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。

- 「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 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

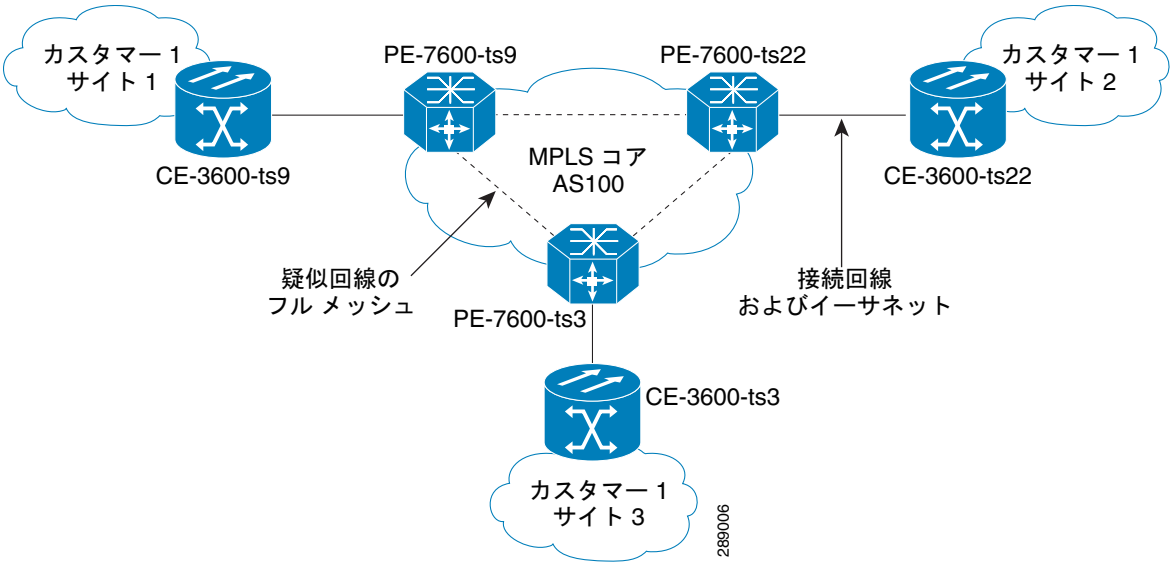
この項では、Prime Provisioning で VPLS 自動検出をイネーブルにする方法について説明します。次の事項について説明します。

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	N-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	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

```
!
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
```

N-PE

```
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

```
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
```

N-PE

```
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	N-PE
!	!
vlan 700	interface GigabitEthernet0/3/1/1.700
exit	l2transport
!	dot1q vlan 700
interface FastEthernet1/0/2	**!**
switchport trunk encapsulation dot1q	**l2vpn**
switchport trunk allowed vlan 700	**pw-class PW_AD3-AD7_Customer1**
switchport mode trunk	**encapsulation mpls**
switchport nonegotiate	**transport-mode vlan**
no keepalive	**preferred-path interface tunnel-te 1370**
mac access-group ISC-FastEthernet1/0/2 in	**fallback disable**
no cdp enable	**!**
spanning-tree bpdufilter enable	**!**
!	**xconnect group L2VPN_Customer1-Gold_class**
!	**p2p GoldPkg_AD3-AD7_Customer1**
interface GigabitEthernet1/0/1	interface GigabitEthernet0/3/1/1.700
switchport trunk encapsulation dot1q	neighbor 192.169.105.30 pw-id 1000
switchport trunk allowed vlan 700	**pw-class PW_AD3-AD7_Customer1**
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	
!	

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 mpls
switchport trunk encapsulation dot1q	no shutdown
switchport mode trunk	!
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

```
!
system mtu 1522
!
vlan 700
exit
!
interface FastEthernet1/0/2
switchport
switchport access vlan 700
switchport mode dot1q-tunnel
switchport nonegotiate
no keepalive
no cdp enable
spanning-tree portfast
spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 700
switchport mode trunk
!
```

N-PE

```
!
interface GigabitEthernet0/3/1/1.700
l2transport
 dot1q vlan 700
!
!
l2vpn
 pw-class PW_AD7-AD3_Cutsomer2
  encapsulation mpls
   transport-mode ethernet
   preferred-path interface tunnel-te 2730
  !
 !
 xconnect group ISC
  p2p cl-test-l2-12404-2--1000
   interface GigabitEthernet0/3/1/1.700
   neighbor 192.169.105.30 pw-id 1000
    pw-class PW_AD7-AD3_Cutsomer2
   !
```

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	N-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	**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

```
!
vlan 566
exit
!
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 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
```

N-PE

```
!
interface GigabitEthernet7/0/2
service instance 43 ethernet
encapsulation dot1q 566
xconnect 1.1.1.1 453366 encapsulation mpls
```

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）

```
!
vlan 500
exit
!
ethernet evc Customer1_166
!
interface GigabitEthernet7/0/4
no shutdown
service instance 1 ethernet Customer1_166
encapsulation dot1q 600
bridge-domain 500 split-horizon
!
interface ATM6/0/0.100 point-to-point
pvc 200/300
encapsulation aal5snap
bridge-domain 500 split-horizon
!
interface Vlan500
no ip address
description UT-9
xconnect 1.1.1.1 6 pw-class
ISC-pw-tunnel-400
no shutdown
```

N-PE 2（イーサネット）

```
!
vlan 800
exit
!
ethernet evc Customer1_166
!
interface GigabitEthernet7/0/5
no shutdown
service instance 1 ethernet Customer1_166
encapsulation dot1q 623
bridge-domain 800 split-horizon
!
interface Vlan800
description UT-9
xconnect 192.169.105.20 6 pw-class
ISC-pw-tunnel-900
```

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 ATM1/0/0.370 point-to-point
  no atm enable-ilmi-trap
  pvc 0/370 l2transport
  encapsulation aal5snap
  xconnect 192.169.105.10 123 pw-class inter-ether
  !
	interface GigabitEthernet0/0/0/4.458
	 l2transport
	  encapsulation dot1q 458
	 !
	 l2vpn
	  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）	N-PE 2（イーサネット）
!	interface GigabitEthernet0/0/0/25.341
interface ATM1/0/0.370 point-to-point	l2transport
no atm enable-ilmi-trap	encapsulation dot1q 341
pvc 0/370 l2transport	rewrite ingress tag push dot1q 430
encapsulation aal5snap	second-dot1q 349 symmetric
xconnect 10.20.21.1 4531 pw-class	!
ISC-pw-tunnel-1	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）

```
!
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 GigabitEthernet0/0/0/20.712
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。