE]：エッジ レイヤ内のデバイスをネットワーク側プロバイダー エッジ（N-PE）デバイスとして割り当てます。
- [U-PE]：ユーザ方向のプロバイダー エッジ内のデバイスを、U-PE デバイスとして割り当てます。
- [P]：コア レイヤ内のデバイスをプロバイダー コア（P）デバイスとして割り当てます。
- [PE-AGG]：集約レイヤ内のデバイスを Provider Edge Aggregation（PE-AGG）デバイスとして割り当てます。

指定した PE ロールが [Role Assignment - PEs] ウィンドウに表示されます。

ステップ 4　PE プロバイダー名や PE リージョン名を編集するには、次のステップを実行します。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [Region/Provider] を選択します。

リージョン名を入力するよう求められます。

b. ポップアップ ウィンドウにリストされたリージョン名のいずれかを横のオプション ボタンをクリックして選択してから、[Select] ボタンをクリックします。

指定したリージョン名と、関連付けられたプロバイダー名が [Role Assignment - PEs] ウィンドウに表示されます。

CE ロールの割り当て

あるデバイスを CE デバイスとして割り当てるには、次のステップを実行します。

ステップ 1　[Role Assignment - Un-assigned Devices] ウィンドウで、CE として割り当てるデバイスを選択します。

- デバイスを選択するには、デバイス名の横のチェックボックスをオンにします。
- デバイスの選択を解除するには、デバイス名の横のチェックボックスをオフにします。

ステップ 2　[Assign as CE(s)] ボタンをクリックします。[Assign as CE] ウィンドウが表示されます。

ステップ 3　[Assign as CE] ウィンドウで、CE に必要な情報を割り当てます。

a. カスタマー名（必須フィールド）を割り当てるには、[Select] ボタンをクリックします。

[Customer Name] ウィンドウが表示されます。

b. カスタマー名を割り当てるには、割り当てるカスタマー名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したカスタマー名が表示された状態で [Assign as CE] ウィンドウが表示されます。

c. CE 管理タイプを割り当てるには、プルダウン リストから [CE Management Type] の値を選択します。

CE 管理タイプは、CE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて CE 管理タイプを割り当てます。

次の CE 管理タイプを選択できます。

- [MANAGED-REGULAR]：デフォルトの CE ロール割り当てです。プロバイダーに管理させる CE にこのロールを割り当てます。CE は Prime Provisioning サーバから到達可能である必要があります。このロールを割り当てると、インベントリ マネージャ インターフェイスでルータを作成するときに、ルータ コンフィギュレーションが自動的にダウンロードされます。
- [UNMANAGED]：手動で管理するデバイスにこのロールを割り当てます。このロールを割り当てると、新しいデバイスの作成時にデバイス コンフィギュレーションは自動で割り当てられず、デバイスを手動で設定する必要があります。プロバイダーは管理対象外 CE を直接プロビジョニングできません。[Unmanaged] を選択すると、プロバイダーは Prime Provisioning を使用してコンフィギュレーションを生成した後、コンフィギュレーションを CE に配置するようカスタマーに送ることができます。
- [MANAGED-MGMT-LAN]：デバイス管理が PE コンフィギュレーションにリンクすることを示します。新規デバイスが作成されると、コンフィギュレーションが自動的にダウンロードされます。管理対象の Management LAN や Management CE（MCE; 管理 CE）は管理対象の CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [UNMANAGED-MGMT-LAN]：デバイス管理が PE コンフィギュレーションに関連付けられているが、新規デバイス作成時にコンフィギュレーションが自動でダウンロードされないことを示します。管理対象外の Management LAN や MCE は管理対象外 CE ルータのように設定

されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。

- [DIRECT-CONNECTED-REGULAR]：ほとんどの場合、CE は PE ルータに接続されます。この場合、CE はワークステーションまたはその他のデバイスに接続されます。
- [DIRECT-CONNECTED-MGMT-HOST]：ほとんどの場合、CE は PE ルータに接続されます。このケースでは、CE は Prime Provisioning の存在するワークステーションや他のデバイスに接続されます。
- [MULTI-VRF]：PE と CE との間に VPN Routing/Forwarding（VRF; VPN ルーティング/転送）インスタンスであるデバイスが存在することを示します。Multi-VRF CE（MVRFCE; マルチ VRF CE）はカスタマーの所有ですが、プロバイダー空間に存在します。PE からのオフロード トラフィックに使用されます。
- [UNMANAGED-MULTI-VRF]：管理対象外のマルチ VRF CE は、管理対象外の CE のようにプロビジョニングされます（プロバイダーによってコンフィギュレーションのアップロードやデバイスへのアップロードが行われない）。これはカスタマーの所有であり、プロバイダー空間に存在します。

d. [OK] をクリックします。

指定した値が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

（注） この時点で、[CE Site] の値は未割り当てです。この値を割り当てるには、設定を編集する必要があります。このタスクについては、「CE ロールの編集」（P.E-40）を参照してください。

CE ロールの編集

1 つ以上のデバイスが CE デバイスとして割り当てられ、[Role Assignment - CEs] ウィンドウに表示された後、CE ロールを編集できます。[Assign as CE] ウィンドウで値が割り当てられなかった場合でも、CE ロールを編集できます。

CE デバイスのロール割り当ての値を編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリのロール割り当てフェーズがアクティブな間に、[Role Assignment - CEs] ウィンドウを選択します。

[Role Assignment - Un-assigned Devices] または [Role Assignment - PE] ウィンドウがアクティブの場合、ウィンドウ下部のプルダウンリストから [Role-Assignment - CEs] を選択します。

[Role Assignment - CEs] ウィンドウが表示されます。

図 E-9　[Role Assignment - CEs] ウィンドウ

図 E-9 に示した [Role Assignment - CEs] ウィンドウでは、CE のうち 2 つにはロール割り当て情報が割り当てられ、2 つには情報が割り当てられていません。CE の情報はすべて、情報が入力されているかどうかにかかわらず編集可能です。

このウィンドウでは、次の列によるソートが無効なことに注意してください。

- CE Device Host Name
- CE Site Name
- CE Customer Name

ステップ 2　編集する 1 つ以上の CE を選択します。

- 特定の CE を選択するには、デバイス名の横のチェックボックスをオンにします。
- ウィンドウ内のすべての CE を選択するには、見出し行のチェックボックスをオンにします。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [Customer] を選択します。

カスタマー名を選択するよう求められます。

b. カスタマー名を選択するには、表示されたいずれかのカスタマー名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したカスタマー名が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ステップ 4　CE 管理タイプを編集するステップは、次のとおりです。

a. 編集する 1 つ以上の CE を選択します。

b. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン ウィンドウから [CE Management Type] を選択します。

CE 管理タイプは、CE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて CE 管理タイプを割り当てます。

次の CE 管理タイプを選択できます。

- [MANAGED-REGULAR]：デフォルトの CE ロール割り当てです。プロバイダーに管理させる CE にこのロールを割り当てます。CE は Prime Provisioning サーバから到達可能である必要があります。このロールを割り当てると、インベントリ マネージャ インターフェイスでルータを作成するときに、ルータ コンフィギュレーションが自動的にダウンロードされます。
- [UNMANAGED]：手動で管理するデバイスにこのロールを割り当てます。このロールを割り当てると、新しいデバイスの作成時にデバイス コンフィギュレーションは自動で割り当てられず、デバイスを手動で設定する必要があります。プロバイダーは管理対象外 CE を直接プロビジョニングできません。[Unmanaged] を選択すると、プロバイダーは Prime Provisioning を使用してコンフィギュレーションを生成した後、コンフィギュレーションを CE に配置するようカスタマーに送ることができます。

- [MANAGED-MGMT-LAN] : デバイス管理が PE コンフィギュレーションにリンクすることを示します。新規デバイスが作成されると、コンフィギュレーションが自動的にダウンロードされます。管理対象の Management LAN や Management CE（MCE; 管理 CE）は管理対象の CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [UNMANAGED-MGMT-LAN] : デバイス管理が PE コンフィギュレーションに関連付けられているが、新規デバイス作成時にコンフィギュレーションが自動でダウンロードされないことを示します。管理対象外の Management LAN や MCE は管理対象外 CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [DIRECT-CONNECTED-REGULAR] : ほとんどの場合、CE は PE ルータに接続されます。この場合、CE はワークステーションまたはその他のデバイスに接続されます。
- [DIRECT-CONNECTED-MGMT-HOST] : ほとんどの場合、CE は PE ルータに接続されます。このケースでは、CE は Prime Provisioning の存在するワークステーションや他のデバイスに接続されます。
- [MULTI-VRF] : PE と CE との間に VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）インスタンスであるデバイスが存在することを示します。Multi-VRF CE（MVRFCE; マルチ VRF CE）はカスタマーの所有ですが、プロバイダー空間に存在します。PE からのオフロード トラフィックに使用されます。
- [UNMANAGED-MULTI-VRF] : 管理対象外のマルチ VRF CE は、管理対象外の CE のようにプロビジョニングされます（プロバイダーによってコンフィギュレーションのアップロードやデバイスへのアップロードが行われない）。これはカスタマーの所有であり、プロバイダー空間に存在します。

c. [Select] をクリックします。

指定した CE 管理タイプが表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ステップ 5　サイト名の指定や既存のサイト名の編集を行うには、次のステップを実行します。

a. 編集する 1 つ以上の CE を選択します。

b. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン ウィンドウから [Site] を選択します。

[Site Name] ウィンドウが表示されます。

c. [Site Name] ウィンドウで、割り当てるサイト名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したサイト名が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ロール割り当て情報の保存

デバイスへのロールの割り当てが終わったら、[Continue] ボタンをクリックします。

[Role Assignment Discovery] インジケータがグリーンに変わり、ロール割り当ての完了（[Complete]）を示します。

これでデバイス ディスカバリの NPC ディスカバリ フェーズ開始の準備ができました。

ステップ 5：NPC ディスカバリの実行

デバイス ディスカバリのロール ディスカバリ フェーズ完了後、[Discovery Workflow] ウィンドウは、NPC ディスカバリ フェーズが入力待ち（[Pending Input]）であることを示します。

検出された NPC のリストを参照したり、必要に応じて NPC を削除したりするには、次の一般的なステップを実行します。

- *イーサネット コアのメトロ イーサネット ネットワーク トポロジ*を検出する場合、「メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ」（P.E-43）に説明されているステップを実行します。
- 「NPC 割り当ての開始」（P.E-44）で説明されている NPC 割り当てのステップを完了させます。
- 必要であれば、「NPC へのデバイスの追加」（P.E-46）や次の項で説明されているように、NPC の追加や変更のためのステップを完了させておきます。

メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ

イーサネット コアのメトロ イーサネット トポロジを検出する場合、次のステップを実行します。

- 1 つ以上のアクセス ドメインを作成し、デバイス ディスカバリ フェーズで検出されたデバイスをアクセス ドメインに割り当てます。
- 最低 1 つのリソース プールを作成します。
- 各デバイスの「Inter-N-PE インターフェイス」を編集します。

これらのステップは、Service Inventory インターフェイスの Inventory and Connection Manager（[Service Inventory] > [Inventory and Connection Manager]）を使用して実行します。

アクセス ドメインの作成

アクセス ドメインを作成し、検出されたデバイスをドメインに追加するには、次のステップを実行します。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[Access Domains] を選択します。

[Access Domains] ウィンドウが表示されます。

ステップ 4　1 つ以上のアクセス ドメインを作成し、L2VPN メトロ イーサネット トポロジ内のデバイスを作成したアクセス ドメインに割り当てます。

アクセス ドメインの作成の詳細については、の第 2 章「Prime Provisioning を設定する前に」「アクセス ドメインの作成」（P.2-43）の項を参照してください。

リソース プールの作成

リソース プールを作成するには、次のステップを実行します。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 4　リソース プールを作成します。

ステップ 5　[Pool Type] で [VLAN] が選択されていることを確認します。

ステップ 6　[Start] の値として 2 を入力します。

ステップ 7　[Pool Size] の値には、リソース プール内のデバイス数に対応できる、十分に大きな値（500 など）を入力します。

リソース プールの作成の詳細については、第 2 章「Prime Provisioning を設定する前に」の「リソース プール」（P.2-46）の項を参照してください。

Inter-N-PE インターフェイスの編集

ご使用のメトロ イーサネット トポロジ内のデバイス用に「Inter N-PE」インターフェイスを編集するには、次のステップを実行します。

（注）　これらのステップが必要なのは、PE デバイスがリポジトリ内にすでに存在している場合だけです。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[PE Devices] を選択します。

[PE Devices] ウィンドウが表示されます。

ステップ 4　トポロジ内の各 PE デバイスを選択し、次の操作を実行します。

a.　[Edit] ボタンをクリックします。

[Edit PE] ウィンドウが表示されます。

b.　デバイスが接続されている各デバイスへのインターフェイスを見つけます。

c.　各インターフェイスについて、[Metro Ethernet] 列の [Any] を [None] に変更します。

d.　変更を保存します。

次の項「NPC 割り当ての開始」（P.E-44）へ進み、NPC 割り当ての開始のステップを実行します。

NPC 割り当ての開始

次のステップを実行して、NPC 割り当てを開始します。

ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[Named Physical Circuits] ウィンドウが表示されます。

[Named Physical Circuits] ウィンドウは、初期状態では検出された回線すべてを表示しています。

この時点で、必要に応じて NPC を作成、追加、または削除できます。

[State] 列には次のカテゴリがあります。

- [New] : Prime Provisioning に対応する NPC が存在しない。新しい NPC だけが Prime Provisioning にコミットされます。
- [Existing] : 検出された NPC は Prime Provisioning の NPC と同一です。
- [Existing Modified] : Prime Provisioning の NPC とは送信元とエンドポイントは同じですが、1 つ以上の中間リンクが異なります。
- [Conflicting] : 検出された NPC と Prime Provisioning の NPC とが競合しています。

Named Physical Circuit（NPC; 名前付き物理回線）は、CPE または U-PE と N-PE との間の物理的な接続を表す名前付き回線です。NPC の中間ノードは U-PE と PE-AGG のいずれかです。これらは、環状に接続でき、デバイスの環を形成します。これは、NPC リングと呼ばれるエンティティによって表されます。NPC リングはデバイスと名前付き物理回線とのリング型トポロジを表します。NPC を作成するには、送信元 CPE/U-PE と宛先 N-PE とがどのように接続されているかを指定し、中間ノードを指定する必要があります。

ステップ 2　NPC を定義する必要がある場合、次のステップを実行します。

a.　[Named Physical Circuits] ウィンドウで、[Create] をクリックします。

[Create a Physical Circuit] ウィンドウが表示されます。

初期状態では、NPC リストは空です。

b.　[Add Device] ボタンをクリックします。

[Select a Device] ウィンドウが表示されます。

ステップ 3　このウィンドウで、デバイスのオプション ボタンをクリックしてから [Select] ボタンをクリックします。

初期デバイスが追加された状態で [Create a Named Physical Circuit] ウィンドウが開きます。

ウィンドウのボタンがアクティブに変わります。

c.　画面上のデバイスをクリックし、次のいずれかの処理を選択します。

- デバイスを挿入するには、[Insert Device] ボタンをクリックします。
- リングを挿入するには、[Insert Ring] ボタンをクリックします。
- デバイスを追加するには、[Add Device] ボタンをクリックします。
- リングを追加するには、[Add Ring] ボタンをクリックします。
- 既存のデバイスやリングを削除するには、デバイスを選択して [Delete] ボタンをクリックします。

ステップ 4　詳細は、次の項を参照してください。

NPC へのデバイスの追加

ステップ 1　[Create a Named Physical Circuit] ウィンドウで着信インターフェイスを選択するには、[Select Incoming Interface] をクリックします。

[Select Device Interface] ウィンドウが表示されます。このウィンドウには、選択されたデバイス上のインターフェイスが表示されています。

ステップ 2　リストでインターフェイス横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

選択されたインターフェイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 3　発信インターフェイスを選択するには、[Select Outgoing Interface] をクリックします。

デバイス上に設定されているインターフェイスのリストが表示されます。

ステップ 4　リストでインターフェイス横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

発信インターフェイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 5　必要に応じて追加デバイスを選択し、着信インターフェイスまたは発信インターフェイスあるいはその両方を指定します。

ステップ 6　完了後、[Create a Named Physical Circuit] ウィンドウの [Save] ボタンをクリックします。

リングの追加

現在選択されているデバイスの前にリングを追加するには、次のステップを実行します。

（注）　リングの増分サービス ディスカバリはサポートされていません。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Add Ring] をクリックします。

[Select NPC Rings] ウィンドウが表示されます。ネットワーク トポロジ内に存在するリングは、すべてこのウィンドウに表示されます。

ステップ 2　ウィンドウにリストされたリング横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

選択されたリングが [Create a Named Physical Circuit] ウィンドウに表示されます。

デバイスの挿入

トポロジ内の最後のデバイスの後にデバイスを挿入するには、次のステップを実行します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Insert Device] ボタンをクリックします。

[Select a Device] ウィンドウが表示されます。

ステップ 2　挿入するデバイスの横にあるチェックボックスをオンにし、[Select] ボタンをクリックします。

デバイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 3　[select incoming interface] をクリックします。

選択されたデバイス上のインターフェイスのリストが表示されます。

ステップ 4　選択するインターフェイス横のチェックボックスをオンにし、[Select] をクリックします。

選択されたインターフェイスがインターフェイスのリストに表示されます。

リングの挿入

トポロジ内の最後のデバイスの後にリングを挿入するには、次のステップを実行します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Insert Ring] ボタンをクリックします。

現在すでに存在するリングのリストが表示されます。

ステップ 2　リングのリストで、挿入するリング横のチェックボックスをオンにし、[Select] をクリックします。

選択したリングが [Create a Named Physical Circuit] ウィンドウに表示されます。

デバイスやリングの削除

デバイスやリングを削除するには、[Create a Named Physical Circuit] ウィンドウでデバイスまたはリングを選択し、[Delete] ボタンをクリックします。

デバイスが削除された状態で [Create NPC] ウィンドウが表示されます。

NPC コンフィギュレーションの保存

選択した 2 つのデバイス間の接続を設定した後、次のステップに従って NPC コンフィギュレーションを保存します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Save] をクリックします。

NPC プロセスが NPC コンフィギュレーションを検証します。

ステップ 2　[Continue] をクリックして続行します。

NPC ディスカバリが完了になった状態でワークフロー ウィンドウが表示されます。

ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）

デバイス ディスカバリの NPC ディスカバリ フェーズの完了後、ディスカバリ プロセス開始時に [MPLS VPN Discovery] を選択していた場合、NPC ディスカバリ フェーズは完了と表示され、MPLS VPN ディスカバリ ステップが入力待ち（[Pending Input]）と表示されます。

MPLS VPN ディスカバリ ユーザ インターフェイスを使用して、検出された MPLS VPN のコンフィギュレーションを開始する準備ができました。MPLS VPN サービスを設定するには、次のステップを実行します。

（注）　MPLS のサービス ディスカバリは、IOS XR が稼働中のデバイスをサポートしていません。

ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[MPLS VPNs] ウィンドウが表示され、検出された MPLS VPN がリストされます。検出された MPLS VPN のステータスは、次のように表示されます。

- 検出された MPLS の MPLS VPN トポロジが有効で、Prime Provisioning リポジトリに保存できる状態の場合、[VPN Status] は [Valid] VPN として表示され、ステータス インジケータはグリーンになります。
- 検出された MPLS の MPLS VPN トポロジが無効（トポロジがパーシャル メッシュ）の場合、カスタマー割り当てが行われていない場合、および無効なルート ターゲットが含まれている場合、[VPN Status] は [Invalid] VPN として表示され、ステータス インジケータはイエローになります。パーシャル メッシュ トポロジ VPN は Prime Provisioning ではサポートされていないため、フル メッシュまたはハブ アンド スポークあるいはその両方のコンポーネントに分割する必要があります。

図 E-10 に示す [MPLS VPN] ウィンドウには、無効な MPLS VPN が表示されています（トポロジがパーシャル メッシュで、カスタマー名が空白）。

図 E-10　無効な MPLS VPN が存在する [MPLS VPNs] ウィンドウ

（注）　MPLS VPN ディスカバリ プロセスでパーシャル メッシュ トポロジの MPLS VPN が検出された場合、VPN をサポートされているトポロジ（ハブ アンド スポークやフル メッシュ）の複数の個別 VPN に分割する必要があります。

ステップ 2　次のいずれかを実行します。

- [MPLS VPNs] ウィンドウの表示を変更する場合、別の表示オプションを選択します。

  MPLS VPN の表示オプションについては、「MPLS VPN 表示のフィルタリング」（P.E-49）を参照してください。
- MPLS VPN が有効であり、現時点で MPLS VPN トポロジに変更を加える必要がない場合、[Continue] をクリックして、検出されたトポロジに基づいた MPLS VPN サービスを作成します。
- 検出された MPLS VPN に 1 つ以上無効なものがある場合、次のステップを完了させる必要があります。
  - **VPN の分割**：無効な VPN を選択し、[Split VPN] ボタンをクリックします。

手順については、「VPN の分割」（P.E-49）を参照してください。

– **新規 VPN を作成しルート ターゲットを追加**：分割した VPN 内のデバイスを含む新規 VPN を作成し、それぞれの新規 VPN にルート ターゲットを追加する必要があります。

手順については、「VPN の作成」（P.E-51）を参照してください。

MPLS VPN 表示のフィルタリング

[MPLS VPNs] ウィンドウの表示方法を変更するには、次のステップを実行します。

ステップ 1　[Show VPNs with] フィールド横のメニューをプルダウンします。

VPN のリストを [VPN Name]、[Customer Name]、[Topology]、[VPN Type]、[Description] でフィルタリングできます。

ステップ 2　選択したカテゴリ内に表示される VPN を制限するには、[Matching] フィールドに値を入力します。

[matching] フィールドの値は、表示されるサイトを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのサイトを指定します。アスタリスクが後に付いた文字列を指定すると、[Show VPNs with] フィールドで指定された要素で始まるサイトすべてが表示されます。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、カスタマー名の一部に「cisco」が含まれる VPN をすべて表示するには、[matching] フィールドに「*cisco*」と入力します。

選択された条件に合致する VPN が表示されるようになります。

VPN の分割

場合によっては、MPLS VPN ディスカバリ プロセスを完了させて MPLS VPN サービスを実際に作成する前に、既存の MPLS VPN の分割が必要になる場合があります。

たとえば、次のように入力します。

- MPLS サービス ディスカバリ プロセスで無効な MPLS VPN（パーシャル メッシュ トポロジの MPLS VPN）が検出された場合、VPN をサポートされているトポロジ（ハブ アンド スポークやフル メッシュ）の複数のルート ターゲットに分割する必要があります。
- 処理の必要に応じて、MPLS VPN を分割してトポロジを変更することも選択できます。一度に分割できる VPN は 1 つだけです。

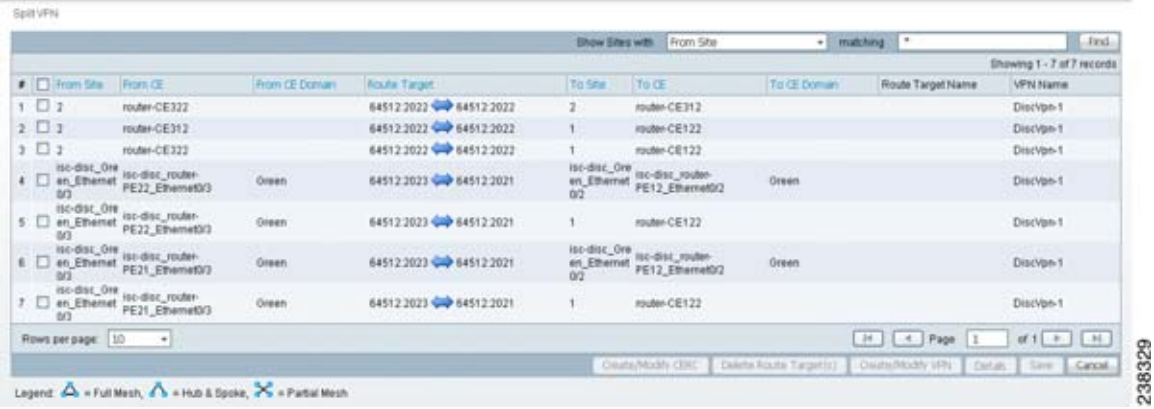
VPN を分割するステップは、次のとおりです。

ステップ 1　[MPLS VPNs] ウィンドウで、分割する VPN の横のチェックボックスをオンにします。

ステップ 2　[Split VPN] ボタンをクリックします。

[Split VPN] ウィンドウが表示されます（図 E-11 を参照）。

図 E-11　[Split VPN] ウィンドウ



ステップ 3　[Split VPN] ウィンドウで、リンクをいくつか選択します。

ハブ アンド スポークまたはフル メッシュ トポロジを構成するリンクを選択します。

たとえば、図 E-11 に示した [Split VPN] ウィンドウでは、最初の 3 つのリンクはすべて **1:102** のルート ターゲットを持ち、フル メッシュ トポロジを形成しています。

残り 2 つのリンクは、**1:106** および **1:105** というルート ターゲットを持っています。これらのリンクは、共同でハブ アンド スポーク トポロジを形成しています。

この VPN を分割するためには、最初の 3 つのリンクが 1 つのルート ターゲットに、残り 2 つのリンクが別のルート ターゲットに関連付けられる必要があります。その後、VPN ごとに 1 つのルート ターゲットの場合の Prime Provisioning ベスト プラクティス表記法に従って、VPN を 2 つの別々の VPN に分割できます。

ステップ 4　[Create/Modify CERC] ボタンをクリックします。

ルート ターゲット名を入力するよう求められます。

ステップ 5　新しいルート ターゲット名を入力して [Save] ボタンをクリックします。

ステップ 6　無効な VPN に含まれる残りのデバイスについても、これらのステップを繰り返します。

たとえば、図 E-11 に示すトポロジでは、ルート ターゲット **1:106** ～ **1:105** を持つデバイスを選択します。

ステップ 7　[Create/Modify CERC] ボタンをクリックします。

ステップ 8　ルート ターゲット名を入力するよう求められたら、新しいルート ターゲット名を入力し、[Save] ボタンをクリックします。

[Split VPNs] ウィンドウが再度表示され、ウィンドウには作成された新しいルート ターゲットが表示されています。

この例では、2 つの新しいルート ターゲットが作成され（**valid_cerc_one** と **valid_cerc_two**）、有効なトポロジであることに注意してください。最初のルート ターゲット **valid_cerc_one** はフル メッシュ トポロジ、2 番めのルート ターゲット **valid_cerc_two** はハブ アンド スポーク トポロジです。

ステップ 9　[Save] ボタンをクリックします。

次のステップに進んで、VPN を作成し VPN にルート ターゲットを追加する準備ができました。

VPN の作成

ルート ターゲットを作成した後、VPN を作成してルート ターゲットを追加する必要があります。

VPN を作成するステップは、次のとおりです。

ステップ 1　[Split VPN] ウィンドウで、[Create/Modify VPN] を選択します。

[Create New VPN] ウィンドウが表示されます。

ステップ 2　VPN に割り当てるルート ターゲットを選択します。

ステップ 3　[VPN Name] フィールドに VPN の名前を入力します。

この例では、**vpn_one** と入力します。

ステップ 4　[Assign VPN Name] ボタンをクリックします。

ステップ 5　[Save] をクリックします。

VPN が作成され、[Split VPN] ウィンドウの [VPN Name] フィールドに表示されます。

ステップ 6　必要に応じて、さらに VPN を作成します。

「VPN の分割」（P.E-49）のサンプル ウィンドウに示すルート ターゲットへと進むには、VPN が作成され、ルート ターゲットが割り当てられている必要があります。次の手順を実行します。

a.　[Split VPN] ウィンドウで、[Create/Modify VPN] をクリックします。

b.　[Create VPN] ウィンドウで、別の VPN を作成し、ルート ターゲットを割り当てます。

例の画面では、2 番めのルート ターゲット（**valid_cerc_two**）を新規作成された VPN に選択します。

ステップ 7　VPN の作成が完了したら、[Split VPN] ウィンドウの [Save] ボタンをクリックします。

[MPLS VPNs] ウィンドウが表示されます。

（注）　例では、VPN のうち 1 つが [Valid] と表示され、ステータス インジケータがグリーンになっています。しかし、ウィンドウ内のその他の VPN は [Invalid] と表示され、インジケータはイエローです。

このような状況が発生する場合があるのは、MPLS ディスカバリ プロセスがデータを完全には検証できないからです。このような状況でも、サービス ディスカバリ プロセスを継続し、MPLS VPN サービスを作成できます。ただし、プロセスでは無効な VPN がスキップされるため、Prime Provisioning プロビジョニング コマンドを使用して VPN サービスを手動設定する必要があります。

ステップ 8　カスタマーを各 VPN に割り当てるには、次のステップを実行します。

a.　[MPLS VPNs] ウィンドウの VPN エントリを選択し、[Edit] ボタンをクリックします。

[Edit VPN] ウィンドウが表示されます。

b.　[Customer Name] フィールドの横にある [Select] ボタンをクリックします。

カスタマー名のリストが表示されます。

c.　カスタマー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

d.　ルート ターゲットの名前を変更するには、[Rename] をクリックして変更します。

e.　[Save] をクリックします。

[MPLS VPNs] ウィンドウにカスタマー名が表示されます。

（注）　場合によっては、有効に思える VPN が無効と表示されることがあります。そのような VPN の処理はスキップされます。この場合、Prime Provisioning プロビジョニング コマンドを使用して手動で設定する必要があります。

ステップ 9　VPN の編集完了後、[Continue] ボタンをクリックして MPLS VPN サービス作成プロセスを開始します。

VPN リンクの詳細の表示

検出された VPN の詳細を表示するには、次のステップを実行します。

ステップ 1　[MPLS VPNs] ウィンドウから詳細事項を表示させる VPN を選択し、[Details] ボタンをクリックします。

[MPLS VPN Links] ウィンドウが表示されます。

ステップ 2　表示される MPLS VPN リンクをフィルタリングするには、[Show Sites with] フィールドのプルダウンリストから値を選択します。

VPN のリストを [From Site]、[From CE]、[From CE Domain]、[Route Target]、[To Site]、[To CE]、[To CE Domain] でフィルタリングできます。

[matching] フィールドの値は、表示されるサイトを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのサイトを指定します。アスタリスクが後に付いた文字列を指定すると、[Show Sites with] フィールドで指定された要素で始まるサイトすべてが表示されます。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、[From CE] 名に「realtime」が含まれるサイトすべてを表示するには、[Show Sites with] フィールドで [From CE Name] を選択してから、[matching] フィールドに「*realtime*」と入力します。

指定したリンクだけが表示された状態に変わります。

MPLS VPN の保存と MPLS VPN サービスの作成開始

検出された MPLS VPN の [MPLS VPNs] ウィンドウでのデータ編集が完了した後、[Continue] ボタンをクリックします。

ディスカバリ プロセスが VPN サービスを作成します。プロセスが完了すると、[Discovery Workflow] ウィンドウには MPLS VPN ディスカバリ プロセスが完了（[COMPLETE]）したことが表示され、ステータス インジケータはグリーンになります。

ディスカバリ プロセス開始前に [Discovery] ウィンドウで [L2VPN (Metro Ethernet) Discovery] も選択していた場合、キャリア イーサネット サービス ディスカバリに進めるようになります。

ステップ 7：L2VPN（メトロ イーサネット）サービス ディスカバリの実行（任意）

ディスカバリ プロセス開始前に [Discovery] ウィンドウで [L2VPN (Metro Ethernet) Discovery] を選択していた場合、前のステップが完了すると、[Discovery Workflow] ウィンドウに [L2VPN (Metro Ethernet) Discovery] が [Pending Input] と表示されます。

メトロ イーサネット サービス ディスカバリを開始するには、次のステップを実行します。

（注） L2VPN サービス ディスカバリは、IOS XR 稼働中のデバイスをサポートしておらず、EVC CLI フレームワークを使用して定義されたサービスを検出しません。

ステップ 1　メトロ イーサネット サービス ディスカバリを開始する前に、次のステップを実行します。

a. [Service Inventory] > [Inventory and Connection Manager] と選択します。

b. [Inventory and Connection Manager] ウィンドウ左にあるタスク ペインで、[Access Domains] を選択します。

c. メトロ イーサネット トポロジ内の N-PE デバイスのいずれかに、アクセス ドメインを作成します。

詳細については、第 2 章「Prime Provisioning を設定する前に」「アクセス ドメインの作成」（P.2-43）の項を参照してください。

d. [Service Inventory] > [Inventory and Connection Manager] と選択します。

e. [Inventory and Connection Manager] ウィンドウ左にあるタスク ペインで、[Resource Pools] を選択します。

f. 作成したアクセス ドメインのそれぞれにリソース プールを作成します。

詳細については、第 2 章「Prime Provisioning を設定する前に」「リソース プール」（P.2-46）の項を参照してください。

g. [Service Inventory] > [Discovery] と選択します。

[Discovery Workflow] ウィンドウに、[L2VPN (Metro Ethernet) Discovery] プロセスが [Pending Input] と表示されます。

ステップ 2　[Continue] をクリックします。

[L2VPN Discovery (Ethernet Services)] ウィンドウが表示されます。

ステップ 3　次のいずれかのアクションを選択します。

- [View/Edit Discovered Layer 2 Services grouped by VPN]：検出された L2VPN サービスを表示し、必要に応じて編集できます。
- [View/Edit Discovered Layer 2 End to End Wires]：検出されたレイヤ 2 エンドツーエンド回線を表示し、必要に応じて編集できます。
- [View/Edit Discovered Layer 2 VPLS Links]：検出されたレイヤ 2 Virtual Private LAN Service（VPLS; 仮想プライベート LAN サービス）リンクを表示し、必要に応じて編集できます。

この章の次の項で、各アクションについて説明します。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの表示

検出されたレイヤ 2 サービスを VPN によってグループ化して表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[VPNs] ボタンをクリックします。

[L2VPNs] ウィンドウが表示されます。

[L2VPNs] ウィンドウでは、次のタスクが実行できます。

- レイヤ 2 VPN についての詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。

- 既存の Layer 2 VPN の設定情報編集ウィンドウを表示する。

  詳細な手順については、「VPN によるグループ化表示された検出済みレイヤ 2 サービスの編集」（P.E-54）を参照してください。

- 既存のレイヤ 2 VPN を削除する。

  このタスクについては、「VPN によるグループ化表示された検出済みレイヤ 2 サービスの削除」（P.E-55）を参照してください。

ステップ 2　レイヤ 2 サービスについての詳細情報を参照するには、詳細を表示させる VPN の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

[L2VPN Details] ウィンドウが表示されます。

[L2VPN Details] ウィンドウには、User-Network Interface（UNI; ユーザネットワーク インターフェイス）など、検出された VPN の詳細が表形式で表示されます。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの編集

検出されたレイヤ 2 VPN サービスを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPN サービスを編集するには、次のステップを実行します。

ステップ 1　[L2VPNs] ウィンドウで、編集する VPN の横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit VPN] ウィンドウが表示されます。

ステップ 2　VPN 名を編集するには、新しい VPN 名を [VPN Name] フィールドに入力します。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a.　カスタマー名の横にある [Select] ボタンをクリックします。

カスタマーのリストが表示されます。

b.　設定する新しいカスタマー名の横にあるオプション ボタンをクリックします。

c.　[Save] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウに、新しい VPN 名またはカスタマー名あるいはその両方が表示されます。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの削除

レイヤ 2 サービスを削除するには、次のステップを実行します。

ステップ 1　[L2VPNs] ウィンドウで、削除する VPN の横にあるチェックボックスをオンにし、[Delete] ボタンをクリックします。

次のメッセージが表示されます。

```
Links/End to End wires associated with all selected VPNs will be deleted as a result of
this operation. Do you really want to Delete?
```

ステップ 2　VPN を削除してよいことを確認し、[OK] をクリックします。削除しない場合、[Cancel] をクリックします。

[OK] をクリックした場合、VPN および関連付けられたリンクとエンドツーエンド回線が削除されます。

検出済みレイヤ 2 VPN サービスを使用するポリシーの編集

検出されたレイヤ 2 VPN サービスを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPN サービスを編集するには、次のステップを実行します。

ステップ 1　[L2VPNs Details] ウィンドウで、VPN に関連付けられた UNI の横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit Link Policy] ウィンドウが表示されます。

ステップ 2　サービスのリンク ポリシーを変更するには、次のステップを実行します。

a.　[Policy Name] フィールドの横にある [Policy] ボタンをクリックします。

ポリシーのリストが表示されます。

[Show VPN policies with] フィールドのプルダウン リストからフィルタを選択したり、[Matching] フィールドにサーチ マスクを入力したりして、ポリシー リストを変更できます。

ポリシー リストを [Policy Name]、[Customer Name]、[Provider Name]、[Global policy name] でフィルタリングできます。[Matching] フィールドに値を入力して、選択したカテゴリのうち表示されるポリシーのリストを制限することも可能です。

ステップ 3　サービスを適用するポリシーの横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　次のいずれかを実行します。

- [Save] をクリックして変更を保存します。
- [Cancel] をクリックすると、変更がキャンセルされます。

検出されたレイヤ 2 エンドツーエンド回線の表示

検出されたレイヤ 2 エンドツーエンド回線を表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[End-End Wires] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウが表示されます。

[Metro Ethernet End to End Wires] ウィンドウでは、次のタスクを実行できます。

- メトロ イーサネット エンドツーエンド回線の詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。

- エンドツーエンド回線に関連付けられた VPN を編集する。

  このタスクについては、「エンドツーエンド回線に関連付けられた VPN の編集」（P.E-56）を参照してください。

- 既存のエンドツーエンド回線を 2 本のエンドツーエンド回線に分割する。

  このタスクについては、「レイヤ 2 サービス エンドツーエンド回線の分割」（P.E-57）を参照してください。

- 複数の既存エンドツーエンド回線を 1 本のエンドツーエンド回線に統合する。

  このタスクについては、「レイヤ 2 サービス エンドツーエンド回線の統合」（P.E-57）を参照してください。

- 既存のエンドツーエンド回線を削除する。

  このタスクについては、「検出されたレイヤ 2 エンドツーエンド回線の表示」（P.E-55）を参照してください。

ステップ 2　レイヤ 2 サービスについての詳細情報を参照するには、詳細を表示させる UNI の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

ステップ 4　エンドツーエンド回線内のインターフェイスの詳細を表示する場合、[AC1 UNI] または [AC2 UNI] フィールドのいずれかのインターフェイス名をクリックします。

インターフェイス名をクリックすると、[Interface Detail] ウィンドウが表示されます。[Interface Detail] ウィンドウは、選択されたインターフェイスについて、インターフェイスが位置するホストのホスト名やインターフェイスで使用されるカプセル化のタイプ、インターフェイスで使用されるスイッチ モードといった詳細情報を表示します。

ステップ 5　インターフェイスの詳細の参照後、[Close] ボタンをクリックします。

エンドツーエンド回線に関連付けられた VPN の編集

[Metro Ethernet End to End Wires] ウィンドウから、エンドツーエンド回線に関連付けられた VPN を編集することも可能です。

エンドツーエンド回線に関連付けられた VPN を編集するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、[VPN name] フィールドに表示された VPN 名をクリックします。

[Edit VPN] ウィンドウが表示されます。

ステップ 2　VPN 名を編集するには、新しい VPN 名を [VPN Name] フィールドに入力します。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a.　カスタマー名の横にある [Select] ボタンをクリックします。

カスタマーのリストが表示されます。

b. 設定する新しいカスタマー名の横にあるオプション ボタンをクリックします。

c. [Save] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウに、新しい VPN 名またはカスタマー名あるいはその両方が表示されます。

レイヤ 2 サービス エンドツーエンド回線の分割

既存のエンドツーエンド回線を、関連付けられた VPN から切り離し、新しい VPN に関連付けることが可能です。

エンドツーエンド回線を既存の VPN から分離するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、VPN から分離させるエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

（注）　エンドツーエンド回線に関連付けられた VPN の ID が 1 つだけである場合、回線上で分離アクションを実行できません。

ステップ 2　[Split] ボタンをクリックします。

続行確認メッセージが表示されます。

ステップ 3　プロセスを続行する場合、[OK] をクリックします。

エンドツーエンド回線は分割され、2 つの新しい VPN と関連付けられます。これらの VPN の名前は、既存の VPN 名の後ろに新しい番号を付加する方法で作成されます。

レイヤ 2 サービス エンドツーエンド回線の統合

2 本の既存エンドツーエンド回線を単一の VPN に統合できます。

2 本の既存エンドツーエンド回線を統合するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、統合する複数のエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

続行確認メッセージが表示されます。

ステップ 2　プロセスを続行する場合、[OK] をクリックします。

選択されたエンドツーエンド回線が新しい VPN に統合されます。この VPN の名前は、最も大きな番号が付いた既存の VPN 名に新しい番号を付加する方法で作成されます。

レイヤ 2 サービス エンドツーエンド回線の削除

既存のエンドツーエンド回線を削除するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、削除する 1 本以上のエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

続行確認メッセージが表示されます。

ステップ 2　プロセスを続行する場合、[OK] をクリックします。

選択したエンドツーエンド回線が削除されます。回線に関連付けられた接続回線もすべて削除されます。

ステップ 3　[Close] をクリックして [Metro Ethernet End to End Wires] ウィンドウを閉じます。

検出されたレイヤ 2 VPLS リンクの表示

検出されたレイヤ 2 VPLS リンクを表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[VPLS Links] ボタンをクリックします。

[VPLS Links] ウィンドウが表示されます。

[VPLS Links] ウィンドウでは、次のタスクが実行できます。

- VPLS リンクの詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。
- 既存の VPLS リンクの設定情報編集ウィンドウを表示する。

  詳細な手順については、「検出されたレイヤ 2 VPLS リンクの編集」（P.E-58）を参照してください。
- 既存のレイヤ 2 VPN を削除する。

  このタスクについては、「検出されたレイヤ 2 VPLS リンクの削除」（P.E-59）を参照してください。

ステップ 2　VPLS リンクについての詳細情報を参照するには、詳細を表示させる VPLS link の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

[VPLS Link Detail] ウィンドウが表示されます。

[VPLS Link Detail] ウィンドウには、検出された VPN とそのリンク プロパティが表示されます。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

検出されたレイヤ 2 VPLS リンクの編集

検出されたレイヤ 2 VPLS リンクを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPLS リンクを編集するには、次のステップを実行します。

ステップ 1　[VPLS Links] ウィンドウで、編集する VPLS リンクの横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit Link Policy] ウィンドウが表示されます。

ステップ 2　リンクのリンク ポリシーを変更するには、次のステップを実行します。

a. [Policy Name] フィールドの横にある [Policy] ボタンをクリックします。

ポリシーのリストが表示されます。

[Show VPN policies with] フィールドのプルダウン リストからフィルタを選択したり、[Matching] フィールドにサーチ マスクを入力したりして、ポリシー リストを変更できます。

ポリシー リストを [Policy Name]、[Customer Name]、[Provider Name]、[Global policy name] でフィルタリングできます。[Matching] フィールドに値を入力して、選択したカテゴリのうち表示されるポリシーのリストを制限することも可能です。

ステップ 3　サービスを適用するポリシーの横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　次のいずれかを実行します。

- [Save] をクリックして変更を保存します。
- [Cancel] をクリックすると、変更がキャンセルされます。

検出されたレイヤ 2 VPLS リンクの削除

VPLS リンクを削除するステップは、次のとおりです。

ステップ 1　[VPLS Links] ウィンドウで、削除する VPLS リンクの横にあるチェックボックスをオンにし、[Delete] ボタンをクリックします。

次のメッセージが表示されます。

```
The selected link(s) will be deleted. Do you really want to Delete?
```

ステップ 2　VPLS を削除してよいことを確認し、[OK] をクリックします。削除しない場合、[Cancel] をクリックします。

[OK] をクリックすると、VPLS リンクが削除されます。

ステップ 3　[Close] をクリックして、[VPLS links] ウィンドウを閉じます。

L2VPN メトロ イーサネット ポリシーの保存とサービスの作成開始

検出された L2VPN メトロ イーサネット トポロジの参照や編集が終了した後、[Close] ボタンをクリックして [L2VPN Discovery (Ethernet Services)] ウィンドウに戻ります。

[Continue] ボタンをクリックして、L2VPN サービス ディスカバリ プロセスを開始します。

[Discovery Workflow] ウィンドウが表示され、L2VPN サービス ディスカバリ プロセスが進行中（[In Progress]）であることを示します。ステータス インジケータはイエローです。

L2VPN サービス ディスカバリ プロセスが完了すると、ステータス インジケータはグリーンに変わり、[Discovery Workflow] ウィンドウは L2VPN サービス ディスカバリ プロセスが完了した（[Complete]）ことを示します。

ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット

[Continue] ボタンをクリックして、検出されたデバイスとサービスを Prime Provisioning リポジトリにコミットします。このステップの前に、検出ワークフローは検出されたデバイスとサービスを、検出ワークフローの最後のステップでだけ Prime Provisioning にコミットされる一時リポジトリに格納します。

ステップ 9：検出されたデバイスへのコンフィギュレーション収集タスクの作成と実行

サービスの表示と編集の前に、次のステップに従ってデバイスのコンフィギュレーション作成タスクを実行します。

（注）　コンフィギュレーション作成タスクについて詳しくは、「タスク」（P.10-25）の第 10 章「モニタリング」の項を参照してください。

ステップ 1　[Prime Provisioning Start] ページで、[Monitoring] を選択します。

[Monitoring] ウィンドウが表示されます。

ステップ 2　[Task Manager] を選択します。

[Tasks] ウィンドウが表示されます。

ステップ 3　[Create] ボタンをクリックし、プルダウン リストから [Collect Config] を選択します。

[Create Task] ウィンドウが表示されます。

ステップ 4　[Next] ボタンをクリックします。

[Collect Config Task] ウィンドウが表示されます。

ステップ 5　[Collect Config Task] ウィンドウで、次のステップに従ってコンフィギュレーション収集タスクを作成し、実行します。

a. [Select/Deselect] ボタンをクリックします。

ディスカバリ プロセスで検出されたデバイスをリストしたダイアログ ウィンドウが表示されます。

b. リストに表示されたデバイスをすべて選択します。

c. [Select] ボタンをクリックします。

再度 [Collect Config Task] ウィンドウが表示されます。

d. 必要に応じてコンフィギュレーション収集タスクの詳細設定を指定します。

e. [Submit] ボタンをクリックします。

次の項（「ステップ 10：サービスの表示と編集」（P.E-61））で説明する、サービスの表示と編集の準備ができました。

ステップ 10：サービスの表示と編集

MPLS VPN または L2VPN メトロ イーサネット サービスあるいはその両方の作成プロセスが成功すると、作成されたサービスを表示させ、サービス要求エディタを使用して変更できます。

L2VPN サービスを表示するには、次のステップを実行します。

ステップ 1　[Service Inventory] ウィンドウが現在アクティブになっていない場合、[Operate] > [Service Request] > [Service Request Manager] とクリックします。

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

必要に応じて、[Service Requests] ウィンドウに表示されているサービス要求を変更できます。

（注）　このプロセスの一部として MPLS VPN を編集する必要がある場合、「VPN の分割」（P.E-49）、「VPN の作成」（P.E-51）、「VPN リンクの詳細の表示」（P.E-52）、および「MPLS VPN の保存と MPLS VPN サービスの作成開始」（P.E-52）を参照してください。

ステップ 2　L2VPN メトロ イーサネット ネットワークのためのサービス要求変更について詳しくは、*『Cisco Prime Provisioning 6.3 User Guide』* を参照してください。

ステップ 3　このリリースについての一般的な情報については、リリース付属の *『Cisco Prime Provisioning 6.3 Release Notes』* を参照してください。

APPENDIX F

サービスに情報を追加する方法

この付録では、Prime Provisioning で追加情報機能がどのようにサポートされるかについて説明します。次の事項について説明します。

概要

追加情報機能によって、ユーザは、一連の属性（名前と値のペア）を XML ファイルで定義できます。ファイルは、後にポリシーに関連付けられます。追加情報の属性は、サービス要求に関連付けられる値を定義します。これらは、GUI のラベルおよび外観を定義します。サービス要求ワークフローで、これらの値は、ユーザが入力できます。テンプレートから、または xDE プロビジョニング ロジックからこれらの属性値にアクセスして、サービスの一部として設定されるデータ値を提供することもできます。これらの値でデータ ファイルを作成する代わりに、テンプレートと組み合わせて追加属性を使用することにより、ポリシーおよびサービス要求 GUI に対して、テンプレート属性値の入力を要求できます。この付録では、Prime Provisioning の追加情報機能を理解し、使用するために必要な情報を提供します。

前提条件と制限事項

追加情報機能の次の前提条件および制約事項に注意してください。

- 追加情報機能は、MPLS、L2VPN、VPLS、および EVC サービスだけでサポートされます。
- MPLS-TP および TEM ポリシーおよびサービス要求は、追加情報をサポートしません。
- VRF サービス要求にはポリシーが存在しないため、追加情報をサポートしません。

- サポートされるポリシーとサービス要求タイプでこの機能を使用する前に、追加情報の定義ファイルを作成する必要があります。これは、ユーザ定義の属性と値のペアを定義する XML ファイルです。ポリシー ワークフロー内の手順で、この定義ファイルを後にロードします。このコマンドの詳細については、「追加情報の定義ファイルの作成」（P.F-7）を参照してください。

追加情報 GUI ワークフローの概要

次の手順では、Prime Provisioning で追加情報を実装するために実行する必要がある作業の概要を示します。この付録の残りの項では、これらのトピックの詳細情報を示します。

1. 追加情報の定義ファイルを作成します（通常、付属の XSD を使用して検証します）。このファイルは、追加情報の属性を定義します。
2. 追加の属性値を参照する、または、xDE プロビジョニングのロジックを拡張するテンプレートを作成します。
3. テンプレートに対して、1 つのデフォルトのデータ ファイルを作成します。
4. 任意で、ネゲート テンプレートとネゲート データ ファイルを追加します。
5. 適切なポリシー タイプのポリシーを作成します。
6. ポリシー作成のワークフローの [Additional Information] ウィンドウに移動します。
7. 作成した追加情報の定義ファイルをロードします。ファイルが解析され、検証され、エラーが GUI に表示されます。
8. 提供されるフィールドの値を、必要に応じて入力します。変更が必要ない標準値である場合は、追加情報の定義ファイルでこれらの値を定義できます。
9. ポリシー ワークフローで、追加情報属性を編集可能または編集不可能としてマークします。これにより、ポリシーに基づいて、サービス要求内のこれらの値を編集できるかどうかが決まります。
10. ポリシー ワークフローでは、テンプレートをイネーブルにし、追加の値にアクセスするテンプレートを参照します。
11. ポリシーを保存します。追加情報が解析され、検証され、エラーが GUI に表示されます。
12. ポリシーに基づいて、サービス要求を作成します。
13. サービス要求ワークフローの [Service Request Editor] ウィンドウには、追加情報の属性が表示され、それらを編集することができます（編集可能な場合）。
14. サービス要求を保存します。追加情報が解析され、検証され、エラーが GUI に表示されます。

ポリシー ワークフローでの追加情報の設定

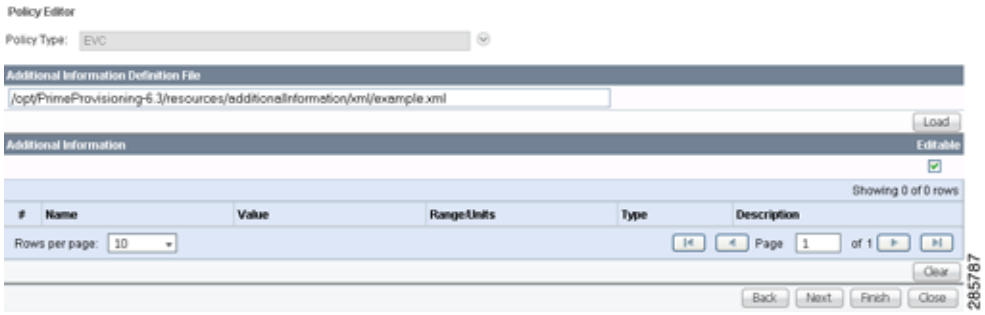
サポートされるポリシー タイプ内で追加情報機能を使用するには、次の手順を実行します。

ステップ 1　属性の追加先として、サポートされるポリシー タイプを編集または作成します。

ステップ 2　ポリシー ワークフロー ウィンドウをナビゲートし、必要に応じて属性値を設定します。

ワークフローでは複数のウィンドウが表示され、図 F-1 に示すように、[Additional Information] ウィンドウが表示されます。このウィンドウは、追加情報機能をサポートするすべてのポリシー タイプで、同様に表示され、動作します。

図 F-1　[Additional Information] ウィンドウ



このウィンドウには、ポリシー ワークフローの最後から 2 番目のウィンドウで、[Template Association] ウィンドウの前に表示されます。

[Additional Information] ウィンドウの使用は任意です。

ステップ 3　追加情報の属性と値のペアを定義する XML 定義ファイルをロードするには、[Load] ボタンをクリックします。

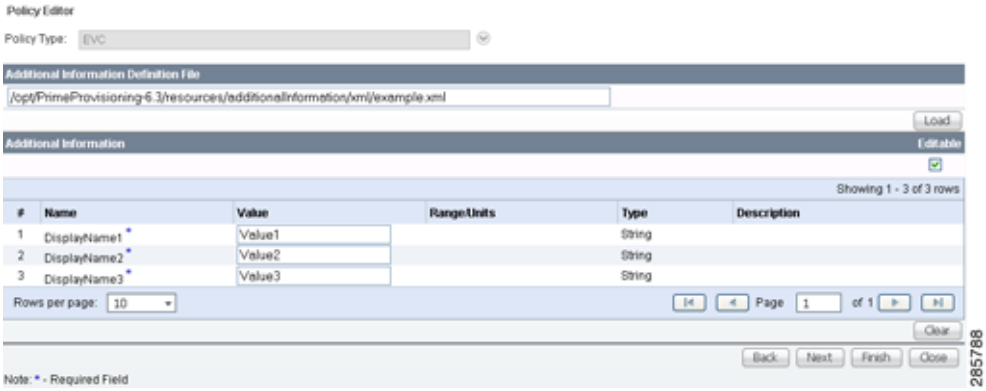
（注）　このファイルの作成方法については、「追加情報の定義ファイルの作成」（P.F-7）を参照してください。

定義ファイルのデフォルトのパスおよび名前は、次のとおりです。

$PRIMEP_HOME/resources/additionalInformation/xml/example.xml

ウィンドウが更新され、定義ファイルの属性と値のペアは、[Additional Information] セクションに表示されます（図 F-2 を参照）。

図 F-2　外部 XML 定義ファイルからロードされる属性



ステップ 4　必要に応じて、[Clear] ボタンをクリックして、ウィンドウの [Display] セクションに表示される属性をクリアできます。

ステップ 5　[Editable] チェックボックスをオンまたはオフにして、すべての追加情報属性を編集可能または編集不可能に設定します。

個々の属性を編集可能または編集不可能にすることはできません。

ステップ 6　ポリシーに対して、必要に応じて追加情報属性の値を設定します。

ウィンドウのこのセクションの内容と動作については、以下の説明を参照してください。

ステップ 7　[Next] をクリックして、ポリシー ワークフローの次のステップに進みます。

ステップ 8　Prime Provisioning の標準の手順に従って、ポリシー ワークフローを完了します。

ウィンドウの [Additional Information] セクションの内容と動作に関して、次の点に注意してください。

- 追加情報属性は、追加情報の定義ファイルで定義されている方法に基づいて、GUI 内でグループ化されます。
- グループが定義されている場合、各グループに対して、追加情報属性を含むページング テーブルの上部に、グループ名が表示されます。
- グループが定義ファイルで定義されていない場合、追加属性情報を含むページング テーブルだけが表示されます。
- 各属性は、ページング テーブル内の各行に表示されます。
- [Name] 列には、定義ファイルで定義されている属性の DisplayName が含まれます。属性が定義ファイルで必須としてマークされると、上付き文字のアスタリスクが DisplayName に付けられます。これは、ポリシー内で属性に値が必要なことを示すものではありません。これは、定義ファイルで値が定義される方法と、このポリシーを使用したサービス要求で、この属性に対して値が要求されることを示します。
- [Value] 列には、定義ファイルで定義されている属性の値が含まれます。
- [Range/Units] 列には、属性の範囲と単位の組み合わせが含まれます。
- [Description] 列には、定義ファイルで定義されている属性の説明が含まれます。

ポリシー ワークフローで定義ファイルに対して実行される検証チェック

XSD の検証に加えて、追加情報があるポリシーを Prime Provisioning データベースに保存するときに、解析チェックが実行され、追加情報の定義ファイルに対して検証が実行され、次の追加の検証チェックが実行されます。[Additional Information] セクションが編集不可能としてとマークされている場合（[Editable] チェックボックスがオフのままになっている場合）、必須としてマークされているすべての属性には、値が定義されている必要があります。これに該当しない場合は、検証エラーが発生します。この制限が課されるのは、ポリシーに基づくサービス要求で、すべての必須の追加情報属性に値が必要であるためです。（追加情報が編集可能ではないために）値を編集できない場合は、ポリシーに基づいてサービス要求を作成することはできません。

ポリシー ワークフローで追加情報に対して実行する検証チェックの詳細については、「XSD の検証方法」（P.F-10）を参照してください。

サービス要求ワークフローでの追加情報の設定

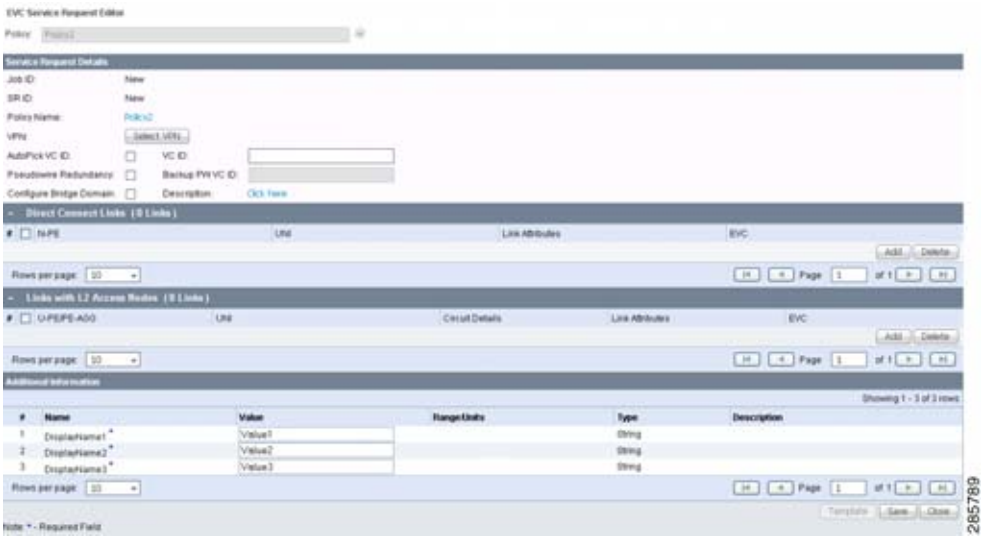
サービス要求ワークフローで追加情報機能を使用するには、次の手順を実行します。

ステップ 1　追加情報機能を使用して作成されたポリシーに基づいて、サービス要求を作成または編集します。

ステップ 2　サービス要求ワークフロー内の [Service Request Editor] ウィンドウに移動します。

サービス要求の基になるポリシーに定義された追加情報の属性がある場合、これらの属性は、図 F-3 に示すように表示されます。

図 F-3　[EVC Service Request] ウィンドウの追加情報属性



属性は、[Service Request Editor] ウィンドウですべての既存の属性の下に表示されます。属性情報の属性の形式は、ポリシーの対応するセクションと同じです。

ステップ 3　設定の要件に基づいて、[Service Request Editor] 内の属性を設定します。

属性の [Additional Information] セクションについて、次の点に注意してください。

- 追加情報の属性を編集できる場合は、属性の値を変更できます。
- 追加情報の属性が編集可能でない場合、値はグレーになり、変更できません。
- サービスの基になっているポリシーに追加情報属性がない場合、[Service Request Editor] ウィンドウに [Additional Information] セクションは表示されません。
- 必須としてマークされた属性には、値を設定する必要があります。この作業を行わないと、サービス要求を保存しようとしたときに、検証エラーが発生します。

ステップ 4　この段階では、追加情報属性にテンプレート変数をマッピングするために、テンプレートをデバイスに追加することもできます。詳細については、「テンプレートおよびデータ ファイルの追加属性の使用」（P.F-5）を参照してください。

ステップ 5　[Save] をクリックして、サービス要求を保存します。

テンプレートおよびデータ ファイルの追加属性の使用

Prime Provisioning の 2 か所で、追加情報属性にテンプレート変数をマッピングできます。

- テンプレートの作成時：これを行うには、次の手順を実行します。
  1. マッピングするテンプレート変数を編集し、文字列型として定義します。
  2. テンプレート変数のデフォルト値として、追加情報の属性名を入力します。追加情報の定義ファイルに定義されている正確な名前を使用する必要があります。

（注） テンプレートで使用される属性の先頭は、$ にする必要があります（*$name* など）。これは、この値が展開時に別の値に置き換えられることを示します。この属性のデフォルト値またはデータ ファイルの作成時には、追加情報属性の正確な名前を指定します。追加情報の属性名の先頭は $ にする必要があります。これは、この属性が、実際の値によって置き換えられ、固定の文字列ではないことをテンプレート マネージャに示します。

- テンプレート データ ファイルの作成時：これを行うには、テンプレート変数の値として、追加情報の属性名を入力します。追加情報の定義ファイルに定義されている正確な名前を使用する必要があります。

上記の 2 つのいずれかを実行した後、ポリシーまたはサービス要求にテンプレートやテンプレート データ ファイルを関連付けたときに、テンプレート変数は、ポリシーまたはサービス要求の対応するユーザ定義の追加情報属性の値に置き換えられます。

xDE プロビジョニングでの追加属性の使用

追加情報属性は、xDE プロビジョニング エンジンに渡される XML ドキュメントに追加されるため、xDE の手順でアクセスできます。

この XML ドキュメントには、次の XML ブロックを追加します。

```
<additionalInformation>
<attribute>
<name>Name1</name>
<value>123</value>
</attribute>
</additionalInformation>
```

（注） XML 属性ブロックは、各 *additionalInformation* 属性に対して繰り返す必要があります。

プロビジョニングのための現在の xDE の手順では、要求属性は、入力 XML ファイルを含むすべての手順に渡されます。xDE の手順で *additionalInformation* 属性値を使用するために、次のように MPLS SR XML 要求ドキュメントから属性 Name1 の値を抽出できます。

```
xml.xpathreference($serviceRequest,
"/MplsSR/additionalInformation/attribute[name=\"Name1\"]/value/text()")
```

また、すべての xDE の手順に渡される $additionalInformation 属性を通じて、追加情報の属性値にアクセスできます。この属性には、すべての追加情報属性の名前と値のペアのマップが含まれます。たとえば、次のように入力します。

```
map.get($additionalInformation, "Name1")
```

Name1 属性に関連付けられた値を返します

追加情報の定義ファイルの作成

ここでは、追加情報の定義ファイルの作成に使用できる参照情報を提供します。これは、必須 XML 要素の最小セットと追加のオプション要素が格納された XML ファイルです。このファイルは、「ポリシー ワークフローでの追加情報の設定」（P.F-2）の項で説明するように後でポリシーにロードされます。

必要最小限の XML 要素

例 F-1 は、追加情報の属性を定義するために、最低限必要な情報が含まれている追加情報のサンプル定義ファイルです。

例 F-1　　最小 XML 要素を備えた追加情報の定義ファイル

```
<additionalInformation>
<attribute>
        <name>Name1</name>
        <value>Value1</value>
    </attribute>
</additionalInformation>
```

必須 XML 要素の説明：

- *additionalInformation : additionalInformation* ブロックは、定義ファイルを開始および終了します。
- *attribute : attribute* ブロックは、定義する必要がある数の属性に対して、繰り返すことができます。各 *attribute* ブロックには、1 つの *name* 要素と 1 つの *value* 要素だけが必要です。
- *name : name* 要素には、ヌル以外の値を割り当てる必要があります。この値は、追加情報の定義ファイルで他の *name* 要素の値に対して一意である必要があります。
- *value : value* 要素には、任意の値（ヌルを含む）を割り当てることができます。この値は、追加情報の定義ファイルで他の *value* 要素の値に対して一意である必要はありません。

任意の XML 要素

追加情報の定義ファイルには、任意の XML 要素も含まれることがあります。ここでは、次の任意の要素について説明します。

- *group*
- *attribute/displayName*
- *attribute/description*
- *attribute/required*
- *attribute/type*
- *attribute/type/string*
- *attrribute/type/integer*
- *attribute/type/ipv4Address*
- *attribute/type/ipv6Address*
- a*ttribute/type/enumeration*

各要素がどのように解析され、どの条件でエラーが生成されるかについて説明します。

設定可能な任意の要素を含む追加情報のサンプル定義ファイルについては、「追加情報機能の例」（P.F-11）を参照してください。

group

0 以上の *group* 要素が存在することがあります。

各 *group* には、少なくとも 1 つの属性ブロックが必要です。*group* 内に属性が存在しない場合は、ファイルがロードされたときにエラーが発生します。

group が定義されている場合は、同じレベル（*group* 外）で属性を定義できません *groups* と *attributes* が同じレベルにあると、ファイルがロードされたときに、解析エラーが発生します。

group 要素には *name* が必要ですが、*name* は空白にすることができます。

group の *name* は、空白の名前を含め、一意にする必要があります（つまり、空白の *name* は、1 回だけ使用できます）。一意ではない *group* の *name* があると、ファイルがロードされたときに、重複名エラーが発生します。

attribute/displayName

displayName 要素には、ポリシーとサービス要求ワークフローの [Additional Information] テーブルで、属性の [Name] 列に表示されるテキストが含まれます。

displayName が定義されていない場合は、*name* 要素のテキストにデフォルト設定されます。

attribute/description

description 要素には、ポリシーとサービス要求ワークフローの [Additional Information] テーブルで、属性の [Description] 列に表示されるテキストが含まれます。*description* が定義されていない場合は、空の文字列にデフォルト設定されます。

attribute/required

required 要素には、属性が必要かどうかを示すブール値が含まれます。true に設定した場合、*name* テキストの横に上付きのアスタリスクが付けられます。このテキストは、ポリシーとサービス要求ワークフローの [Additional Information] テーブルで、属性の [Name] 列に表示されます。

ポリシーで、ある属性が必須として設定され、追加情報が編集不可能として設定されている場合にだけ、その属性に値を割り当てる必要があります。それ以外の場合は、属性に値を割り当てる必要はありません。

サービス要求で、ある属性が必須として設定されている場合、その属性には値セットを割り当てる必要があります。

required が定義されていない場合は、true にデフォルト設定されます。

attribute/type

type 要素には、定義している属性のタイプを記述します。

使用できるタイプは次のとおりです。

- *string*

- *integer*
- *ipv4Address*
- *ipv6Address*
- *enumeration*

type 要素が定義されていない場合、デフォルト タイプは *string* です（ranges または regex は定義されません）。

type 要素が定義されているが、サブ要素として使用可能ないずれかのタイプがない（タイプが存在しない、またはタイプがサポートされていない）場合、ファイルがロードされたときに、解析エラーが発生します。

属性に複数の *type* 要素がある場合は、ファイルがロードされたときに解析エラーが発生します。

attribute/type/string

string タイプには、次のような範囲および単位を記述する任意のパラメータがいくつかあります。

- *minLength*：文字列の最小長を定義します。属性の文字列値の長さは、検証に合格するために、この値以上にする必要があります。*minLength* が定義されていない場合、デフォルトは 1 です。
- *maxLength*：文字列の最大長を定義します。属性の文字列値の長さは、検証に合格するために、この値以下にする必要があります。
- *rangeUnits*：定義されている場合は range パラメータとともに、[Range]/[Units] 列に表示する単位を定義します。*rangeUnits* が定義されていない場合、デフォルトは「characters」です。
- *regex*：属性の文字列値を検証するために使用する正規表現を定義します。文字列値は、検証に合格するために、regex と一致する必要があります。また、*regex* が定義されている場合、*rangeDescription* には、「Pattern: regex」が追加されます。

attribute/type/integer

integer タイプには、次のような範囲および単位を記述する任意のパラメータがいくつかあります。

- *lower*：範囲の下限値を定義します。属性の *integer* 値は、検証に合格するために、この値以上にする必要があります。
- *upper*：範囲の上限値を定義します。属性の *integer* 値は、検証に合格するために、この値以下にする必要があります。
- *rangeUnits*：定義されている場合は range パラメータとともに、[Range]/[Units] 列に表示する単位を定義します。*rangeUnits* が定義されていない場合、デフォルトは空の文字列です。

attribute/type/ipv4Address

ipv4Address タイプには、次のような範囲および単位を記述する任意のパラメータがいくつかあります。

- *ipv4Lower*：範囲の *ipv4Lower* 値を定義します。属性の *ipv4Address* 値は、検証に合格するために、この値以上にする必要があります。
- *ipv4Upper*：範囲の *ipv4Upper* 値を定義します。属性の *ipv4Address* 値は、検証に合格するために、この値以下にする必要があります。

attribute/type/ipv6Address

ipv6Address タイプには、次のような範囲および単位を記述する任意のパラメータがいくつかあります。

- *ipv6Lower*：範囲の *ipv6Lower* 値を定義します。属性の *ipv6Address* 値は、検証に合格するために、この値以上にする必要があります。
- *ipv6Upper*：範囲の *ipv6Upper* 値を定義します。属性の *ipv6Address* 値は、検証に合格するために、この値以下にする必要があります。
- *rangeUnits*：定義されている場合は range パラメータとともに、[Range]/[Units] 列に表示する単位を定義します。*rangeUnits* が定義されていない場合、デフォルトは空の文字列です。

attribute/type/enumeration

enumeration タイプには、次のような範囲および単位を記述する任意のパラメータがいくつかあります。

- *enumOptions*：属性の列挙オプションを定義します。
  - 1 つ以上の *enumOptions* 要素を定義できます。
  - 少なくとも 1 つの *enumOption* 要素が定義されていない場合は、ファイルがロードされたときに解析エラーが発生します。
  - 空の文字列は、有効な *enumOption* 値ではありません。いずれかの *enumOption* 要素に空の文字列が割り当てられている場合は、ファイルがロードされたときに解析エラーが発生します。
- *rangeUnits*：定義されている場合は range パラメータとともに、[Range]/[Units] 列に表示する単位を定義します。*rangeUnits* が定義されていない場合、デフォルトは空の文字列です。

XSD の検証方法

追加情報 XML は、XML スキーマ定義（XSD）を使用して検証されます。XSD は、メイン JAR ファイルで定義されており、ユーザは編集できません。ただし、追加情報の定義ファイルを作成する必要があるユーザは、次の場所でファイルのコピーを入手できます。

$PRIMEP_HOME/resources/additionalInformation/extAttrs.xs

ユーザが、XSD 検証をオンまたはオフにすることができる DCPL プロパティがあります。DCPL プロパティは、**additionalInformation.XML.validateWithXSD** です。デフォルトではオンになります。

追加情報の定義ファイルの検証方法

実行される XSD 検証と解析チェックに加えて、追加情報の定義ファイルがポリシーにロードされたときに、次の追加の検証チェックが実行されます。

- *Enumeration* 型：属性値が定義されているが、いずれかの *enumeration* オプションと一致しないと、認証エラーが発生します。重複 *enumeration* オプションがある場合は、認証エラーが発生します。
- *integer*、*ipv4Address*、および *ipv6Address* 型：属性値が定義されている場合、その値は範囲に照らしてチェックされます（範囲が定義されていない場合は、デフォルトが使用されます）。この範囲外の場合は、認証エラーが発生します。

- *string* 型：属性値が定義されている場合は、（上記の）範囲チェックに加えて、*regex* と一致する必要があります（定義されている場合）。

追加情報機能の例

ここでは、追加情報機能のエンドツーエンドの例を示します。この例では、次の情報を提供します。

- テンプレート
- テンプレート データ ファイル
- 追加情報の定義ファイル
- GUI に表示される属性のリスト
- サンプル GUI 入力および生成されるコンフィグレット

テンプレート

次に、ポリシー テンプレート本体の例を示します。テンプレートは、非常に汎用的です。これは、アクセス ポートの E-Line サービスを示しています。これは、Cisco 3400 ルータの着信トラフィック用です。

```
policy-map qos-in-$Interface_Name
class class-default
#if($PIR_in_mbps==0)
     police cir $CIR_in_mbps m
#elseif($PIR_in_mbps!=0)
     police cir $CIR_in_mbps m pir $PIR_in_mbps m
#end

!
interface $Interface_Name
service-policy input qos-in-$Interface_Name
```

テンプレート データ ファイル

次に、ポリシーに添付されるテンプレート データ ファイルを示します。

```
CIR_in_mbps:   $CIR_in_mbps
PIR_in_mbps:   $PIR_in_mbps
Interface_Name: $UNI_INTERFACE_NAME
```

追加属性の定義ファイル

次に、追加情報の定義ファイルを示します。

```
<additionalInformation>
<group name="QoS">
        <attribute>
                <name>$CIR_in_mbps</name>
                <value></value>
                <displayName>Committed Bandwidth</displayName>
                <type>
```

```
                        <integer>
                                <lower>1</lower>
                                <upper>32000</upper>
                                <rangeUnits>Mbps</rangeUnits>
                        </integer>
                </type>
                <description>CIR value in Mbps</description>
                <required>true</required>
        </attribute>
        <attribute>
                <name>$PIR_in_mbps</name>
                <value></value>
                <displayName>Peak Bandwidth</displayName>
                <type>
                        <integer>
                                <lower>1</lower>
                                <upper>32000</upper>
                                <rangeUnits>Mbps</rangeUnits>
                        </integer>
                </type>
                <description>PIR value in Mbps</description>
                <required>false</required>
        </attribute>
</group>
</additionalInformation>
```

サービス要求ワークフローで表示される追加属性

この例に基づいて、2 つの新しい属性が、サービス要求ワークフローで表示されます。

- Committed Bandwidth
- Peak Bandwidth

[Committed Bandwidth] は必須フィールドで、[Peak Bandwidth] は任意のフィールドです。

ユーザ入力とサンプル コンフィグレット

次の例は、新しい属性に対するユーザ入力と、その結果生成されるコンフィグレットを示しています。

例 1

ユーザ入力：

- Committed Bandwidth：25

生成されるコンフィグレット：

```
policy-map qos-in-<uni interface>
class class-default
    police cir 25m
!
interface <uni interface>
service-policy input qos-in-<uni interface>
```

例 2

ユーザ入力：

- Committed Bandwidth：25
- Peak Bandwidth：50

生成されるコンフィグレット：

```
policy-map qos-in-<uni interface>
class class-default
    police cir 25 m pir 50 m
!
interface <uni interface>
service-policy input qos-in-<uni interface>
```

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/