CHAPTER 2

ISC サービスの設定

L2VPN ポリシー、VPLS ポリシーと FlexUNI/EVC ポリシー、およびサービス リクエストを作成するには、まず、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の要素を定義する必要があります。通常、これらの要素を 1 回作成します。

この章では、L2VPN サービスの Cisco IP Solution Center（ISC）サービスを設定する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。

（注） この章では、L2VPN に関連する ISC サービスの概要を示します。これらのサービスおよび他の基本的な ISC サービスの設定の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』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

ISC が管理するネットワーク要素はすべて、システムのデバイスとして定義する必要があります。要素は、ISC 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、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』を参照してください。

ISC をサポートするためのデバイス設定

ネットワークで ISC 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 透過モードで操作する必要があります。
- ループバック アドレスは、N-PE デバイスで設定する必要があります。

（注）　これらは、ネットワーク内で ISC が正常に動作するために必要な 2 つの最小デバイス設定です。ネットワーク内のデバイスが正常に動作するためには、他のデバイスのコンフィギュレーション手順も実行する必要があります。

VTP 透過モードでのスイッチの設定

セキュリティ上の理由で、ISC は、L2VPN サービス リクエストをプロビジョニングする前に、ERS サービスまたは EWS サービスに関与するすべてのスイッチで VTP を透過モードに設定することを要求します。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 モードが透過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

N-PE のループバック アドレスは、Any Transport over MPLS（AToMPLS）接続で適切に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される IP アドレスは、リモート ペア PE から到達可能である必要があります。Label Distribution Protocol（LDP; ラベル配布プロトコル）トンネルは、PE ペアの 2 つのループバック インターフェイス間で確立されます。PE ループバック アドレスは、[Edit PE device] ウィンドウで設定します。ISC の [Edit PE device] ウィンドウにアクセスするには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] を選択します。

ステップ 2　[Selection] ウィンドウで [PE Devices] を選択します。

ステップ 3　特定のデバイスを選択して、[Edit] ボタンをクリックします。

間違ったループバック アドレスをシステムに入力しないよう、GUI 上のループバック IP アドレス フィールドは読み取り専用になっています。[Select] ボタンをクリックすると表示される、別のポップアップ ウィンドウでループバック アドレスを選択します。こうすることによって、デバイスで定義されている有効なループバック アドレスだけが必ず選択されます。

さらに検索を絞り込むには、[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。すると、リストが LDP 終端のループバック インターフェイスのみに制限されます。

IOS XR サポートのためのデバイス設定

ISC 6.0 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。IOS XR は Cisco IOS ファミリの新しいメンバですが、常時接続の動作向けに設計された固有の自己回復および自己防衛機能を持つオペレーティング システムであり、システム容量を 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している Cisco XR12000 シリーズ ルータおよび CRS-1 シリーズ ルータだけでサポートされています。

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

- CE あり、またはなしのポイントツーポイント ERS。
- CE あり、またはなしの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 上の標準 UNI ポート（IOS XR を実行している N-PE デバイス上に UNI がある場合、[Link Attributes] ウィンドウの [Standard UNI Port] 属性がディセーブルになります）。
- IOS XR を実行している N-PE 上の SVI インターフェイス（IOS XR デバイスでは、[Link Attributes] ウィンドウの [N-PE Pseudo-wire On SVI] 属性がディセーブルになります）。
- 疑似回線トンネルの選択（IOS XR デバイスでは、[Link Attributes] ウィンドウの [PW Tunnel Selection] 属性がディセーブルになります）。
- IOS XR を実行している N-PE 上の EWS UNI（dot1q トンネルまたは Q-in-Q）。
- フレーム リレー /ATM および VPLS サービス。

L2VPN での IOS XR サポートをイネーブルにするには、次の手順を実行します。

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

有効値は、CLI、CLI_XML、および XML（デフォルト）です。

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

a. [Service Inventory] > [Inventory and Connection Manager] > [Devices] > [Create] を選択して、シスコ デバイスを作成します。[Create Cisco Device] ウィンドウが表示されます。

b. [Device and Configuration Access Information] の下にある [OS] 属性を [IOS_XR] に設定します。

（注）　DCPL プロパティの設定、およびシスコ デバイスの作成の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』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 リクエストを作成および導入します。

IOS XR デバイスのサンプル コンフィグレットは、付録 A「コンフィグレットの例」を参照してください。

サービス プロバイダーとサービス プロバイダー 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 Autonomous System（AS; 自律システム）番号を持つ ISP の管理ドメインです。プロバイダー管理ドメインが所有するネットワークは、バックボーン ネットワークと呼ばれます。1 つの ISP に 2 つの AS 番号がある場合は、その ISP を 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、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』を参照してください。

カスタマーとカスタマー サイトの定義

L2VPN をプロビジョニングする前に、カスタマーとカスタマー 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、唯一のカスタマーに所属して、多数の CPE を所有できます。カスタマーを作成する手順の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』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 を複数のサービス タイプで共有できます。VPLS では、各 VPLS インスタンスに 1 つの VPN が必要です。

VPN を作成するには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] を選択します。

ステップ 2　左のカラムで、[VPNs] をクリックします。

[VPNs] ウィンドウが表示されます。

VPN を作成する手順の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』を参照してください。

（注）　L2VPN 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名前だけです。この VPN には、MPLS VPN のような固有の意味がありません。

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、ISC 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、ISC 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、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。これが、VLAN に N-PE を自動的に割り当てる方法です。

開始前に次の事項を確実に行います。

- 作成するアクセス ドメインの名前の確認。
- 新しいアクセス ドメインに関連付けるサービス プロバイダーの作成。
- プロバイダーおよび PE デバイスに関連付けるプロバイダー リージョンの作成。
- 新しいアクセス ドメインに関連付ける PE デバイスの作成。
- 新しいアクセス ドメインに関連付ける各 VLAN の開始値およびサイズの確認。
- どの VLAN が管理 VLAN として機能するかの確認。

アクセス ドメインを作成するには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] を選択します。

ステップ 2　左のカラムで、[VPAccess Domains] をクリックします。

[Access Domains] ウィンドウが表示されます。

[Access Domains] ウィンドウの構成は、次のとおりです。

- [Access Domain Name] : アクセス ドメインの名前を示します。最初の 1 桁は文字である必要があります。この名前には、文字、数字、および句読文字（ピリオド、下線、ダッシュ）を使用できます。最大 80 文字です。アクセス ドメイン名ごとに、リストを並べ替えできます。
- [Provider Name] : プロバイダーの名前を示します。文字で始まる必要があります。文字、数字、および句読記号文字（ピリオド、下線、ダッシュ記号）を使用できます。最大 80 文字です。プロバイダー名ごとに、リストを並べ替えできます。
- [Access Domains] ウィンドウから次のボタンを使用して、アクセス ドメインを作成、編集、または削除できます。
  - [Create] : クリックすると、新しいアクセス ドメインを作成できます。アクセス ドメインを選択しない場合のみ選択できます。
  - [Edit] : クリックすると、選択したアクセス ドメイン（対応するボックスをオンにして選択）を編集できます。単一のアクセス ドメインを選択した場合のみ選択できます。
  - [Delete] : クリックすると、選択したアクセス ドメイン（対応するボックスをオンにして選択）を削除できます。1 つ以上のアクセス ドメインを選択した場合のみ選択できます。

VLAN プールの作成

L2VPN および VPLS では、ISC が VLAN をリンクに割り当てできるように VLAN プールを作成します。VLAN ID プールは、VLAN プールの開始値およびサイズを使用して定義されます。1 つのアクセス ドメインには、1 つの VLAN プールを接続できます。イーサネット サービスの導入中に、VLAN ID は、アクセス ドメインの既存の VLAN プールから自動的に割り当てできます。新しいサービスを導入すると、ISC は VLAN プールのステータスを [Available] から [Allocated] に変更します。自動割り当てにより、サービス プロバイダーは VLAN ID 割り当ての制御を強化できます。

VLAN ID は手動でも割り当てできます。

（注）　ISC サービスで VLAN ID を手動で設定している場合、VLAN ID が定義済みの VLAN プールの有効範囲外である場合は ISC が警告を出します。その場合、ISC は手動で定義された VLAN ID を VLAN プールに含めません。VLAN プールの範囲をプリセットし、手動で割り当てる VLAN ID の範囲がすべて含まれるようにすることを推奨します。

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

開始前に次の事項を確実に行います。

- 各 VLAN プールの開始番号の確認。
- 各 VLAN プール サイズの確認。
- VLAN プールのアクセス ドメインの作成。「アクセス ドメインの作成」（P.2-4）を参照してください。
- 各 VLAN プールが割り当てられるアクセス ドメインの名前の確認。

ISC が VLAN をリンクに自動的に割り当てるようにするには、次の手順を実行します。

ステップ 1　[Service Inventory] を選択します。

ステップ 2　[Inventory and Connection Manager] を選択します。

ステップ 3　[Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 4　[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 5　[Create] をクリックします。

[Create VLAN Pool] ウィンドウが表示されます。

ステップ 6　VLAN プールの開始番号を入力します。

ステップ 7　VLAN プールのサイズ値を入力します。

ステップ 8　[Access Domain] フィールドに適切なアクセス ドメインが表示されていない場合は、[Access Domain] フィールドの右にある [Select] をクリックします。

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

適切なアクセス ドメインが表示されている場合は、ステップ 9 に進みます。

a.　そのアクセス ドメインの左にある [Select] カラム内のボタンをクリックして、アクセス ドメイン名を選択します。

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

ステップ 9　[Save] をクリックします。

更新された [VLAN Resource Pools] 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 ドメインを作成したときに Reserved VLAN 情報が入力済みである場合、[Status] フィールドは [Allocated] になっています。アクセス ドメインを作成したときに Reserved VLAN 情報が入力されていない場合、[Status] フィールドは [Available] になっています。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 情報に入力します（「アクセス ドメインの作成」

（P.2-4）を参照）。VLAN プール ステータスは、作業を保存するときに [Resource Pools] ウィンドウで自動的に [Allocated] に設定されます。

ステップ 10　この手順を、VLAN 内で定義する各範囲分繰り返します。

VC ID プールの作成

VC ID プールは、VC ID プールの開始値および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 サービスまたは VPLS サービスの導入中は、VC ID を同じ VC ID プールから自動割り当てすることができ、また、VC ID を手動でも設定できます。

（注）　ISC サービスで VC ID を手動で設定しているとき、VC ID が定義済みの VC ID プールの有効範囲外である場合は ISC が警告を出します。その場合に ISC は、手動で定義された VC ID を VC ID プールに含めません。VC ID プールの範囲をプリセットし、手動で割り当てる VC ID の範囲がすべて含まれるようにすることを推奨します。

ネットワークごとに 1 つの VC ID プールを作成します。

VPLS インスタンスでは、すべての N-PE ルータが同じ VC ID を使用して、エミュレート Virtual Circuit（VC; 仮想回線）を確立します。VC-ID は、VPLS VPN とのコンテキストで、VPN ID とも呼ばれます（複数のアタッチメント回線は、VPLS インスタンスのプロバイダー コアで連結する必要があります。プロバイダー コアは、複数のアタッチメント回線を接続する仮想ブリッジをシミュレートする必要があります。この仮想ブリッジをシミュレートするため、VPLS インスタンスに関与しているすべての N-PE ルータは、エミュレート VC を N-PE ルータ間に形成します）。

（注）　VC ID は、回線またはポートを識別する 32 ビットの固有識別情報です。

開始する前に、作成する必要がある各 VC ID の次の情報を確認してください。

- VC プールの開始番号
- VC プールのサイズ

次の手順を、すべての L2VPN サービスおよび VPLS サービスに実行します。

ステップ 1　[Service Inventory] を選択します。

ステップ 2　[Inventory and Connection Manager] を選択します。

[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 3　[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、他のどのオブジェクトにも関連付けられません。

ステップ 4　[Create] をクリックします。

[Create VC ID Pool] ウィンドウが表示されます。

ステップ 5　VC プールの開始番号を入力します。

ステップ 6　VC プールのサイズ値を入力します。

ステップ 7　[Save] をクリックします。

更新された [VC ID 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 サービス リクエストまたは VPLS サービス リクエストを作成する前に、CE と PE 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）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るため、NPC は 1 回定義されますが、複数の L2VPN サービス リクエストまたは VPLS サービス リクエストの作成時に使用されます。

NPC リンクを作成するには、次の 2 つの方法があります。

- NPC GUI エディタによる作成。この実行方法の詳細については、「NPC GUI エディタによる NPC の作成」（P.2-9）を参照してください。
- 自動ディスカバリ プロセスによる作成。この実行方法の詳細については、「自動ディスカバリ プロセスによる NPC リンクの作成」（P.2-10）を参照してください。

NPC 定義は、次の作成規則に従う必要があります。

- NPC は、CE、UNI が存在するデバイスのアップリンク、またはリングで始まる必要があります。
- NPC は、N-PE、または N-PE 内で終わるリングで終了する必要があります。

CE と UNI との間のリンクに NPC 情報を挿入する場合は、次のような情報を入力します。

- 送信元デバイスは CE デバイスです。
- 送信元インターフェイスは、UNI に接続している CE ポートです。
- 宛先デバイスは UNI ボックスです。
- 宛先インターフェイスは UNI ポートです。

この場合に該当しない CE に NPC 情報を挿入する場合は、次の情報を入力します。

- 送信元デバイスは UNI ボックスです。
- 送信元インターフェイスは、該当する N-PE や他の U-PE、または PE-AGG に接続している UNI ボックス上の UP-LINK ポートであり、UNI ポートではありません。
- 宛先デバイスは、U-PE、PE-AGG、または N-PE です。
- 宛先インターフェイスは、N-PE、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（U-PE および CE）がない場合は、示される必要がある物理リンクがないため、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）が必要である場合（例：NPC が ence11、enpe1、および enpe12 に接続する）は、その NPC を次のように構築できます。

- mlce1 と mlpe4 の 2 つの端に接続するリンクを構築します。
- 作成したばかりのリンクにデバイス（enpe12）を挿入します。
- [Insert Device] をクリックして、デバイスを挿入します。

NPC GUI エディタによる NPC の作成

NPC GUI エディタにより NPC を作成するには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [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、リンクの始端として CE を選択し、終端として N-PE を選択します。リンク内に 3 つ以上のデバイスがある場合は、さらにデバイス（またはリング）を NPC に追加できます。

（注）　追加された新しいデバイスまたはリングは常に、選択されたデバイスの後に置かれますが、挿入された新しいデバイスまたはリングは、選択されたデバイスの前に置かれます。

ポイントツーポイントのエディタ上の各ラインは、物理リンクを表します。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 である必要あり）
- [Destination Interface]
- [Ring]

（注）　NPC にリングを追加または挿入する前に、リングを作成してリポジトリに保存する必要があります。NPC リングの作成についての情報を取得するには、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』を参照してください。

[Source Device] はリンクの始端で、[Destination Device] はリンクの終端です。

ステップ 2　[Create] をクリックします。

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

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　リンクの始端として 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 に挿入するには、[Add Device] または [Add Ring] をクリックします。たとえば、[Add Device] をクリックして、N-PE を追加します。

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] カラムで、[Select outgoing interface] をクリックします。

デバイスに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。

これで、作成した NPC が、[Named Physical Circuits] ウィンドウに表示されるようになります。

リング専用 NPC の作成

リングだけが含まれる NPC を、CE を指定せずに作成するには、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [Named Physical Circuits] を選択します。

ステップ 2　[Create] をクリックします。

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

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、[Select] をクリックします。リングが表示されます。

ステップ 5　[Select device] リンクをクリックして、リングの始端を選択します。

デバイスのリストを示すウィンドウが表示されます。

ステップ 6　リングの始端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　[Select device] リンクをクリックして、リングの終端を選択します。

ステップ 8　リングの終端であるデバイスを選択して、[Select] をクリックします。

（注）　リング専用 NPC の終端のデバイスは、N-PE である必要があります。

ステップ 9　リング専用 NPC を示す [Create a Named Physical Circuits] ウィンドウが表示されます。

ステップ 10　[Save] をクリックして、NPC をリポジトリに保存します。

2 つの N-PE でのアクセス リングの終端

ISC 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、万一 1 つのアクセス リンクがドロップした場合フェールオーバーを提供します。これは、アクセス リンクを 2 つの異なる N-PE デバイスで終端できる、NPC リングの特別な使用方法により実現できます。リングの N-PE は、N-PE のループバック 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 デバイスから始まり、オプションで PE-AGG デバイスを含む場合があります。

ISC でこれを実装する方法については、付録 D「2 つの N-PE でのアクセス リングの終端」を参照してください。

自動ディスカバリ プロセスによる NPC リンクの作成

自動ディスカバリでは、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、ISC データベースに保存できます。NPC は、検出された接続から、さらに抽出されます。

自動ディスカバリを使用して NPC を作成する手順の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』を参照してください。

IOS XR デバイスの疑似回線クラスの作成および変更

疑似回線クラス機能を使用すると、IOS XR 対応デバイスで L2VPN サービス リクエストの一部として導入される疑似回線に関連付けられる、さまざまな属性を設定できます。

（注）　疑似回線クラス機能は、IOS XR 3.6.1 以上でサポートされます。

疑似回線クラス機能は、カプセル化、転送モード、フォールバック オプション、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 ダウンの選択のコンフィギュレーションをサポートします。トンネル選択では、ISC Traffic Engineering Management（TEM）アプリケーションが使用されている場合は使用して、トンネルを選択できます。別の方法として、ネットワーク内でプロビジョニング済みのトンネルの ID を指定できます。IOS XR 対応デバイスの場合、疑似回線クラスは、L2VPN のサービス ポリシーまたはサービス リクエストに接続できる、ISC で個別に定義されたオブジェクトです。疑似回線クラス機能を使用できるのは、L2VPN の ERS、EWS、ならびに ATM ポリシーおよびサービス リクエストで使用する場合だけです。

この項では、疑似回線クラスを作成および変更する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 リクエスト内で使用する方法については、第 7 章「L2VPN ポリシーの作成」および第 8 章「L2VPN サービス リクエストの管理」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、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] に移動します。

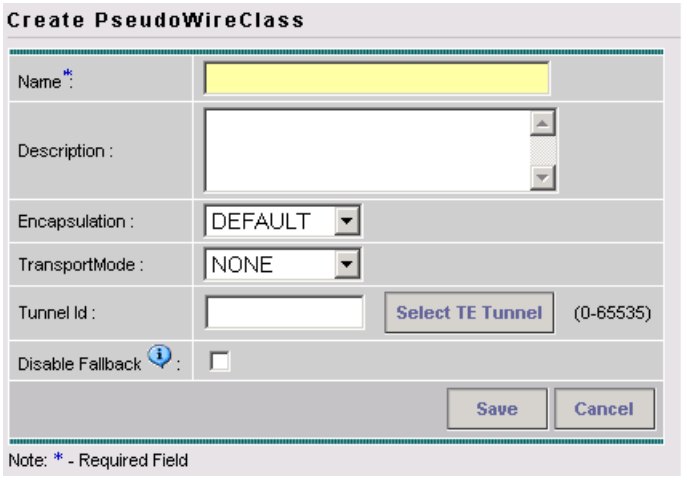
ステップ 2　[PseudoWireClass] アイコンをクリックします。

[Pseudowire Classes] ウィンドウが表示されます。

ステップ 3　[Create] ボタンをクリックします。

[Create PseudowireClass] ウィンドウが表示されます（図 2-1 を参照）。

図 2-1　[Create PseudoWireClass] ウィンドウ



ステップ 4　[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、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 文字を超えてはいけません。また、スペースを含めてはいけません。

ステップ 5　[Description] フィールドに、128 より少ない文字数で意味のある説明を入力します。

このフィールドは省略可能です。

ステップ 6　[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カプセル化のタイプは、MPLS だけです。

ステップ 7　[TransportMode] ドロップダウン リスト転送モードを選択します。選択肢は次のとおりです。

- [Ethernet]
- [Vlan]
- [NONE]（デフォルト）

（注）　[TransportMode] を [Vlan] に設定するときに、使用されている IOS XR のバージョンで疑似回線クラスがサポートされている場合は、疑似回線クラス経由で実行することを推奨します。IOS XR の特定のバージョンで疑似回線クラスがサポートされていない場合は、Dynamic Component Properties Library（DCPL）プロパティを使用して、「疑似回線クラスがサポートされない場合の転送モードの設定」（P.2-14）の項で説明されているように、[TransportMode] を設定する必要があります。

ステップ 8　ISC 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、またはデバイスで手動によりプロビジョニングされた TE トンネルの [Tunnel ID] を入力します。

この値は省略可能です。次の手順で説明されるように、ISC によってプロビジョニング済みの TE トンネルも選択できます。

ステップ 9　ISC によって以前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、[Select] をクリックします。これにより、[TE Tunnel] フィールドに、選択された TE トンネルの ID が入力されます。

（注）　TE トンネルが疑似回線クラスに関連付けられた後、または、サービス リクエストでプロビジョニングされた後に、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 リクエストに関連付けられている TE トンネルは、削除できません。

ステップ 10　[Disable Fallback] チェックボックスをオンにして、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します。

IOS XR のバージョンに基づいて、このオプションを選択します。このオプションは、IOS XR 3.6.1 では必須で、IOS XR 3.7 以上では省略可能です。

疑似回線クラス オブジェクトの変更

この項では、既存の疑似回線クラスを変更（編集）する方法、および編集操作の L2VPN サービス リクエストへの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、次の手順を実行します。

ステップ 1　[Service Inventory] > [Inventory and Connection Manager] > [PseudoWireClass] に移動します。

[PseudoWire Classes] 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、[Edit] をクリックします。

[Edit PseudoWire Class] ウィンドウが表示されます。

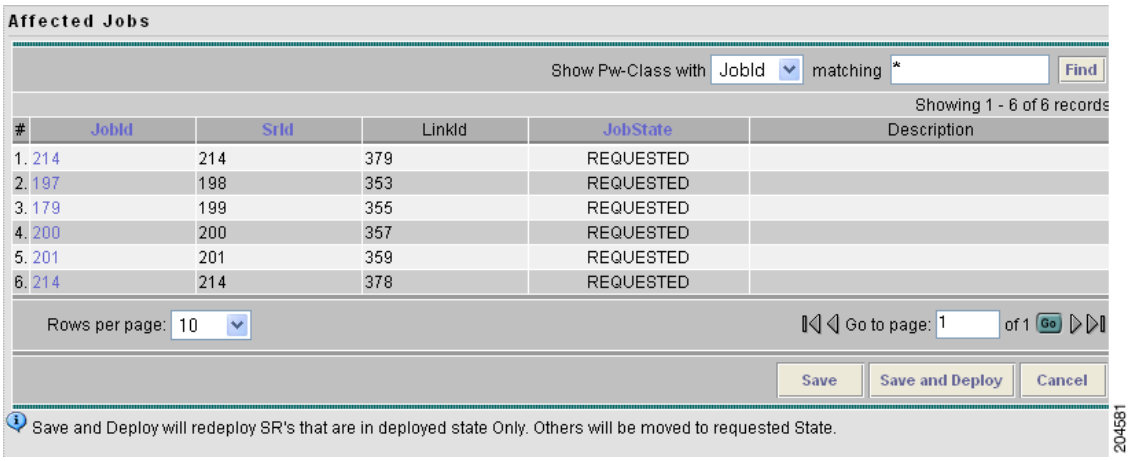
ステップ 3　変更を加えて [Save] をクリックします。

（注）　疑似回線クラスがどのサービス リクエストにも関連付けられない場合は、[Name] フィールドを編集できません。

変更されている疑似回線クラスが L2VPN サービス リクエストに関連付けられている場合は、図 2-2 に示されるように、影響を受けるサービス リクエストのリストを示す [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 リクエストのリストは、変更されている疑似回線クラスで転送モード、トンネル ID、またはディセーブル フォールバック値が変更された場合にだけ表示されます。

図 2-2　[Affected Jobs]



ステップ 4　[Save] をクリックして、変更された疑似回線クラスに関連付けられているサービス リクエストを更新します。

影響を受けるサービス リクエストが、[Requested] 状態になります。

ステップ 5　[Save and Deploy] をクリックして、変更された疑似回線クラスに関連付けられているサービス リクエストを更新および導入します。

導入タスクは、前に [Deployed] 状態であった、影響を受けるサービス リクエストに作成されます。

ステップ 6　[Cancel] をクリックして、変更された疑似回線クラスに対する変更内容を廃棄します。

この場合は、疑似回線クラスに関連付けられているサービス リクエストの状態はすべて変更されません。

疑似回線クラスがサポートされない場合の転送モードの設定

この項では、疑似回線の転送モードを、疑似回線クラスをサポートしない IOS XR のバージョンの Vlan タイプに設定する方法について説明します。これは、Dynamic Component Properties Library（DCPL）プロパティの設定により実行されます。その他の情報については、手順の後にある使用上の注意事項を参照してください。

次の手順を実行します。

ステップ 1　ISC で、[Administration] > [Control Center] > [Hosts] に移動します。

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、[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** に移動します。

ステップ 4　このプロパティを [true] に設定します。

ステップ 5　[Set Property] をクリックします。

すると、ISC は、疑似回線の VLAN 転送モード コンフィギュレーションを生成します。

使用上の注意事項は次のとおりです。

- 転送モードを [Vlan] に設定するには、使用されている IOS XR のバージョンで疑似回線クラスがサポートされている場合、疑似回線クラス経由でこれを実行することを推奨します。疑似回線クラス機能がサポートされない場合は、この項の手順で説明されているように、DCPL プロパティを使用して転送モードを設定する必要があります。
- DCPL プロパティが [true] に設定されている場合、DCPL プロパティの pseudoWireVlanMode は、PseudoWireClass TransportMode のデフォルト値を [Vlan] に設定するだけです。ユーザは常にデフォルト値を上書きできます。
- DCPL プロパティ pseudoWireVlanMode は、次の 2 つの方法で動作します。
  - DCPL プロパティは、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、DCPL プロパティは、推奨されないコマンドの **transport-mode vlan** を生成します。**transport-mode vlan** コマンドは、IOS XR 3.6 以降では推奨されないコマンドです。したがって、IOS XR デバイスで疑似回線クラスが選択されて、DCPL プロパティが [true] に設定された場合、**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** コマンドは共存できません。疑似回線クラスが存在する場合、疑似回線クラスは、推奨されない **transport-mode vlan** コマンドよりも優先されます。
- DCPL プロパティ pseudoWireVlanMode の値は、サービス リクエストの寿命の間は変更してはいけません。

IOS XR デバイスの L2VPN グループ名の定義

この項では、IOS XR デバイスのポリシーおよびサービス リクエストで使用可能な L2VPN グループ名を指定する方法について説明します。ポリシーおよびサービス リクエストの [L2VPN Group Name] 属性のドロップダウン リストに選択肢が表示されます。選択された名前は、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。これらの選択肢は、Dynamic Component Properties Library（DCPL）プロパティの設定により定義されます。

次の手順を実行します。

ステップ 1　ISC で、[Administration] > [Control Center] > [Hosts] に移動します。

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、[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** に移動します。

ステップ 4　[New Value] フィールドに、L2VPN グループ名のカ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。