



CHAPTER 3

Managing L2VPN and Carrier Ethernet Services

This chapter describes how to use Prime Provisioning policies and service requests to manage various L2VPN and Carrier Ethernet services. It contains the following sections:

- [Getting Started with L2VPN Services, page 3-1](#)
- [Setting Up the Prime Provisioning Services, page 3-6](#)
- [Creating an EVC Ethernet Policy, page 3-19](#)
- [Managing an EVC Ethernet Service Request, page 3-35](#)
- [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#)
- [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#)
- [Creating an L2VPN Policy, page 3-92](#)
- [Managing an L2VPN Service Request, page 3-120](#)
- [Creating a VPLS Policy, page 3-131](#)
- [Managing a VPLS Service Request, page 3-160](#)
- [Deploying, Monitoring, and Auditing Service Requests, page 3-167](#)
- [Using Autodiscovery for L2 Services, page 3-168](#)
- [Provisioning VPLS Autodiscovery on Devices using EVC Service Requests, page 3-168](#)
- [Setting Up VLAN Translation for L2VPN ERS \(EVPL\) Services, page 3-172](#)
- [Sample Configlets, page 3-177](#)

Getting Started with L2VPN Services

This section provides a road map to help you get started using the L2VPN component in Cisco Prime Provisioning 6.3. It contains the following sections:

- [Overview, page 3-2](#)
- [Prepopulating a Service by Selecting Endpoints in Prime Network, page 3-2](#)
- [Installing Prime Provisioning and Configuring the Network, page 3-2](#)
- [Configuring the Network to Support Layer 2 Services, page 3-3](#)
- [Setting Up Basic Prime Provisioning Services, page 3-3](#)
- [Working with EVC, L2VPN, and VPLS Policies and Service Requests, page 3-5](#)

- [A Note on Terminology Conventions, page 3-5](#)

Overview

Before you can use the L2VPN component to provision Layer 2 services, you must complete several installation and configuration steps, as outlined in this section. In addition, you should be familiar with basic concepts for Prime Provisioning and L2VPN services. The following subsections provide a summary of the key tasks you must accomplish to be able to provision L2VPN, VPLS and EVC services using Prime Provisioning. You can use the information in this section as a checklist. Where appropriate, references to other sections in this guide or to other guides in the Prime Provisioning documentation set are provided. See the referenced documentation for more detailed information. After the basic installation and configuration steps are completed for both Prime Provisioning and the L2VPN component, see the subsequent sections to create and provision L2VPN, VPLS and EVC services.

Prepopulating a Service by Selecting Endpoints in Prime Network

It is possible to create service by picking endpoints on a map in Prime Network Vision.

-
- | | |
|---------------|--|
| Step 1 | On any map, select one or more endpoint devices by using CTRL click. |
| Step 2 | In the right click menu, select Fulfill/Create Service . |
| Step 3 | You will be taken to the same first screen as you see when creating a service in Prime Provisioning. |
| Step 4 | Pick a policy.

Depending on the number of endpoints selected, not all policies will work. For example, you cannot create a point-to-point service if you have five endpoints selected, but you can create a VPLS or a L3 VPN. |
| Step 5 | Once you have selected the policy, the service request main page will appear as usual, prepopulated with links and with the selected devices. |
-

Installing Prime Provisioning and Configuring the Network

Before you can use the L2VPN module in Prime Provisioning to provision L2VPN or VPLS services, you must first install Prime Provisioning and do the basic network configuration required to support Prime Provisioning. Details on these steps are provided in [Chapter 2, “Before Setting Up Prime Provisioning.”](#) See that chapter for information about Prime Provisioning installation and general network configuration requirements.

**Note**

To use the L2VPN component within Prime Provisioning, you must purchase and activate the L2VPN license.

Configuring the Network to Support Layer 2 Services

In addition to basic network configuration required for Prime Provisioning, you must perform the following network configuration steps to support Layer 2 services. Information on doing these steps is not provided in the Prime Provisioning documentation. See the documentation for your devices for information on how to perform these steps.

1. Enable MPLS on the core-facing interfaces of the N-PE devices attached to the provider core.
2. Set up /32 loopback addresses on N-PE devices. These loopback addresses should be the termination of the LDP connection(s).
3. Set all Layer 2 devices (switches) to VTP transparent mode. This ensures that none of the switches will operate as VLAN servers and will prevent VLAN information from automatically propagating through the network.

Setting Up Basic Prime Provisioning Services

After the basic network configuration tasks are completed to support Prime Provisioning and L2 services, you use Prime Provisioning to define elements in the Prime Provisioning repository, such as providers and regions, customers and sites, devices, VLAN and VC pools, NPCs, and other resources that are necessary to provision L2 services. Detailed steps to perform general Prime Provisioning tasks are covered in [Chapter 2, “Before Setting Up Prime Provisioning.”](#) You can also find a summary of some important Prime Provisioning set up tasks in [Setting Up the Prime Provisioning Services, page 3-6](#). The information below is a checklist of basic Prime Provisioning services you must set up before provisioning L2 services.

Setting Up Providers, Customers, and Devices

Perform the following steps to set up providers, customers, and devices in the Prime Provisioning repository. These are global resources that can be used by all Prime Provisioning services.

1. **Set up service providers and regions.** The region is important because a single provider could have multiple networks. The region is used as a further level of differentiation to allow for such circumstances. To create a provider and a region, see [Setting Up Resources, page 2-40](#). See also [Defining a Service Provider and Its Regions, page 3-9](#).
2. **Set up customers and customer sites.** A customer is a requestor of a VPN service from an ISP. Each customer can own many customer sites. Each customer site belongs to one and only one Customer and can own many CEs. For detailed steps to create customers and sites, see [Setting Up Resources, page 2-40](#). See also [Defining Customers and Their Sites, page 3-9](#).
3. **Import or add raw devices.** Every network element that Prime Provisioning manages must be defined as a device in the Prime Provisioning repository. An element is any device from which Prime Provisioning can collect information. In most cases, devices are Cisco IOS routers and switches. You can set up devices in Prime Provisioning manually, through autodiscovery, or through importing device configuration files. For detailed steps for importing, adding, and collecting configurations for devices, see [Appendix E, “Inventory - Discovery.”](#) See also [Using Autodiscovery for L2 Services, page 3-168](#).
4. **Assign devices roles as PE or CE.** After devices are created in Prime Provisioning, you must define them as customer (CE) or provider (PE) devices. You do this by editing the device attributes on individual devices or in batch editing through the Prime Provisioning inventory manager. To set device attributes, see [Setting Up Devices and Device Groups, page 2-1](#).

Setting Up the N-PE Loopback Address

Within Prime Provisioning, you must set the loopback address on the N-PE device(s). For details about this procedure, see [Setting Up the N-PE Loopback Address, page 3-4](#).

Setting Up Prime Provisioning Resources for L2VPN and VPLS Services

Some Prime Provisioning resources, such as access domains, VLAN pools, and VC pools are set up to support Prime Provisioning L2VPN and VPLS services only. To set up these resources, perform the following steps.

1. **Create access domain(s).** For L2VPN and VPLS, you create an access domain if you provision an Ethernet-based service and want Prime Provisioning to automatically assign a VLAN for the link from the VLAN pool. For each Layer 2 access domain, you need a corresponding access domain object in Prime Provisioning. During creation, you select all the N-PE devices that are associated with this domain. Later, one VLAN pool can be created for an access domain. For detailed steps to create access domains, see [Setting Up Resources, page 2-40](#). See also [Creating Access Domains, page 3-9](#).
2. **Create VLAN pool(s).** A VLAN pool is created for each access domain. For L2VPN and VPLS, you create a VLAN pool so that Prime Provisioning can assign a VLAN to the links. VLAN ID pools are defined with a starting value and a size. For detailed steps to create VLAN pools, see [Setting Up Resources, page 2-40](#). See also [Creating VLAN Pools, page 3-10](#).
3. **Create VC pool(s).** VC ID pools are defined with a starting value and a size of the VC ID pool. A given VC ID pool is not attached to any inventory object (a provider or customer). Create one VC ID pool per network. For detailed steps to create VC pools, see [Setting Up Resources, page 2-40](#). See also [Creating a VC ID Pool, page 3-11](#).

Setting Up NPCs

Before creating an L2VPN or VPLS service request, you must predefine the physical links between CEs and PEs or between U-PEs and N-PEs. The Named Physical Circuit (NPC) represents a link going through a group of physical ports. Thus, more than one logical link can be provisioned on the same NPC. Therefore, the NPC is defined once but used by several L2VPN or VPLS service requests. For detailed steps to create NPCs, see [Setting Up Logical Inventory, page 2-53](#). See also [Creating Named Physical Circuits, page 3-12](#).

Setting Up VPNs

You must define VPNs before provisioning L2VPN or VPLS services. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance. To define VPNs, see [Setting Up Logical Inventory, page 2-53](#). See also [Defining VPNs, page 3-9](#).

Working with EVC, L2VPN, and VPLS Policies and Service Requests

After you have set up providers, customers, devices, and resources in Prime Provisioning, you are ready to create EVC, L2VPN, or VPLS policies, provision service requests (SRs), and deploy the services. After the service requests are deployed you can monitor, audit and run reports on them. All of these tasks are covered in this guide. To accomplish these tasks, perform the following steps.

1. **Review overview information about L2 services concepts.** See the chapter “Prime Provisioning Layer 2 VPN Concepts” in the *Cisco Prime Provisioning 6.3 Administration Guide*.
 2. **Set up an EVC, L2VPN, or VPLS policy.** See the appropriate section, depending on the type of policy you want to create:
 - [Creating an EVC Ethernet Policy, page 3-19](#)
 - [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#)
 - [Creating an L2VPN Policy, page 3-92](#)
 - [Creating a VPLS Policy, page 3-131](#)
 3. **Provision the EVC, L2VPN, or VPLS service request.** See the appropriate section, depending on the type service request you want to provision:
 - [Managing an EVC Ethernet Service Request, page 3-35](#)
 - [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#)
 - [Managing an L2VPN Service Request, page 3-120](#)
 - [Managing a VPLS Service Request, page 3-160](#)
 4. **Deploy the service request.** See [Deploying, Monitoring, and Auditing Service Requests, page 3-167](#).
 5. **Check the status of deployed services.** You can use one or more of the following methods:
 - Monitor service requests. See [Deploying, Monitoring, and Auditing Service Requests, page 3-167](#).
 - Audit service requests. See [Deploying, Monitoring, and Auditing Service Requests, page 3-167](#).
 - Run L2 and VPLS reports. See [Generating L2 and VPLS Reports, page 10-32](#).
-

A Note on Terminology Conventions

The Prime Provisioning GUI and this chapter of the user guide use specific naming conventions for Ethernet services. These align closely with the early MEF conventions. This is expected to be updated in future releases of to conform with current MEF conventions. For reference, the equivalent terms used by the MEF forum are summarized in [Table 3-1](#).

See the chapter “Prime Provisioning Layer 2 VPN Concepts,” in the *Cisco Prime Provisioning 6.3 Administration Guide*, for more information on terminology conventions and how these align with underlying network technologies.

Table 3-1 Ethernet Service Terminology Mappings

Term Used in GUI and This User Guide	Current MEF Equivalent Term
L2VPN over MPLS Core	
Ethernet Wire Service (EWS)	Ethernet Private Line (EPL)
Ethernet Relay Service (ERS)	Ethernet Virtual Private Line (EVPL)
ATM over MPLS (ATMoMPLS)	—
Frame Relay over MPLS (FRoMPLS)	—
VPLS Over MPLS Core	
Ethernet Wire Service (EWS) or Ethernet Multipoint Service (EMS)	Ethernet Private LAN (EP-LAN)
Ethernet Relay Service (ERS) or Ethernet Relay Multipoint Service (ERMS)	Ethernet Virtual Private LAN (EVP-LAN)
VPLS over Ethernet Core	
Ethernet Wire Service (EWS)	Ethernet Private LAN (EP-LAN)
Ethernet Relay Service (ERS)	Ethernet Virtual Private LAN (EVP-LAN)

Setting Up the Prime Provisioning Services

To create L2VPN, VPLS, and EVC policies and service requests, you must first define the service-related elements, such as target devices, VPNs, and network links. Normally, you create these elements once.

This section contains the basic steps to set up the Cisco Prime Provisioning 6.3 resources for L2VPN services. It contains the following sections:

- [Creating Target Devices and Assigning Roles \(N-PE or U-PE\), page 3-7](#)
- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Defining a Service Provider and Its Regions, page 3-9](#)
- [Defining Customers and Their Sites, page 3-9](#)
- [Defining VPNs, page 3-9](#)
- [Creating Access Domains, page 3-9](#)
- [Creating VLAN Pools, page 3-10](#)
- [Creating Outer VLAN Pools, page 3-11](#)
- [Creating a VC ID Pool, page 3-11](#)
- [Creating Named Physical Circuits, page 3-12](#)
- [Creating and Modifying Pseudowire Classes, page 3-15](#)
- [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#)



Note

This section presents high-level information on Prime Provisioning services that are relevant to L2VPN. For more detailed information on setting up these and other basic Prime Provisioning services, see [Chapter 2, “Before Setting Up Prime Provisioning.”](#)

Creating Target Devices and Assigning Roles (N-PE or U-PE)

Every network element that Prime Provisioning manages must be defined as a device in the system. An element is any device from which Prime Provisioning can collect information. In most cases, devices are Cisco IOS routers that function as N-PE, U-PE, or P. For detailed steps to create devices, see [Setting Up Devices and Device Groups, page 2-1](#).

Configuring Device Settings to Support Prime Provisioning

Two device settings must be configured to support the use of Prime Provisioning in the network:

- Switches in the network must be operating in VTP transparent mode.
- Loopback addresses must be set on N-PE devices.

**Note**

These are the two minimum device settings required for Prime Provisioning to function properly in the network. You must, of course, perform other device configuration steps for the proper functioning of the devices in the network.

Configuring Switches in VTP Transparent Mode

For security reasons, Prime Provisioning requires VTPs to be configured in transparent mode on all the switches involved in ERS or EWS services before provisioning L2VPN service requests. To set the VTP mode, enter the following Cisco IOS commands:

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

Enter the following Cisco IOS command to verify that the VTP mode has changed to transparent:

```
Switch# Show vtp status
```

Setting the Loopback Addresses on N-PE Devices

The loopback address for the N-PE has to be properly configured for an Any Transport over MPLS (AToMPLS) connection. The IP address specified in the loopback interface must be reachable from the remote pairing PE. The label distribution protocol (LDP) tunnels are established between the two loopback interfaces of the PE pair. To set the PE loopback address, perform the following steps.

-
- Step 1** Choose **Inventory > Provider Devices**.
The Provider Devices window appears.
 - Step 2** Choose a specific PE device and click the **Edit** button.
The Edit Provider Device window appears.
To prevent a wrong loopback address being entered into the system, the Loopback IP Address field on the GUI is read-only.
 - Step 3** Choose the loopback address by clicking the **Select** button (in the Loopback IP Address attribute).
The Select Device Interface window appears.
 - Step 4** Choose one of the loopback addresses listed in the Interface Name column.

This step ensures that you choose only a valid loopback address defined on the device.

- Step 5** To further narrow the search, you can check the **LDP Termination Only** check box and click the **Select** button.

This limits the list to the LDP-terminating loopback interface(s).

Setting Up Devices for IOS XR Support

L2VPN in Cisco Prime Provisioning 6.3, supports devices running Cisco's IOS XR software. IOS XR, a new member of the Cisco IOS family, is a unique self-healing and self-defending operating system designed for always-on operation while scaling system capacity up to 92Tbps. In L2VPN, IOS XR is only supported on Cisco XR12000 and CRS-1 series routers functioning as network provider edge (N-PE) devices.

In L2VPN, the following E-line services are supported for IOS XR:

- Point-to-point ERS with or without a CE.
- Point-to-point EWS with or without a CE.

The following L2VPN features are not supported for IOS XR:

- Standard UNI port on an N-PE running IOS XR. (The attribute **Standard UNI Port** in the Link Attributes window is disabled when the UNI is on an N-PE device running IOS XR.)
- SVI interfaces on N-PEs running IOS XR. (The attribute **N-PE Pseudo-wire On SVI** in the Link Attributes window is disabled for IOS XR devices.)
- Pseudowire tunnel selection. (The attribute **PW Tunnel Selection** in the Link Attributes window is disabled for IOS XR devices.)
- EWS UNI (dot1q tunnel or Q-in-Q) on an N-PE running IOS XR.
- Frame Relay/ATM and VPLS services.

To enable IOS XR support in L2VPN, perform the following steps.

- Step 1** Set the DCPL property Provisioning\Service\l2vpn\platform\CISCO_ROUTER\IosXRConfigType to XML.

Possible values are CLI, CLI_XML, and XML (the default).

- Step 2** Create the device in Prime Provisioning as an IOS XR device, as follows:

- Create the Cisco device by choosing **Inventory > Devices > Create Cisco Device**.
- Choose **Cisco Device** in the drop-down list.
The Create Cisco Router window appears.
- Set the **OS** attribute, located under Device and Configuration Access Information, to **IOS_XR**.



Note For additional information on setting DCPL properties and creating Cisco devices, see [Appendix B, "Property Settings."](#)

- Step 3** Create and deploy L2VPN service requests, following the procedures in this guide.

Sample configlets for IOS XR devices are provided in [Sample Configlets, page 3-177](#).

Defining a Service Provider and Its Regions

You must define the service provider administrative domain before provisioning L2VPN. The provider administrative domain is the administrative domain of an ISP with one BGP autonomous system (AS) number. The network owned by the provider administrative domain is called the backbone network. If an ISP has two AS numbers, you must define it as two provider administrative domains. Each provider administrative domain can own many region objects.

For detailed steps to define the provider administrative domain, see [Setting Up Resources, page 2-40](#).

Defining Customers and Their Sites

You must define customers and their sites before provisioning L2VPN. A customer is a requestor of a VPN service from an ISP. Each customer can own many customer sites. Each customer site belongs to one and only one Customer and can own many CPEs. For detailed steps to create customers, see [Setting Up Resources, page 2-40](#).

Defining VPNs

You must define VPNs before provisioning L2VPN or VPLS. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance. For detailed steps to create VPNs, see [Setting Up Logical Inventory, page 2-53](#).

**Note**

The VPN in L2VPN is only a name used to group all the L2VPN links. It has no intrinsic meaning as it does for MPLS VPN.

Creating Access Domains

For L2VPN and VPLS, you create an Access Domain if you provision an Ethernet-based service and want Prime Provisioning to automatically assign a VLAN for the link from the VLAN pool.

For each Layer 2 access domain, you need a corresponding Access Domain object in Prime Provisioning. During creation, you select all the N-PE devices that are associated with this domain. Later, one VLAN pool can be created for an Access Domain. This is how N-PEs are automatically assigned a VLAN.

Before you begin, be sure that you:

- Know the name of the access domain that you want to create.
- Have created a service provider to associate with the new access domain.
- Have created a provider region associated with your provider and PE devices.
- Have created PE devices to associate with the new access domain.
- Know the starting value and size of each VLAN to associate with the new access domain.
- Know which VLAN will serve as the management VLAN.

For detailed steps on creating Access Domains, see [Setting Up Resources, page 2-40](#).

Creating VLAN Pools

For L2VPN and VPLS, you create a VLAN pool so that Prime Provisioning can assign a VLAN to the links. VLAN ID pools are defined with a starting value and a size of the VLAN pool. A VLAN pool can be attached to an access domain. During the deployment of an Ethernet service, VLAN IDs can be autoallocated from the access domain's pre-existing VLAN pools. When you deploy a new service, Prime Provisioning changes the status of the VLAN pool from Available to Allocated. Autoallocation gives the service provider tighter control of VLAN ID allocation.

You can also allocate VLAN IDs manually.



Note

When you are setting a manual VLAN ID on a Prime Provisioning service, Prime Provisioning warns you if the VLAN ID is outside the valid range of the defined VLAN pool. If so, Prime Provisioning does not include the manually defined VLAN ID in the VLAN pool. We recommend that you preset the range of the VLAN pool to include the range of any VLAN IDs that you manually assign.

Create one VLAN pool per access domain. Within that VLAN pool, you can define multiple ranges.

Before you begin, be sure that you:

- Know each VLAN pool start number.
- Know each VLAN pool size.
- Have created an access domain for the VLAN pool.
- Know the name of the access domain to which each VLAN pool will be allocated.

To have Prime Provisioning automatically assign a VLAN to the links, perform the following steps.

Step 1 Choose **Service Design > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **VLAN** from the **Pool Type** drop-down list.

Step 3 Click **Create**.

The Create New VLAN Resource Pool window appears.

Step 4 Enter a VLAN Pool Start number.

Step 5 Enter a VLAN Pool Size number.

Step 6 If the correct access domain is not showing in the Access Domain field, click **Select** to the right of Access Domain field.

The Select Access Domain dialog box appears.

If the correct access domain is showing, continue with Step 9.

- a. Choose an Access Domain Name by clicking the button in the Select column to the left of that Access Domain.
- b. Click **Select**. The updated Create New VLAN Resource Pool window appears.

Step 7 Click **Save**.

The updated VLAN Resource Pool window appears.

**Note**

The pool name is created automatically, using a combination of the provider name and the access domain name.

**Note**

The Status field reads “Allocated” if you already filled in the Reserved VLANs information when you created the access domain. If you did not fill in the Reserved VLANs information when you created the access domain, the Status field reads “Available.” To allocate a VLAN pool, you must fill in the corresponding VLAN information by editing the access domain. (See [Creating Access Domains, page 3-9](#).) The VLAN pool status automatically sets to “Allocated” on the Resource Pools window when you save your work.

Step 8 Repeat this procedure for each range you want to define within the VLAN.

Creating Outer VLAN Pools

An outer VLAN pool is used in conjunction with the AutoPick Outer VLAN attribute in EVC Ethernet and EVC ATM-Ethernet policies. For instructions on how to set up outer VLAN pools, see the section [Resource Pools, page 2-44](#).

Creating a VC ID Pool

VC ID pools are defined with a starting value and a size of the VC ID pool. A given VC ID pool is not attached to any inventory object (a provider or customer). During deployment of an L2VPN or VPLS service, the VC ID can be autoallocated from the same VC ID pool or you can set it manually.

**Note**

When you are setting a manual VC ID on a Prime Provisioning service, Prime Provisioning warns you if the VC ID is outside the valid range of the defined VC ID pool. If so, Prime Provisioning does not include the manually defined VC ID in the VC ID pool. We recommend that you preset the range of the VC ID pool to include the range of any VC IDs that you manually assign.

Create one VC ID pool per network.

In a VPLS instance, all N-PE routers use the same VC ID for establishing emulated Virtual Circuits (VCs). The VC-ID is also called the VPN ID in the context of the VPLS VPN. (Multiple attachment circuits must be joined by the provider core in a VPLS instance. The provider core must simulate a virtual bridge that connects the multiple attachment circuits. To simulate this virtual bridge, all N-PE routers participating in a VPLS instance form emulated VCs among them.)

**Note**

VC ID is a 32-bit unique identifier that identifies a circuit/port.

Before you begin, be sure that you have the following information for each VC ID pool you must create:

- The VC Pool start number
- The VC Pool size

For all L2VPN and VPLS services, perform the following steps.

-
- Step 1** Choose **Service Design > Resource Pools**.
The Resource Pools window appears.
- Step 2** Choose **VC ID** from the **Pool Type** drop-down list.
Because this pool is a global pool, it is not associated with any other object.
- Step 3** Click **Create**.
The Create New VC ID Resource Pool window appears.
- Step 4** Enter a VC pool start number.
- Step 5** Enter a VC pool size number.
- Step 6** Click **Save**.
The updated Resource Pools window appears.
-

Creating Named Physical Circuits

Before creating an L2VPN or VPLS service request, you must predefine the physical links between CEs and PEs. The Named Physical Circuit (NPC) represents a link going through a group of physical ports. Thus, more than one logical link can be provisioned on the same NPC; therefore, the NPC is defined once but used during several L2VPN or VPLS service request creations.

There are two ways to create the NPC links:

- Through an NPC GUI editor. For details on how to do this, see [Creating NPCs Through the NPC GUI Editor, page 3-13](#).
- Through the autodiscovery process. For details on how to do this, see [Creating NPC Links Through the Autodiscovery Process, page 3-15](#).

An NPC definition must observe the following creation rules:

- An NPC must begin with a CE or an up-link of the device where UNI resides or a Ring.
- An NPC must end with an N-PE or a ring that ends in an N-PE.

If you are inserting NPC information for a link between a CE and UNI, you enter the information as:

- Source Device is the CE device.
- Source Interface is the CE port connecting to UNI.
- Destination Device is the UNI box.
- Destination interface is the UNI port.

If you are inserting NPC information for a CE not present case, you enter the information as:

- Source Device is the UNI box.
- Source Interface is the UP-LINK port, not the UNI port, on the UNI box connecting to the N-PE or another U-PE or PE-AGG.
- Destination Device is the U-PE, PE-AGG, or N-PE.
- Destination Interface is the DOWN-LINK port connecting to the N-PE or another U-PE or PE-AGG.

If you have a single N-PE and no CE (no U-PE and no CE), you do not have to create an NPC since there is no physical link that needs to be presented.

If an NPC involves two or more links (three or more devices), for example, it connects ence11, enpe1, and enpe12, you can construct this NPC as follows:

- Build the link that connects two ends: mlce1 and mlpe4.
- Insert a device (enpe12) to the link you just made.

Creating NPCs Through the NPC GUI Editor

To create NPCs through the NPC GUI editor, perform the following steps.

Step 1 Choose **Inventory > Named Physical Circuits**.

The Named Physical Circuits window appears.

To create a new NPC, you choose a CE as the beginning of the link and a N-PE as the end. If more than two devices are in a link, you can add or insert more devices (or a ring) to the NPC.



Note

The new device or ring added is always placed after the device selected, while a new device or ring inserted is placed before the device selected.

Each line on the Point-to-Point Editor represents a physical link. Each physical link has five attributes:

- **Source Device**
- **Source Interface**
- **Destination Device** (must be an N-PE)
- **Destination Interface**
- **Ring**



Note

Before adding or inserting a ring in an NPC, you must create a ring and save it in the repository. To obtain information on creating NPC rings, see [Setting Up Logical Inventory, page 2-53](#).

Source Device is the beginning of the link and **Destination Device** is the end of the link.

Step 2 Click **Create**.

The Create Named Physical Circuits window appears.

Step 3 Click **Add Device**.

The Select a Device window appears.

Step 4 Choose a CE as the beginning of the link.

Step 5 Click **Select**.

The device appears in the Create a Named Physical Circuits window.

Step 6 To insert another device or a ring, click **Insert Device** or **Insert Ring**.

To add another device or ring to the NPC, click **Add Device** or **Add Ring**. For this example, click **Add Device** to add the N-PE.

Step 7 Choose a PE as the destination device.


Step 8 Click **Select**.

The device appears.

- Step 9** In the Outgoing Interface column, click **Select outgoing interface**.
A list of interfaces defined for the device appears.
- Step 10** Choose an interface from the list and click **Select**.
- Step 11** Click **Save**.
The Create Named Physical Circuits window now displays the NPC that you created.
-

Creating a Ring-Only NPC

To create an NPC that contains only a ring without specifying a CE, perform the following steps.

-
- Step 1** Choose **Inventory > Named Physical Circuits**.
- Step 2** Click **Create**.
The Create Named Physical Circuits window appears.
- Step 3** Click **Add Ring**.
The Select NPC Ring window appears.
- Step 4** Choose a ring and click **Select**. The ring appears.
- Step 5** Click the **Select device** link to select the beginning of the ring.
A window appears showing a list of devices.
- Step 6** Choose the device that is the beginning of the ring and click **Select**.
- Step 7** Click the **Select device** link to choose the end of the ring.
- Step 8** Choose the device that is the end of the ring and click **Select**.
- 

Note The device that is the end of the ring in a ring-only NPC must be an N-PE.
-
- Step 9** The Named Physical Circuits window appears showing the Ring-Only NPC.
- Step 10** Click **Save** to save the NPC to the repository.
-

Terminating an Access Ring on Two N-PEs

Prime Provisioning supports device-level redundancy in the service topology to provide a failover in case one access link should drop. This is accomplished through a special use of an NPC ring that allows an access link to terminate at two different N-PE devices. The N-PEs in the ring are connected by a logical link using loopback interfaces on the N-PEs. The redundant link starts from a U-PE device and may, optionally, include PE-AGG devices.

For details on how to implement this in Prime Provisioning, see [Appendix C, “Terminating an Access Ring on Two N-PEs.”](#)

Creating NPC Links Through the Autodiscovery Process

With autodiscovery, the existing connectivity of network devices can be automatically retrieved and stored in the Prime Provisioning database. NPCs are further abstracted from the discovered connectivity.

For detailed steps to create NPCs using autodiscovery, see [Setting Up Logical Inventory, page 2-53](#).

Creating and Modifying Pseudowire Classes

The pseudowire class feature provides you with the capability to configure various attributes associated with a pseudowire that is deployed as part of an L2VPN service request on IOS XR-capable devices.



Note

The pseudowire class feature is supported for IOS XR 3.6.1 and higher.

The pseudowire class feature supports configuration of the encapsulation, transport mode, fallback options, and selection of a traffic engineering tunnel down which the pseudowire can be directed. For tunnel selection, you can select the tunnel using the Prime Provisioning Traffic Engineering Management (TEM) application, if it is being used. Otherwise, you can specify the identifier of a tunnel that is already provisioned within the network. For IOS XR-capable devices, the pseudowire class is a separately defined object in the Prime Provisioning repository, which can be attached to an L2VPN service policy or service request. The pseudowire class feature is only available for use in L2VPN ERS, EWS and ATM policies and service requests.

This section describes how to create and modify pseudowire classes. For information on how the pseudowire class is associated to a L2VPN policy and used within a service request, see [Creating an L2VPN Policy, page 3-92](#), and [Managing an L2VPN Service Request, page 3-120](#).

Creating a Pseudowire Class

To create a pseudowire class, perform the following steps.

Step 1 Choose **Inventory > Pseudowire Class**.

The Pseudowire Class window appears.

Step 2 Click the **Create** button.

The Create Pseudowire Class window appears.

Step 3 In the **Name** field, enter a valid PseudoWireClass name.

The pseudowire class name is used for provisioning **pw-class** commands on the IOS XR device. The name should not exceed 32 characters and should not contain spaces.

Step 4 In the **Description** field, enter a meaningful description of less than 128 characters.

This field is optional.

Step 5 Choose the **MPLS** encapsulation type from the **Encapsulation** drop-down list.



Note

Currently, the only encapsulation type supported is MPLS.

Step 6 Choose the transport mode from the **TransportMode** drop-down list. The choices are:

- **NONE** (default)

- **Vlan**
- **Ethernet**



Note If you want to set the TransportMode to Vlan, we recommend you do this via a pseudowire class, if supported by the version of IOS XR being used. If pseudowire class is not supported in a particular version of IOS XR, then you must set the TransportMode using a Dynamic Component Properties Library (DCPL) property, as explained in the section [Configuring the Transport Mode When Pseudowire Classes are Not Supported, page 3-18](#).

- Step 7** Choose the protocol from the **Protocol** drop-down list. The choices are:
- **NONE** (default)
 - **LDP**—Configures LDP as the signaling protocol for this pseudowire class.
- Step 8** To configure sequencing on receive or transmit, choose a selection from the **Sequencing** drop-down list. The choices are:
- **NONE** (default)
 - **BOTH**—Configures sequencing on receive and transmit.
 - **TRANSMIT**—Configures sequencing on transmit.
 - **RECEIVE**—Configures sequencing on receive.
- Step 9** Enter a **Tunnel ID** of a TE tunnel that has already been provisioned by Prime Provisioning or that has been manually provisioned on the device.
- This value is optional. You can also select a TE tunnel that has already been provisioned by Prime Provisioning, as covered in the next step.
- Step 10** Click **Select TE Tunnel** if you want to select a TE tunnel that has been previously provisioned by Prime Provisioning.
- The Select TE Tunnel pop-up window appears. Choose a TE tunnel and click **Select**. This populates the TE Tunnel field with the ID of the selected TE tunnel.



Note After a TE tunnel is associated to a pseudowire class or provisioned in a service request, you will receive an error message if you try to delete the TE tunnel using the Traffic Engineering Management (TEM) application. TE tunnels associated with a pseudowire class or service request cannot be deleted.

- Step 11** Check the **Disable Fallback** check box to disable the fallback option for the pseudowire tunnel.
- Choose this option based on your version of IOS XR. It is required for IOS XR 3.6.1 and optional for IOS XR 3.7 and above.

Modifying a Pseudowire Class

This section describes how to modify (edit) an existing pseudowire class and how the editing operation might impact L2VPN service requests.

To modify a pseudowire class, perform the following steps.

Step 1 Choose **Inventory > Pseudowire Class**.

The Pseudowire Class window appears.

Step 2 Select the pseudowire class object you want to modify, and click **Edit**.

The Pseudowire Class Edit window appears.

Step 3 Make the desired changes and click **Save**.



Note The Name field is not editable if the pseudowire class is associated with any service requests.

If the pseudowire class being modified is associated with any L2VPN service requests, the Affected Jobs window appears, which displays a list of affected service requests



Note A list of affected service requests only appears if the Transport Mode, Tunnel ID, or Disable Fallback values are changed in the pseudowire class being modified.

Step 4 Click **Save** to update service requests associated with the modified pseudowire class.

The impacted service requests are moved to the Requested state.

Step 5 Click **Save and Deploy** to update and deploy service requests associated with the modified pseudowire class.

Deployment tasks are created for the impacted service requests that were previously in the Deployed state.

Step 6 Click **Cancel** to discard changes made to the modified pseudowire class.

In this case, no change of state occurs for any service requests associated with the pseudowire class.

Deleting a Pseudowire Class

To delete a Pseudowire class, follow these steps:



Note A Pseudowire Class that is in use with a service request or policy cannot be deleted.

Step 1 Choose **Inventory > Pseudowire Class**.

The Pseudowire Classes window appears.

Step 2 Check the check box(es) next to the pseudowire class(es) you want to delete.

Step 3 Click the **Delete** button and a window appears with the selected pseudowire class name.

Step 4 Click the **Delete** button to confirm that you want to delete the specified pseudowire class(es).

Step 5 Click **Cancel** if you want to return without deleting the selected pseudowire class(es).

Configuring the Transport Mode When Pseudowire Classes are Not Supported

This section describes how to configure the pseudowire transport mode to be of type Vlan for versions of IOS XR that do not support pseudowire classes. This is done through setting a Dynamic Component Properties Library (DCPL) property. See the usage notes following the steps for additional information.

Perform the following steps.

-
- Step 1** In Prime Provisioning, navigate to **Administration > Hosts**.
 - Step 2** Check a check box for a specific host and click the **Config** button.
 - Step 3** Navigate to the DCPL property **Services\Common\pseudoWireVlanMode**.
 - Step 4** Set the property to **true**.
 - Step 5** Click **Set Property**.
- Prime Provisioning then generates VLAN transport mode configuration for the pseudowire.
-

Usage notes:

- To set the transport mode to Vlan, it is recommended that you do this via a pseudowire class, if supported by the version of IOS XR being used. If the pseudowire class feature is not supported, then the transport mode must be set using a DCPL property, as explained in the steps of this section
- The DCPL property pseudoWireVlanMode only sets the default value for PseudoWireClass TransportMode as Vlan if the DCPL property is set to true. Users can always over ride it.
- The DCPL property pseudoWireVlanMode acts in a dual way:
 - It sets a default value for PseudoWireClass TransportMode to Vlan.
 - In the absence of a pseudowire class, it generates a deprecated command **transport-mode vlan**. The **transport-mode vlan** command is a deprecated command in IOS XR 3.6 and later. Thus, when a pseudowire class is selected for an IOS XR device and the DCPL property is also set to true, the **transport-mode vlan** command is not generated. Pseudowire class and the **transport-mode vlan** command do not co-exist. If a pseudowire class is present, it takes precedence over the deprecated **transport-mode vlan** command.
- The value of the DCPL property pseudoWireVlanMode should not be changed during the life of a service request.

Defining L2VPN Group Names for IOS XR Devices

This section describes how to specify the available L2VPN group names for policies and service requests for IOS XR devices. The choices appear in a drop-down list of the L2VPN Group Name attribute in policies and service requests. The name chosen is used for provisioning the L2VPN group name on IOS XR devices. The choices are defined through setting a Dynamic Component Properties Library (DCPL) property.

Perform the following steps.

-
- Step 1** In Prime Provisioning, navigate to **Administration > Hosts**.
 - Step 2** Check a check box for a specific host and click the **Config** button.
 - Step 3** Navigate to the DCPL property **Services\Common\l2vpnGroupNameOptions**.

- Step 4** Enter a comma-separated list of L2VPN group names in the **New Value** field.
- Step 5** Click **Set Property**.
-

Creating an EVC Ethernet Policy

This section contains an overview of EVC support in Cisco Prime Provisioning 6.3, as well as the basic steps to create an EVC Ethernet policy. It contains the following subsections:

- [Defining the EVC Ethernet Policy, page 3-19](#)
- [Setting the Service Options, page 3-20](#)
- [Setting the EVC Attributes, page 3-23](#)
- [Setting the Interface Attributes, page 3-29](#)
- [Enabling Template Association, page 3-34](#)

For information on creating EVC Ethernet service requests, see [Managing an EVC Ethernet Service Request, page 3-35](#).

**Note**

For a general overview of EVC support in Prime Provisioning, see the chapter “Layer 2 Concepts” in the *Cisco Prime Provisioning 6.3 Administration Guide*.

**Note**

For Ethernet (E-Line and E-LAN) services, use of the EVC policy and service request is recommended. If you are provisioning services using the EVC syntax, or plan to do so in the future, use the EVC service. Existing services that have been provisioned using the L2VPN and VPLS service policy types are still supported and can be maintained with those service types. For ATM and FRoMPLS services, use the L2VPN service policy, as before.

Defining the EVC Ethernet Policy

You must define an EVC Ethernet policy before you can provision a service. A policy can be shared by one or more service requests that have similar service requirements.

A policy is a template of most of the parameters needed to define an EVC service request. After you define it, an EVC policy can be used by all the EVC service requests that share a common set of characteristics. You create a new EVC policy whenever you create a new type of service or a service with different parameters. EVC policy creation is normally performed by experienced network engineers.

An Editable check box in for an attribute in the policy gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change the value(s) of the particular policy attribute. If the value is *not* set to editable, the service request creator cannot change the attribute.

You can also associate Prime Provisioning templates and data files with a policy. See [Chapter 9, “Managing Templates and Data Files”](#) for more about using templates and data files in policies.

It is also possible to create user-defined attributes within a policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#)

To define an EVC Ethernet policy, you start by setting the service type attributes. To do this, perform the following steps.

-
- Step 1** Choose **Service Design > Create Policy**.
The Policy Editor window appears.
- Step 2** Choose **EVC** from the Policy Type drop-down list.
The Policy Editor window appears.
- Step 3** Enter a **Policy Name** for the EVC policy.
- Step 4** Choose the **Policy Owner** for the EVC policy.
There are three types of EVC policy ownership:
- Customer ownership
 - Provider ownership
 - Global ownership—Any service operator can make use of this policy.
- This ownership has relevance when the Prime Provisioning Role-Based Access Control (RBAC) comes into play. For example, an EVC policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy. Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.
- Step 5** Click **Select** to choose the owner of the EVC policy.
The policy owner was established when you created customers or providers during Prime Provisioning setup. If the ownership is global, the Select function does not appear.
- Step 6** Choose the **Policy Type**.
The choices are:
- **ETHERNET**—This section.
 - **ATM**—See [Creating an ATM Policy, page 4-19](#).
 - **ATM-Ethernet Interworking**—See [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#).
 - **TDM Circuit Emulation**—See [Creating a CEM TDM Policy, page 4-7](#).
- Step 7** Click **Next**.
The Service Options window appears.
- Step 8** Continue with the steps contained in the next section, [Setting the Service Options, page 3-20](#).
-

Setting the Service Options

This section describes how to set the service options for the EVC Ethernet policy.
To set the EVC service options, perform the following steps.

-
- Step 1** Check the **CE Directly Connected to EVC** check box if the CEs are directly connected to the N-PE.
This check box is not checked by default.

**Note**

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this EVC policy can modify the editable parameter during EVC service request creation.

Usage notes:

- If the check box is checked, a service request created using this policy can have only directly connected links. No Ethernet access nodes will be involved.
- If the check box is unchecked, a service request created using this policy might or might not have Ethernet access nodes in the links.
- When a CE is directly connected to the N-PE, NPCs are not applicable to the link while creating service requests.
- When a CE is not directly connected to the N-PE, NPCs are used during service request creation, as per standard Prime Provisioning behavior. There is no change in NPC implementation to support EVC functionality.

Step 2 Check the **All Links Terminate on EVC** check box if all links need to be configured with EVC features.

This check box is not checked by default. Usage notes:

- If the check box is checked, a service request created using such policy will have all links using the EVC feature.
- If the check box is unchecked, zero or more links can use the EVC feature. This ensures that existing platforms can still be used in one or more links while delivering the services. This allows the possibility of a link with EVC support being added in the future.

**Note**

If the check box is unchecked, in the service request creation process the user must indicate whether or not the created link is EVC or non-EVC.

- If no links are expected to use the EVC feature even in the future (for example, if the provider is not planning to upgrade to the EVC infrastructure for the service that is being created), existing Prime Provisioning policy types (L2VPN or VPLS) can be used instead of EVC.

Step 3 Choose an **MPLS Core Connectivity Type** from the drop-down list.

**Note**

The core option supports MPLS only. There is no L2TPv3 support for this service.

The choices are:

- **PSEUDOWIRE**—Choose this option to allow connectivity between two N-PEs across the MPLS core. This option does not limit the service to point-to-point (E-Line). This is because even with the PSEUDOWIRE option selected, there can still be multiple CEs connected to a bridge domain on one or both sides of the pseudowire.
- **LOCAL**—Choose this option for local connect cases in which there is no connectivity required across the MPLS core.

Local connect supports the following scenarios:

- All interfaces on the N-PE are EVC-capable and using the EVC infrastructure. This is configured by associating all of the customer traffic on these interfaces to a bridge domain. This consumes a VLAN ID on the N-PE (equal to the bridge domain ID).

- Some interfaces on the N-PE are EVC-capable, while others are switch-port-based. In such cases, all of the customer traffic on the interfaces that are configured with the EVC infrastructure are associated to a bridge domain. The traffic on the non-EVC interfaces (and all the access nodes/interfaces beyond this N-PE) are configured with the Service Provider VLAN ID, where the Service Provider VLAN ID is the same as the bridge domain ID for the EVC-based services.
- Only two interfaces on the N-PE are involved, and both are based on EVC-capable line cards. In the first case, the operator might choose not to configure the bridge domain option. In this case, the **connect** command that is used for the local connects are used, and the global VLAN is conserved on the device. If the operator chooses to configure with the bridge domain option, both interfaces are associated to a bridge domain ID, so that additional local links can be added to the service in future. This consumes a VLAN ID (bridge domain ID) on the N-PE.
- **VPLS**—Choose this option to allow connectivity between multiple N-PEs across the MPLS core.
 - This includes support for multi-segment pseudowire over an MPLS-TP enabled network. Some or all of the LSPs interconnecting the VPLS instances can be admitted onto existing MPLS-TP tunnels (which may have been provisioned using Prime Provisioning). The LSPs may be configured as multi-segment pseudowires, where each hop can be admitted onto an MPLS-TP tunnel. Prime Provisioning will automatically route the multi-segment pseudowire along the shortest path, taking into consideration any included and/or excluded nodes and/or tunnels.
 - The LSP/pseudowire labels may be statically allocated by Prime Provisioning. This eliminates the need for a directed protocol to be run within the VPLS to do label exchange and therefore further eliminates the need for IP connectivity between the endpoints in the VPLS.
 - The pool of MPLS labels is shared across VPLS and MPLS-TP services (if they come from the same MPLS static label range on the device). Otherwise Prime Provisioning uses the separate tunnel and service label ranges that are configured on the device. Labels already in use are discovered and removed from the label pool to ensure unique allocation of MPLS labels.

There is no limit on the number of N-PEs across the MPLS core within a service request. However, many service requests can refer to the same customer-associated VPN.

**Note**

Attributes available in subsequent windows of the policy workflow dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE, LOCAL, or VPLS). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

**Note**

Also, some attributes are supported only on IOS or IOS XR platforms. Attributes apply to both platforms, unless otherwise noted. All platform-specific attributes are visible in the policy workflow windows. Later, when a service request is created based on the policy (and specific devices are associated with the service request), platform-specific attributes are filtered from service request windows, depending on the device type (IOS or IOS XR).

Step 4 Check the **Configure With Bridge Domain** check box to determine bridge domain characteristics.

The behavior of the Configure With Bridge-Domain option works in tandem with the choice you selected in the MPLS Core Connectivity Type option, as follows.

- **PSEUDOWIRE** as the MPLS Core Connectivity Type. There are two cases:
 - A. With EVC:

- If **Configure With Bridge Domain** is checked, the policy configures pseudowires under SVIs associated to the bridge domain.
- If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under the service instance. This conserves the global VLAN.

B. Without EVC:

- If **Configure With Bridge Domain** is checked, the policy configures pseudowires as in L2VPN services (with SVIs).
- If **Configure With Bridge Domain** is unchecked, the policy configures pseudowires directly under subinterfaces.

Only pseudowires can be either configured directly under service instance of the corresponding EVC-capable interface or under SVIs associated to the bridge domain.

- **LOCAL** as the MPLS Core Connectivity Type:
 - If **Configure With Bridge Domain** is checked, the policy allows either point-to-point or multipoint local connect services.
 - If **Configure With Bridge Domain** is unchecked, Prime Provisioning allows only point-to-point local connects without bridge domain.

- **VPLS—Configure With Bridge Domain** is checked by default and non-editable.

When the VPLS service option is selected, VPLS-specific service options appear.

- Check the **Static VPLS (AutoPick MPLS Labels)** check box to automatically allocate static labels.
The static labels are allocated when the service request is saved.
- Check the **Configure Pseudowire Segment(s)** check box to allow the VPLS service to be admitted onto MPLS-TP tunnels and “stitch” together tunnels to form a simulated end-to-end path.

Step 5 Click **Next**.

The EVC Attributes window appears.

Step 6 Continue with the steps contained in the next section, [Setting the EVC Attributes, page 3-23](#).

Setting the EVC Attributes

This section describes how to set the EVC attributes for the EVC Ethernet policy.

EVC attributes are organized under the following categories:.

- Service Attributes
- VLAN Match Criteria
- VLAN Rewrite Criteria

The following sections describe how to set the options under each category.

Setting the Service Attributes

The EVC service attributes are the same no matter which MPLS Core Connectivity Type has been selected.

To set the EVC service attributes, perform the following steps.

-
- Step 1** Check the **AutoPick Service Instance ID** check box to specify that the service instance ID will be autogenerated and allocated to the link during service request creation.
- If the check box is unchecked, while setting the Prime Provisioning link attributes during service request creation, Prime Provisioning will prompt the operator to specify the service instance ID.
- Usage notes:
- The service instance ID represents an Ethernet Flow Point (EFP) on an interface in the EVC infrastructure. The service instance ID is locally significant to the interface. This ID has to be unique only at the interface level. The ID must be a value from 1 to 8000.
 - There are no resource pools available in Prime Provisioning from which to allocate the service instance IDs.
 - It is the responsibility of the operator creating the service request to maintain the uniqueness of the ID at the interface level.
- Step 2** Check the **AutoPick Service Instance Name** check box to have Prime Provisioning autogenerated a service instance name when you create a service request based on the policy. The autogenerated value is in the following pattern: *CustomerName_ServiceRequestJobID*.
- If the check box is unchecked, then you can enter a value during service request creation.
- Step 3** Check the **Enable PseudoWire Redundancy** check box to enable pseudowire redundancy (alternative termination device) under certain conditions.
- Usage notes:
- Enable Pseudo Wire Redundancy is only available if the MPLS Core Connectivity Type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options, page 3-20](#)).
 - See [Appendix C, “Terminating an Access Ring on Two N-PEs”](#) and, specifically, the section [Using N-PE Redundancy in FlexUNI/EVC Service Requests, page C-3](#), for notes on how this option can be used.
- Step 4** Check the **AutoPick VC ID** check box to have Prime Provisioning autopick the VC ID during service request creation.
- If this check box is unchecked, the operator will be prompted to specify a VC ID during service request creation.
- Usage notes:
- This attribute is available only if MPLS Core Connectivity of Type was set as PSEUDOWIRE or VPLS in the Service Options window (see [Setting the Service Options, page 3-20](#)).
 - When AutoPick VC ID is checked, Prime Provisioning allocates a VC ID for pseudowires from the Prime Provisioning-managed VC ID resource pool.
 - If MPLS Core Connectivity of Type is VPLS, Prime Provisioning allocates the VPLS VPN ID from the Prime Provisioning-managed VC ID resource pool.
- Step 5** Check the **AutoPick VFI Name** check box to have Prime Provisioning autopick the virtual forwarding instance (VFI) name during service request creation.
- If this check box is unchecked, the operator will be prompted to specify a VFI name during service request creation.

**Note**

The AutoPick VFI Name attribute is only applicable if the MPLS Core Connectivity Type is set as VPLS. For other core types (PSEUDOWIRE and LOCAL), this attribute will not be displayed.

Step 6 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID for the service request during service request creation.

If this check box is unchecked, the operator will be prompted to specify a VLAN ID during service request creation.

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain/VLAN ID is picked from the existing Prime Provisioning VLAN pool. Once the VLAN ID is assigned in the service request, Prime Provisioning makes the VLAN ID unavailable for subsequent service requests.
- In the case of manual VLAN ID allocation, Prime Provisioning does not manage the VLAN ID if the ID lies outside the range of an Prime Provisioning-managed VLAN pool. In this case, the operator must ensure the uniqueness of the ID in the Ethernet access domain. If an operator specifies a VLAN ID that is within the range of an Prime Provisioning-managed VLAN pool and the VLAN ID is already in use in the access domain, Prime Provisioning displays an error message indicating that the VLAN ID is in use.

Note on Access VLAN IDs

An access VLAN ID is of local significance to the EVC-capable ports. It should not be confused with the global VLANs. This can be visualized as a partitioning of the Ethernet access network beyond the EVC ports into several subEthernet access domains (one each for an EVC-capable port).

However, all the service interfaces on the Ethernet access nodes beyond the EVC ports will have this very same VLAN ID for a link. This ID must be manually specified by the operator when setting the link attributes during service request creation. The operator must ensure the uniqueness of the ID across the EVC-demarcated Ethernet access domain.

These VLAN IDs are not managed by Prime Provisioning by means of locally-significant VLAN pools. But once a VLAN ID is assigned for a link in the service request, Prime Provisioning makes the VLAN unavailable for subsequent service requests within the Ethernet access domain demarcated by the EVC. Likewise, if a manually-specified VLAN is already in use in the access domain delimited by the EVC, Prime Provisioning will display an error message indicating that the new VLAN ID being specified is already in use on the NPC. The operator will be prompted to specify a different VLAN ID, which will be provisioned on the L2 access nodes.

Step 7 Check the **AutoPick Bridge Group Name** check box to have Prime Provisioning autopick the group name for the service request during service request creation.

If this check box is unchecked, the operator will be prompted to specify a group name during service request creation. If the check box is checked, the group name will default to the customer name.

**Note**

This attribute is applicable only for supported IOS XR devices.

Step 8 Check the **AutoPick Bridge Domain Name** check box to have Prime Provisioning autopick the domain name for the service request during service request creation.

Usage notes:

- If this check box is unchecked, the operator will be prompted to specify a domain name during service request creation.
- If the check box is checked, the domain name will default to the following format:
 - For pseudowire and local connect core types: *ISC-Job-Job_ID*, where *Job_ID* is the service request job ID.
 - For VPLS core type: *ISC-VPN_Name-VPN_ID*, where *VPN_Name* is the name of the VPLS VPN being used, and *VPN_ID* is the VPN ID used in the service request.

**Note**

This attribute is applicable only for supported IOS XR devices.

- Step 9** Continue with the steps contained in the next section, [Setting the VLAN Matching Criteria Attributes](#), page 3-26.

Setting the VLAN Matching Criteria Attributes

Prior to the introduction of the EVC capability, service providers could either deploy service-multiplexed services (ERS/ERMS or EVPL/EVCS) or service-bundled services on a single port. Both could not be supported simultaneously due to the limitations in the infrastructure, which only allowed matching the outer-most VLAN tag.

One of the key benefits of EVC support in Prime Provisioning is to provide a flexible means to examine the VLAN tags (up to two levels) of the incoming frames and associate them to appropriate Ethernet Flow Points (EFPs). This allows service providers to deploy simultaneously both the service-multiplexed and service-bundled services on a single port.

To set the EVC VLAN matching criteria attributes, perform the following steps.

- Step 1** Check the **Both Tags** check box to enable service requests created with the policy to match both the inner and outer VLAN tags of the incoming frames.
- If you do not check this check box, service requests created with the policy will match only the outer VLAN tag of the incoming frames.
- Checking the Both Tags attribute causes the Inner VLAN Ranges attribute (covered in the next steps) to appear in the EVC Attribute window.
- Step 2** Check the **Inner VLAN Ranges** check box to enable the range of inner VLAN tags to be specified during service request creation.
- If the check box is unchecked, the range of inner VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.
- Step 3** Check the **Outer VLAN Ranges** check box to enable the range of outer VLAN tags to be specified during service request creation.
- If the check box is unchecked, the range of outer VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.
- Step 4** Check the **AutoPick Outer VLAN** check box to have Prime Provisioning autopick the outer VLAN ID from a previously created outer VLAN ID resource pool during service request creation.
- If this check box is unchecked, the operator will be prompted to specify an outer VLAN ID during service request creation.

**Note**

Use of the AutoPick Outer VLAN attribute requires that two elements have already been set up in Prime Provisioning. One is an Interface Access Domain, which is a logical element that groups the physical ports of an N-PE device. The other is an EVC Outer VLAN resource pool, which is used by the Interface Access Domain. For instructions on how to set up these elements, see the sections [Setting Up Resources, page 2-40](#), and [Resource Pools, page 2-44](#).

Usage notes:

- AutoPick Outer VLAN can be used for interfaces that support EVC functionality.
- AutoPick Outer VLAN consumes a VLAN ID on the interface that supports EVC.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 5

Continue with the steps contained in the next section, [Setting the VLAN Rewrite Criteria Attributes, page 3-27](#).

Setting the VLAN Rewrite Criteria Attributes

Together with VLAN matching criteria, VLAN rewrite makes the EVC infrastructure very powerful and flexible. The following VLAN rewrite options are supported:

- Pop one or two tags.
- Push one or two tags.
- Translation (1:1, 2:1, 1:2, 2:2).

Be aware of the following considerations when setting the VLAN rewrite criteria attributes:

- Only one kind of rewrite can be done on every CE-facing EVC link.
- All VLAN rewrites are done using the **symmetric** keyword on the ingress traffic (for example, **rewrite ingress tag pop 2 symmetric**).
- For any service instance, only one type of rewrite option (pop, push, or translate) is allowed per instance. For example, if pop out is enabled, push inner, push outer, translate inner, and translate outer are not available.

To set the EVC VLAN rewrite criteria attributes, perform the following steps.

Step 1

Check the **Pop Outer** check box to pop the outer VLAN ID tag of the incoming frames that fulfill the match criteria.

If this check box is unchecked, the outer tag of the incoming traffic is not popped.

Step 2

Check the **Pop Inner** check box to pop the inner VLAN ID tag of the incoming frames that fulfill the match-criteria.

If this check box is unchecked, the inner tag is not popped. Note that, if Pop Inner is checked, Pop Outer is automatically checked.

Step 3

Check the **Push Outer** check box to impose an outer VLAN ID tag onto the incoming frames that fulfill the match criteria.

If this check box is unchecked, no outer tag is imposed on the incoming frames.

Usage notes:

- If Push Outer is checked, all service requests created with the policy push a dot1q outer tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an outer tag with a value from 1 to 4096.
- This attribute is available regardless of the number of tags used in the match criteria. Whether the incoming traffic is double tagged or single tagged, if Push Outer is enabled, all corresponding service requests push an outer tag. All subsequent nodes consider only the outer-most two tags (if EVC-capable) or just one tag (not EVC-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Provisioning-managed VLAN ID pools.

Step 4 Check the **Push Inner** check box to impose an inner VLAN ID tag onto the incoming frames that fulfill the match criteria.

This operation pushes both an inner and an outer tag onto the incoming packet, not just an inner tag. If this check box is unchecked, no inner tag is imposed on the incoming frames.

Usage notes:

- If Push Inner is checked, all service requests created with the policy push a dot1q inner tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an inner tag with a value from 1 to 4096.
- If Push Inner is checked, Push Outer is automatically checked.
- This attribute is available regardless of the number of tags used in the match criteria. Regardless of whether the incoming traffic is double tagged or single tagged, if Push Inner is enabled, all corresponding service requests push an inner tag. All subsequent nodes consider only the outer-most two tags (if EVC-capable) or just one tag (not EVC-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Provisioning-managed VLAN ID pools.

Step 5 Check the **Translate Outer** check box to allow the operator to specify a target outer VLAN ID during service request creation.

The outer tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no outer tag translation is performed. See [Table 3-2](#).

Step 6 Check the **Translate Inner** check box to allow the operator to specify a target inner VLAN ID during service request creation.

The inner tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no inner tag translation is performed. See [Table 3-2](#).



Note

[Table 3-2](#) summarizes the realization of different VLAN translations available in the EVC infrastructure. The second and third columns (Match Outer Tag and Match Inner Tag) refer to policy settings. The last two columns (Translate Outer Tag and Translate Inner Tag) indicate the VLAN translation that occurs on the incoming frames.

Table 3-2 VLAN Translation Summary Table

Type	Match Outer Tag	Match Inner Tag	Translate Outer Tag	Translate Inner Tag	Push Outer Tag
1:1	True	N/A	Yes	No	N/A
1:2	True	N/A	N/A	N/A	Yes

Table 3-2 VLAN Translation Summary Table

Type	Match Outer Tag	Match Inner Tag	Translate Outer Tag	Translate Inner Tag	Push Outer Tag
2:1	True	True	Yes	No	N/A
2:2	True	True	Yes	Yes	N/A

Step 7 Click **Next**.

The Interface Attribute window appears.

Step 8 Continue with the steps contained in the next section, [Setting the Interface Attributes, page 3-29](#).

Setting the Interface Attributes

This step of creating the EVC Ethernet policy involves setting the interface attributes in the Interface Attribute window. The attributes you can configure in this window are grouped under the following categories:

- UNI Information
- VLAN
- Pseudowire
- ACL
- Security
- UNI Storm Control
- Protocol

In some cases, checking an attribute causes additional attributes to appear in the GUI. This is covered in the steps that follow.



Note

If the CE is directly connected to an N-PE, only speed, duplex, UNI shutdown, and other generic options are presented. In this case, port security, storm control, L2 protocol tunneling, and other advanced features are not supported due to the current platform limitations. If these features are needed for a service, the service provider must deploy Layer 2 Ethernet access nodes beyond the EVC to support these requirements.



Note

Attributes available in the Interface Attributes window dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE, LOCAL, or VPLS) in the Service Options window (see [Setting the Service Options, page 3-20](#)). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

To set the EVC interface attributes, perform the following steps.

Step 1 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 2 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 3 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable, in order to support modification on a per-service request basis.

Step 4 Enter a **Link Media** (optional) of None, auto-select, rj45, or sfp.

Step 5 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 6 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 7 Choose an **Encapsulation** type.

The choices are:

- **DOT1QTRUNK**—Configures the UNI as a trunk with 802.1q encapsulation. If the UNI belongs to a directly connected and EVC link, this setting signifies that the incoming frames are 802.1q encapsulated and that they match the VLAN ID configured for the link. This specific topology does not involve a trunk UNI as such.
- **DOT1QTUNNEL**—Configures the UNI as an 802.1q tunnel (also known as a dot1q tunnel or Q-in-Q) port.
- **ACCESS**—Configures the UNI as an access port.

Step 8 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation. Translates an incoming customer VLAN to another.
- **2:1**—2:1 VLAN translation. Converts both inner and outer VLANs to a single VLAN.
- **1:2**—1:2 VLAN translation. Pushes one more provider VLAN.
- **2:2**—2:2 VLAN translation. Translates both inner and outer VLANs to two other VLANs.



Note For more details on how VLAN translation is supported in EVC Ethernet services, see the coverage of the VLAN Translation attribute in [Managing an EVC Ethernet Service Request, page 3-35](#).

Step 9 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#) for additional information on pseudowire class support for IOS XR devices.
- If **Use PseudoWireClass** is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning.

- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 10 For **L2VPN Group Name** choose one of the following from the drop-down list:

- **ISC**
- **VPNSC**

Usage notes:

- This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- The L2VPN Group Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- L2VPN Group Name is only applicable for IOS XR devices.

Step 11 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

Usage notes:

- If no value is specified for the **E-Line Name** in either the policy or the service request based on the policy, Prime Provisioning autogenerates a default name as follows:

- For PSEUDOWIRE core connectivity type, the format is:

DeviceName--VC_ID

- For LOCAL core connectivity type, the format is:

DeviceName--0--VLAN_ID

If the default name is more than 32 characters, the device names are truncated.

- The E-Line Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- E-Line Name is only applicable for IOS XR devices.

Step 12 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default.

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 13 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Provisioning generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Provisioning generates forwarding commands under the service instance.

For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the policy workflow in the EVC Policy Editor - Service Options window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- Prime Provisioning supports a hybrid configuration for EVC service requests. In a hybrid configuration, the forwarding commands (such as xconnect) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- For examples of these cases, see configlet examples [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\)](#), page 3-212 and [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\)](#), page 3-213.
- N-PE Pseudo-wire on SVI is applicable for all connectivity types (PSEUDOWIRE, VPLS, and LOCAL), but a hybrid SVI configuration is possible only for pseudowire connectivity.
- When MPLS Core Connectivity Type is set as VPLS, the N-PE Pseudo-wire on SVI attribute is always enabled in the policy and service request.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. Only subinterfaces are supported on ASR 9000 devices; service instance is not supported. All the xconnect commands are configured on L2 subinterfaces.
- [Table 3-3](#) shows various use cases for hybrid configuration for EVC service requests.

Table 3-3 Use Cases for Hybrid Configuration for EVC Service Requests

Use Bridge Domain	EVC	N-PE Pseudowire on SVI	CLIs Generated
True	True	True	<ul style="list-style-type: none"> • xconnect under VLAN interface. • Service instance under main interface.
True	True	False	<ul style="list-style-type: none"> • xconnect under service instance. • Service instance under main interface.
False	True	N/A	<ul style="list-style-type: none"> • xconnect under service instance. • Service instance under main interface.
True	False	True	xconnect under VLAN interface.
True	False	False	xconnect under subinterface.
False	False	False	xconnect under subinterface.

Step 14 Check the **Use Existing ACL Name** check box if you want to assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 15 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note**

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 17 Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 18 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 19 Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

For each protocol that you choose, enter the shutdown threshold and drop threshold for that protocol:

- a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- b. **cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

- h. **stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 20 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In Cisco Prime Fulfillment 1.0, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500 to 1546.
- For the Cisco 7600 Ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500 to 9216. However, Prime Provisioning uses 9216 in both cases.
- For the Cisco 7600 SVI (interface VLAN), the MTU size is 1500 to 9216.

Step 21 If you would like to enable template association for this policy, click the **Next** button.

See the section [Enabling Template Association, page 3-34](#) for information about this feature.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 22 To save the EVC policy, click **Finish**.

To create a service request based on an EVC policy, see [Managing an EVC Ethernet Service Request, page 3-35](#).

Enabling Template Association

The Prime Provisioning template feature gives you a means to download free-format CLIs to a device. If you enable templates, you can create templates and data files to download commands that are not currently supported by Prime Provisioning.

Step 1 To enable template association for the policy, click the **Next** button in the Interface Attribute window (before clicking **Finish**).

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#).

- Step 2** When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.
- Step 3** To save the EVC policy, click **Finish**.
-

To create a service request based on an EVC policy, see [Managing an EVC Ethernet Service Request, page 3-35](#).

Managing an EVC Ethernet Service Request

This section provides information on how to provision an EVC Ethernet service request. It contains the following subsections:

- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Creating an EVC Service Request, page 3-36](#)
- [Setting the Service Request Details, page 3-36](#)
- [Modifying the EVC Service Request, page 3-54](#)
- [Using Templates and Data Files with an EVC Ethernet Service Request, page 3-55](#)
- [Saving the EVC Service Request, page 3-55](#)

Introducing EVC Service Requests

An EVC Ethernet service request allows you to configure interfaces on an N-PE to support the EVC features described in [Creating an EVC Ethernet Policy, page 3-19](#). To create an EVC service request, an EVC service policy must already be defined. Based on the predefined EVC policy, an operator creates an EVC service request and deploys the service. One or more templates can also be associated to the N-PE as part of the service request.

Creating an EVC Ethernet service request involves the following steps:

- Choose an existing EVC Ethernet policy.
- Choose a VPN.

**Note**

When working with VPN objects in the context of EVC Ethernet policies and service requests, only the VPN name and customer attributes are relevant. Other VPN attributes related to MPLS and VPLS are ignored.

- Specify a bridge domain configuration (if applicable).
- Specify a service request description.
- Specify automatic or manual allocation of the VC ID or VPLS VPN ID.
- Add direct connect links (if applicable).
- Add links with L2 access nodes (if applicable).
- Choose the N-PE and UNI interface for links.
- For links with L2 access nodes, choose a Named Physical Circuit (NPC) if more than one NPC exists from the N-PE or the UNI interface.

- Edit the link attributes.
- Modify the service request.
- Save the service request.

For sample configlets for EVC Ethernet scenarios, see [Sample Configlets, page 3-177](#).

Creating an EVC Service Request

To create an EVC Ethernet service request, perform the following steps.

-
- Step 1** Choose **Operate > Service Request Manager**.
The Service Request Manager window appears.
- Step 2** Click **Create**.
The Service Request Editor window appears.
- Step 3** From the policy picker, choose an EVC policy from the policies previously created (see [Creating an EVC Ethernet Policy, page 3-19](#)).
The EVS Service Request editor window appears.
The new service request inherits all the properties of the chosen EVC policy, such as all the editable and non-editable features and pre-set parameters.
- Step 4** Continue with the steps contained in the next section, [Setting the Service Request Details, page 3-36](#).
-

Setting the Service Request Details

After you have selected the EVC Ethernet policy to be used as the basis of the service request, the EVC Service Request Editor window appears. It is divided into three main sections:

- Link Page
- Direct Connect Links (no NPCs)
- Links with L2 Access Nodes (involves NPCs)

This window enables you to specify options for the service request, as well as configure directly connected links and links with L2 access nodes. The options displayed in first section of the window change, depending on the MPLS Core Connectivity Type that was specified in the policy (pseudowire, VPLS, or local). For clarity, each of these scenarios is presented in a separate section below, to highlight the different window configurations and behavior of the displayed options.

Proceed to the appropriate section, as determined by the MPLS Core Connectivity Type for the policy:

- [Pseudowire Core Connectivity, page 3-37](#)
- [VPLS Core Connectivity, page 3-38](#)
- [Local Core Connectivity, page 3-40](#)

Instructions for setting up direct connect links and links with L2 access nodes are presented in later sections.

Pseudowire Core Connectivity

This section covers the case in which the MPLS Core Connectivity Type for the EVC Ethernet policy is PSEUDOWIRE.

To set the attributes in the first section of the Link Page window, perform the following steps.



Note

The **Job ID** and **SR ID** fields are read-only. When the service request is being created for the first time, the fields display a value of NEW. When an existing service request is being modified, the values of the fields indicate the respective IDs that the Prime Provisioning database holds within the editing flow of the service request.



Note

The **Policy** field is read-only. It displays the name of the policy on which the service request is based. Clicking on the read-only policy name displays a list of all the attribute values set within the policy.

Step 1 Click **Select VPN** to choose a VPN for use with this service request.

The Select VPN window appears with the VPNs defined in the system.



Note

The same VPN can be used by service requests with LOCAL and PSEUDOWIRE core types. If a VPN for a service request is used with VPLS core type, the same VPN cannot be used for service requests with LOCAL or PSEUDOWIRE core type.

Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**.

The EVC Service Request Editor window appears with the VPN name displayed.

Step 4 Check the **AutoPick VC ID** check box if you want Prime Provisioning to choose a VC ID.

If you do not check this check box, you will be prompted to provide the ID in the VC ID field, as covered in the next step.

When AutoPick VC ID is checked, Prime Provisioning allocates a VC ID for pseudowires from the Prime Provisioning-managed VC ID resource pool. In this case, the text field for the VC ID option is non-editable.

Step 5 If AutoPick VC ID was unchecked, enter a VC ID in the **VC ID** field.

Usage notes:

- The VC ID value must be an integer value corresponding to a VC ID.
- When a VC ID is manually allocated, Prime Provisioning verifies the VC ID to see if it lies within Prime Provisioning's VC ID pool. If the VC ID is in the pool but not allocated, the VC ID is allocated to the service request. If the VC ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VC ID. If the VC ID lies outside of the Prime Provisioning VC ID pool, Prime Provisioning does not perform any verification about whether or not the VC ID allocated. The operator must ensure the VC ID is available.
- The VC ID can be entered only while creating a service. If you are editing the service request, the VC ID field is not editable.

Step 6 Check the **Enable PseudoWire Redundancy** check box to enable pseudowire redundancy (alternative termination device) under certain conditions.

See [Appendix C, “Terminating an Access Ring on Two N-PEs”](#) and, specifically, the section [Using N-PE Redundancy in FlexUNI/EVC Service Requests, page C-3](#), for notes on how this option can be used.

- Step 7** If the AutoPick VC ID attribute was unchecked, enter a VC ID for the backup pseudowire in the **Backup PW VC ID** field.

See the usage notes for the AutoPick VC ID attribute in Step 7, above. The backup VC ID behaves the same as the VC ID of the primary pseudowire.

- Step 8** Check the **Configure Bridge Domain** check box to determine bridge domain characteristics.

The behavior of the Configure Bridge Domain option works in tandem with the choice you selected in the MPLS Core Connectivity Type option in the EVC policy, which in this case is pseudowire core connectivity. There are two cases:

- With EVC:
 - If **Configure With Bridge Domain** is checked, the policy will configure pseudowires under SVIs associated to the bridge domain.
 - If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under the service instance. This will conserve the global VLAN.
- Without EVC:
 - If **Configure With Bridge Domain** is checked, the policy will configure pseudowires under SVIs.
 - If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under subinterfaces.

Pseudowires can be configured either directly under service instance of the corresponding EVC-capable interface or under SVIs associated to the bridge domain.

- Step 9** Check the **Use Split Horizon** check box to enable split horizon with bridge domain.

Usage notes:

- The Use Split Horizon attribute is disabled by default.
- The Use Split Horizon attribute can be used only when the Configure Bridge Domain check box is checked (enabled).
- When Use Split Horizon is enabled, the **bridge domain** command in the CLI will be generated with split horizon. When it is disabled, the **bridge domain** command will be generated without split horizon.

- Step 10** Click the “Click here” link of the **Description** attribute to enter a description label for the service request.

This is useful for searching the Prime Provisioning database for the particular service request.

A dialogue appears in which you can enter a description.

- Step 11** To set up direct connect links, see the section [Setting Direct Connect Links, page 3-42](#).

- Step 12** To set up links with L2 access nodes, see the section [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

VPLS Core Connectivity

This section covers the case in which the MPLS Core Connectivity Type for the EVC Ethernet policy is VPLS.

To set the attributes in the first section of the Link Page window, perform the following steps.

-
- Step 1** The **Job ID** and **SR ID** fields are read-only.
- When the service request is being created for the first time, the fields display a value of NEW. When an existing service request is being modified, the values of the fields indicate the respective IDs that the Prime Provisioning database holds within the editing flow of the service request.
- Step 2** The **Policy** field is read-only. It displays the name of the policy on which the service request is based.
- Step 3** Click **Select VPN** to choose a VPN for use with this service request.
- The Select VPN window appears with the VPNs defined in the system.



Note The same VPN can be used by service requests with LOCAL and PSEUDOWIRE core types. If a VPN for a service request is used with VPLS core type, the same VPN cannot be used for service requests with LOCAL or PSEUDOWIRE core type.



Note If the same VPN is used among multiple service requests, all having VPLS core type, then all these service requests participate in the same VPLS service.

- Step 4** Choose a **VPN Name** in the Select column.
- Step 5** Click **Select**.
- The EVC Service Request Editor window appears with the VPN name displayed.
- Step 6** Check the **AutoPick VPLS VPN ID** check box if you want Prime Provisioning to choose a VPLS VPN ID.
- If you do not check this check box, you will be prompted to provide the VPN ID in the VPLS VPN ID field, as covered in the next step.
- When AutoPick VPLS VPN ID is checked, Prime Provisioning allocates a VPLS VPN ID from the Prime Provisioning-managed VC ID resource pool. In this case, the text field for the VPLS VPN ID option is non-editable.
 - If AutoPick VPLS VPN ID is checked and a service request already exists that refers to same VPN object, the VPLS VPN ID of the existing service request is allocated to the new service request.
- Step 7** If AutoPick VPLS VPN ID was unchecked, enter a VPLS VPN ID in the **VPLS VPN ID** field.
- Usage notes:
- The VPLS VPN ID value must be an integer value corresponding to a VPN ID.
 - When a VPLS VPN ID is manually allocated, Prime Provisioning verifies the VPLS VPN ID to see if it lies within Prime Provisioning's VC ID pool. If the VPLS VPN ID is in the pool but not allocated, the VPLS VPN ID is allocated to the service request. If the VPLS VPN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VPLS VPN ID. If the VPLS VPN ID lies outside of the VC ID pool, Prime Provisioning does not perform any verification about whether the VPLS VPN ID allocated. The operator must ensure the VPLS VPN ID is available.
 - The VPLS VPN ID can be entered only while creating a service. If you are editing the service request, the VPLS VPN ID field is not editable.
- Step 8** Check the **AutoPick VFI Name** check box if you want Prime Provisioning to choose a virtual forwarding instance (VFI) name.

If you do not check this check box, you can provide the VFI name in the VFI Name field, as covered in the next step.

Usage notes:

- When AutoPick VFI name is checked, Prime Provisioning generates a VFI name in the following format:
VPN name-VC ID
- This attribute is useful when importing an existing service into Prime Provisioning and mapping it to a service request which has been created for this purpose. Manually specifying the VFI name in the service request allows the VFI name to be matched to that of existing service.

Step 9 If AutoPick VFI Name was unchecked, enter a VFI name in the **VFI Name** field.

Step 10 Choose the **Discovery Mode** type for VPLS autodiscovery.

The choices are:

- **Manual**—Does not provision VPLS autodiscovery on VPLS PE devices configured by the service request. In this case, when a new PE is device is added or removed from the VPLS domain, manual configuration of each neighbor in the VPLS domain is required.
- **Auto Discovery**—Provisions VPLS autodiscovery on VPLS PE devices configured by the service request. With VPLS autodiscovery enabled, neighbor devices automatically detect when PEs are added or removed from the VPLS domain.

For details on how this feature is supported in Prime Provisioning, device preconfiguration requirements, and limitations, see [Provisioning VPLS Autodiscovery on Devices using EVC Service Requests, page 3-168](#).

Step 11 Check the **Static VPLS** check box to enable static allocation of LSP/pseudowire labels.

Step 12 The **Configure Bridge Domain** check box is checked by default and cannot be changed.

Usage notes:

- For VPLS, all configurations are under the SVI.
- When the EVC feature is used, all configurations are under the SVI and also associated to a bridge domain.

Step 13 Click the “Click here” link of the **Description** attribute to enter a description label for the service request.

A dialogue appears in which you can enter a description.

Step 14 To set up direct connect links, see the section [Setting Direct Connect Links, page 3-42](#).

Step 15 To set up links with L2 access nodes, see the section [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

Local Core Connectivity

This section covers the case in which the MPLS Core Connectivity Type for the EVC Ethernet policy is LOCAL.

To set the attributes in the first section of the Link Page window, perform the following steps.

Step 1 The **Job ID** and **SR ID** fields are read-only.

When the service request is being created for the first time, the fields display a value of NEW. When an existing service request is being modified, the values of the fields indicate the respective IDs that the Prime Provisioning database holds within the editing flow of the service request.

Step 2 The **Policy** field is read-only.

It displays the name of the policy on which the service request is based.

Step 3 Click **Select VPN** to choose a VPN for use with this service request.

The Select VPN window appears with the VPNs defined in the system.



Note The same VPN can be used by service requests with LOCAL and PSEUDOWIRE core types. If a VPN for a service request is used with VPLS core type, the same VPN cannot be used for service requests with LOCAL or PSEUDOWIRE core type.

Step 4 Choose a **VPN Name** in the Select column.

Step 5 Click **Select**.

The EVC Service Request Editor window appears with the VPN name displayed.

Step 6 Check the **Configure Bridge Domain** check box to determine bridge domain characteristics.

Usage notes:

- If Configure Bridge Domain is checked, all links will have the same bridge domain ID allocated from the VLAN pool on the N-PE. All non-EVC links will have the Service Provider VLAN as the bridge domain ID. On the other hand, if no EVC links are added, the Service Provider VLAN will be allocated first and this will be used as the bridge domain ID when EVC links are added.
- If Configure Bridge Domain is unchecked, a maximum of two links that terminate on the same N-PE can be added. (This uses the **connect** command available in the EVC infrastructure.)



Note See the following comments for details on how Prime Provisioning autogenerates the connect name.

Because the device only accepts a maximum of 15 characters for the connect name, the connect name is generated using the following format:

CustomerNameTruncatedToMaxPossibleCharacters_ServiceRequestJobID

For example, if the customer name is NorthAmericanCustomer and the service request job ID is 56345, the autogenerated connect name would be NorthAmer_56345.

The CLI generated would be:

```
connect NorthAmer_56345 GigabitEthernet7/0/5 11 GigabitEthernet7/0/4 18
```

In this case, 11 and 18 are service instance IDs.

- If the policy setting for Configure Bridge Domain is non-editable, the option in the service request will be read-only.

Step 7 Check the **Use Split Horizon** check box to enable split horizon with bridge domain.

Usage notes:

- The Use Split Horizon attribute is disabled by default.
- The Use Split Horizon attribute can be used only when the Configure Bridge Domain check box is checked (enabled).

- When Use Split Horizon is enabled, the **bridge domain** command in the CLI will be generated with split horizon. When it is disabled, the **bridge domain** command will be generated without split horizon.
- Step 8** Click the “Click here” link of the **Description** attribute to enter a description label for the service request.
- A dialogue appears in which you can enter a description.
- Step 9** To set up direct connect links, see the section [Setting Direct Connect Links, page 3-42](#).
- Step 10** To set up links with L2 access nodes, see the section [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).
-

Setting up Links to the N-PE

The lower two sections of the EVC Service Request Editor window allow you to set up links to the N-PE. For direct connect links, the CE is directly connected to the N-PE, with no intermediate L2 access nodes. For links with L2 access nodes, there are intermediate devices present between the CE and NPE requiring NPCs to be created in Prime Provisioning.

The Direct Connect Links section of the window is where you set up links that directly connect to the N-PE. No NPC are involved. The Links with L2 Access Nodes section is where you set up links with L2 (Ethernet) access nodes. NPCs are involved.

See the appropriate section, depending on which type of link you are setting up:

- [Setting Direct Connect Links, page 3-42](#)
- [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#)
- [Setting VPLS Neighbor Links \(VPLS only\), page 3-54](#)



Note

Many of the steps for setting up the two link types are the same. The basic workflow for setting up links, as well as the attributes to be set, are presented in the section [Setting Direct Connect Links, page 3-42](#). Even if you are setting up links with L2 access nodes, it will be helpful to refer to the information presented in that section, as the section on L2 access nodes only covers the unique steps for such links.

Setting Direct Connect Links

To set up the direct connect links, perform the following steps. Most of these steps apply to links with L2 access nodes also.

-
- Step 1** Click **Add** to add a link.
- A new numbered row for the link attributes appears.
- Step 2** Click **Select NPE** in N-PE column.
- The Select PE Device window appears. This window displays the list of currently defined PEs.
- The **Show PEs with** drop-down list shows PEs by Provider, PE Region Name, or by Device Name.
 - The **Find** button allows a search for a specific PE or a refresh of the window.
 - The **Rows per page** drop-down list allows the user to configure the number of entries displayed on the screen at one time.

Step 3 In the **Select** column, choose the PE device name for the link.

Step 4 Click **Select**.

The EVC Service Request Editor window reappears displaying the name of the selected PE in the N-PE column.

Step 5 Choose the UNI interface from the interface picker in the UNI column.



Note

Prime Provisioning only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Detail** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name, job ID, service request ID, service request type, translation type, and VLAN ID information.



Note

When the UNI is configured on an N-PE device running IOS XR, the Standard UNI Port attribute is not supported. All the CLIs related to Standard UNI Port and UNI Port Security are ignored in this case.

Step 6 Check the **EVC** check box to mark the link for configuring service instance for the links.



Note

The EVC check box is mentioned at this stage because the setting of the check box alters the behavior of the link editing function available in the Link Attributes column. This is covered in the next steps.



Note

The EVC check box is unchecked by default. The default value for the check box can be changed by setting the value of the DCPL property `Pr ovisioning\ProvDrv\CheckFlexUniCheckBox`.

Editing the Link Attributes

The next steps document the use of the **Edit** link in the Link Attributes column. (In the case where the link attributes have already been set, this link changes from **Edit** to **Change**.) The link editing workflow changes depending on the status of the EVC check box for the link. If the EVC check box is checked, the editing workflow involves setting attributes in two windows, for two sets of link attributes:

- The EVC Details
- Standard UNI Details

If the EVC check box for the link is not checked, only the Standard UNI Details window is presented.

In the steps that follow, both scenarios covered.

Step 7 Click **Edit** in the Link Attributes column to specify the UNI attributes.

EVC Details Window

If the EVC check box is checked, the EVC Details window appears.

All of the fields in the EVC Details screen are enabled based on the policy settings. For example, if Both Tags is selected in the policy and is editable, then the Match Inner and Outer Tags check box will be selected and editable in this window. The behavior is similar for the other attributes in the EVC Details window

Step 8 Check the **AutoPick Service Instance ID** check box to specify that the service instance ID will be autogenerated and allocated to the link during service request creation.

If the check box is unchecked, you must specify the service instance ID (see the next step).

Usage notes:

- The service instance ID represents an Ethernet Flow Point (EFP) on an interface in the EVC infrastructure. The service instance ID is locally significant to the interface. This ID has to be unique only at the interface level. The ID must be a value from 1 to 8000.
- There are no resource pools available in Prime Provisioning from which to allocate the service instance IDs.
- In the case of a manually provided service instance ID, it is the responsibility of the operator to maintain the uniqueness of the ID at the interface level.
- This attribute is not displayed for IOS XR devices.

Step 9 If the AutoPick Service Instance ID check box is not checked, enter an appropriate value for the service instance ID in the **Service Instance ID** field.

This attribute is not displayed for IOS XR devices.

Step 10 Check the **AutoPick Service Instance Name** check box to specify that the service instance name will be autogenerated.

If the check box is unchecked, you can specify the service instance name (see the next step).

Usage notes:

- If the check box is checked, the Service Instance Name text field is disabled.
- The service instance name is autogenerated in the following pattern:
CustomerName_ServiceRequestJobID.
- For example configlets, see [EVC \(AutoPick Service Instance Name\)](#), page 3-214, [EVC \(User-Provided Service Instance Name, Pseudowire Core Connectivity\)](#), page 3-216, and [EVC \(User-Provided Service Instance Name, Local Core Connectivity\)](#), page 3-217.
- This attribute is not displayed for IOS XR devices.

Step 11 If the AutoPick Service Instance Name check box is not checked, enter an appropriate value for the service instance ID in the **Service Instance Name** field.

Usage notes:

- The text string representing the service instance name must be 40 characters or less and contain no spaces. Other special characters are allowed.
- If AutoPick Service Instance Name is unchecked and no service instance name is entered in the text field, then Prime Provisioning does not generate the global **ethernet evc evcname** command in the device configuration generated by the service request.

Step 12 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID for the service request during service request creation.

If this check box is unchecked, the you must specify a bridge domain VLAN ID (see the next step).

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 13 If the AutoPick Bridge Domain/VLAN ID check box is unchecked, enter an appropriate value in the **Bridge Domain/VLAN ID** field.

**Note**

This configuration applies in conjunction with the Configure Bridge Domain option in the EVC Service Request Editor window. If the option is not enabled in that window, then AutoPick Bridge Domain/VLAN ID check box is redundant and not required.

When a VLAN ID is manually allocated, Prime Provisioning verifies the VLAN ID to see if it lies within Prime Provisioning's VLAN ID pool. If the VLAN ID is in the pool but not allocated, the VLAN ID is allocated to the service request. If the VLAN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VLAN ID. If the VLAN ID lies outside of the Prime Provisioning VLAN ID pool, Prime Provisioning does not perform any verification about whether the VLAN ID allocated. The operator must ensure the VLAN ID is available.

- Step 14** Check the **AutoPick Bridge Domain/VLAN ID Secondary N-PE** check box to have Prime Provisioning autopick the bridge domain VLAN ID for the secondary N-PE of a dual-homed ring during service request creation.

If this check box is unchecked, the you must specify a secondary bridge domain VLAN ID for the secondary N-PE (see the next step).

Usage notes:

- This attribute is only applicable in the case of a dual-homed ring (a ring that terminates on two different N-PEs). Prime Provisioning supports having a separate bridge domain VLAN ID for the secondary N-PE.
- In a dual-homed ring, if the two N-PEs are in different access domains, Prime Provisioning allocates the bridge domain VLAN IDs from both primary and secondary N-PE access domains. When both are in the same Access Domain, Prime Provisioning allocates a common VLAN ID from the Access Domain to which these belong.
- AutoPick Bridge Domain/VLAN ID Secondary N-PE consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.
- This attribute is not displayed for IOS XR devices.

- Step 15** If the AutoPick Bridge Domain/VLAN ID Secondary N-PE check box is unchecked, enter an appropriate value in the **Bridge Domain/VLAN ID Secondary N-PE** field.

- Step 16** Set the service instance details.
Choose an encapsulation type from the **Match** drop-down list as shown in the figure below.
The choices are:

- **DOT1Q**
- **Default**

Selecting **Default** as the match criteria disables the Outer VLAN ID and Outer VLAN Ranges fields on the page. If Default is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

- Step 17** Check the **Match Inner and Outer Tags** check box to enable service requests created with the policy to match both the inner and outer VLAN tags of the incoming frames.

If you do not check this check box, service requests created with the policy will match only the outer VLAN tag of the incoming frames.

Checking the Match Inner and Outer Tags attribute causes the Inner VLAN ID and Outer VLAN ID fields (covered in the next steps) to appear.

- Step 18** If the Match Inner and Outer Tags check box is checked, enter the inner and outer VLAN tags in the **Inner VLAN ID** and **Outer VLAN ID** fields.

Usage notes:

- You can specify single values, single ranges, multiples values, multiple ranges, or combinations of these. Examples:
 - 10
 - 10, 15,17
 - 10-15
 - 10-15,17-20
 - 10,20-25
- If the Inner VLAN Ranges attribute is set to true in the policy, the Inner VLAN ID field can take a range of inner VLAN tags.
- If the Outer VLAN Ranges attribute is set to true in the policy, the Outer VLAN ID field can take a range of Outer VLAN tags.

Step 19 If the Match Inner and Outer Tags check box is unchecked, enter the outer VLAN tag in the **Outer VLAN ID** field.



Note

The VLAN specified in Outer VLAN ID will be provisioned on the rest of the L2 access nodes (if the link has any), including the customer-facing UNI.



Note

You may also have Prime Provisioning autopick the outer VLAN ID as covered in the next step.

Step 20 Check the **AutoPick Outer VLAN** check box to have Prime Provisioning autopick the outer VLAN ID from a previously created outer VLAN ID resource pool.

If this check box is unchecked, the operator will be prompted to specify an outer VLAN ID.



Note

Use of the AutoPick Outer VLAN attribute requires that two elements have already been set up in Prime Provisioning. One is an Interface Access Domain, which is a logical element that groups the physical ports of an N-PE device. The other is an EVC Outer VLAN resource pool, which is used by the Interface Access Domain. For instructions on how to set up these elements, see the sections [Setting Up Resources, page 2-40](#), and [Resource Pools, page 2-44](#).

Usage notes:

- AutoPick Outer VLAN can be used for interfaces that support EVC functionality
- AutoPick Outer VLAN consumes a VLAN ID on the interface that supports EVC.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 21 In the VLAN Rewrite section of the window, choose a **Rewrite Type** from the drop-down list.

The choices are:

- **Pop**
- **Push**
- **Translate**

The subsequent attributes in the GUI change depending on the choice of Rewrite Type, as covered in the next steps.

Step 22 If Pop is the Rewrite Type, two check boxes appear:

- a. Check the **Pop Outer Tag** check box to pop the outer VLAN ID tag of the incoming frames that fulfill the match criteria. If this check box is unchecked, the outer tag of the incoming traffic will not be popped.
- b. Check the **Pop Inner Tag** check box to pop the inner VLAN ID tag of the incoming frames that fulfill the match-criteria. If this check box is unchecked, the inner tag will not be changed.

Note that if Pop Inner Tag is checked, Pop Outer Tag is automatically checked.

Step 23 If Push is the Rewrite Type, two text boxes appear:

- a. In the text box **Outer VLAN ID**, enter an outer VLAN ID tag that will be imposed on the incoming frames that fulfill the match criteria. All service requests created with this setting push a dot1q outer tag on the incoming frames matching the match criteria. If a value is not provided, the push operation is ignored and not configured on the device.
- b. In the text box **Inner VLAN ID**, enter an inner VLAN ID tag that will be imposed on the incoming frames that fulfill the match criteria. All service requests created with this setting push a dot1q inner tag on the incoming frames matching the match criteria. The Inner VLAN tag cannot be pushed without an Outer VLAN tag. That is, when pushing an Inner VLAN tag, the Outer VLAN tag also must be defined.

Step 24 If Translate is the Rewrite Type, a **Translation Type** drop-down list appears.

The choices available in this list vary depending on the setting of the Match Inner and Outer Tags attribute (set in a previous step).

- a. If the Match Inner and Outer Tags check box is checked (true), choose a translation type of **1:1**, **1:2**, **2:1**, or **2:2** from the Translation Type drop-down list.
 - If you choose 1:1 or 2:1, enter a value in the **Outer VLAN ID** text box that appears. The outer tag of all the incoming frames that fulfill the match criteria will be translated to this ID.
 - If you choose 1:2 or 2:2, enter values in the **Outer VLAN ID** and **Inner VLAN ID** text boxes that appear. The outer and inner tags of all the incoming frames that fulfill the match criteria will be translated to these IDs.
- b. If the Match Inner and Outer Tags check box is unchecked (false), choose a translation type of **1:1** or **1:2** from the Translation Type drop-down list.
 - If you choose 1:1, enter a value in the **Outer VLAN ID** text box that appears. The outer tag of all the incoming frames that fulfill the match criteria will be translated to this ID.
 - If you choose 1:2, enter values in the **Outer VLAN ID** and **Inner VLAN ID** text boxes that appear. The outer and inner tags of all the incoming frames that fulfill the match criteria will be translated to these IDs.

Step 25 Clicked **Next** to save the settings in the EVC Details window.

The Standard UNI Details window appears.

Step 26 Continue with setting the standard UNI link attributes in the next steps.

Editing the Standard UNI Attributes

The following steps cover setting the attributes in the Standard UNI Details window. In the case of a link which is not set as an EVC link (by not checking the EVC check box in the EVC Service Request Editor window), editing the link attributes begins with this window.

**Note**

The attributes that appear in the Standard UNI Details window are dynamically configured by Prime Provisioning. Some of the attributes covered in the steps below might not appear in the window, depending on the policy and service request settings or the link type. For example, if the MPLS core connectivity type of the EVC policy is VPLS or local, the pseudowire-related attributes will not appear. Also, setting the link as EVC or non-EVC will change the attributes that appear in the window. In addition, attributes are filtered based on device type (IOS or IOS XR). These and other cases are noted in the steps, for reference.

Step 27 The **N-PE/U-PE Information** and **Interface Name** fields display the PE device and interface name selected in previous steps.

These fields are read-only.

Step 28 Choose an **Encapsulation** type from the drop-down list.

The choices are:

- **DOT1QTRUNK**—Configures the UNI as a trunk with 802.1q encapsulation. If the UNI belongs to a directly connected and EVC link, this setting signifies that the incoming frames are 802.1q encapsulated and that they match the VLAN ID configured for the link. This specific topology does not involve a trunk UNI as such.
- **DOT1QTUNNEL**—Configures the UNI as an 802.1q tunnel (also known as a dot1q tunnel or Q-in-Q) port.
- **ACCESS**—Configures the UNI as an access port.

This attribute allows you to deploy different types of UNI encapsulation on different links of a service.

Usage notes:

- When a U-PE running with IOS is added in the same circuit terminating on an ASR 9000 (functioning in an N-PE role), the all three encapsulation types values will be visible in the drop-down list of the Encapsulation attribute.
- DOT1QTUNNEL is not directly supported for ASR 9000 devices.
- In the case of direct connect links for which EVC is enabled (by checking the EVC check box in the EVC Service Request Editor window), the choices for the Encapsulation type are DOT1Q and DEFAULT.

Step 29 In the **PE/UNI Interface Description** field, enter a description for the interface, if desired.

Step 30 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation (for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time).

Step 31 Specify the type of **VLAN Translation** for the service request by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.
- **1:2**—1:2 VLAN translation.
- **2:2**—2:2 VLAN translation.

Usage notes:

- The VLAN Translation attribute does not appear for direct connect links if the EVC check box is enabled. It does appear for the following combinations:
 - Direct connect links with EVC check box disabled.
 - L2 access nodes with EVC check box enabled or disabled.
- Choosing a selection other than No causes other fields to appear in the GUI, which you can set based on your configuration:
 - **CE VLAN**—Provide a value between 1 and 4096.
 - **Auto Pick**—Check this check box to have Prime Provisioning autopick the outer VLAN from the VLAN resource pool.
 - **Outer VLAN**—If Auto Pick is unchecked, provide a value between 1 and 4096.
 - **Select where 2:1 or 2:2 translation takes place**—Specify the device where the 2:1 or 2:2 VLAN translation will take place. If you choose Auto, the VLAN translation takes place at the device closest to the UNI port.
- VLAN translation, and all standard UNI and port security attributes are applicable for links with L2 access. If the UNI is on an N-PE, these attributes will not appear.
- When the VLAN translation takes place on a U-PE or PE-AGG device, the VLAN translation command is configured on the NNI interface of the selected device. When the VLAN translation takes place on an NP-E, the VLAN translation command is configured on the UNI interface of the device.
- When there are two NNI interfaces in a ring-based environment, VLAN translation is applied for both of these NNI interfaces.
- 1:1 and 2:1 VLAN translations are supported with the same syntax as for non-EVC (switchport-based N-PE syntax) terminating attachment circuits.

Step 32 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Provisioning generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Provisioning generates forwarding commands under the service instance.

For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the service request workflow in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE pseudo-wire on SVI is enabled.
- Prime Provisioning supports a hybrid configuration for EVC service requests. In a hybrid configuration, the forwarding commands (such as xconnect) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- N-PE Pseudo-wire on SVI is applicable for all connectivity types (PSEUDOWIRE, VPLS, and LOCAL), but a hybrid SVI configuration is possible only for pseudowire connectivity.

- When MPLS Core Connectivity Type is set as VPLS, the N-PE Pseudo-wire on SVI attribute is always enabled in the policy and service request.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- For examples of these cases, see configlet examples [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\)](#), page 3-212 and [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\)](#), page 3-213.
- For additional information on the N-PE Pseudo-wire on SVI attribute, see the corresponding coverage in the EVC policy section in the section [Setting the Interface Attributes](#), page 3-29.
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. All the xconnect commands are configured on L2 subinterfaces.

Step 33 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

Usage notes:

- Checking the PW Tunnel Selection check box activates the Interface Tunnel attribute field (see the next step).
- This attribute only appears if the MPLS core connectivity type is set as pseudowire in the EVC policy.
- The PW Tunnel Selection attribute is not supported for IOS XR devices.

Step 34 If you checked the PW Tunnel Selection check box, enter the TE tunnel ID in the **Interface Tunnel** text field.

Usage notes:

- Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. During service request creation, Prime Provisioning does not check the validity of the tunnel ID number. That is, Prime Provisioning does not verify the existence of the tunnel.
- The Interface Tunnel attribute is not supported for IOS XR devices.

Step 35 Check the **AutoPick Bridge Group Name** check box to have Prime Provisioning autopick the bridge group name during service request creation.

If this check box is unchecked, you are prompted to specify a bridge group name during service request creation (see the next step).

Usage notes:

- This attribute only displays for IOS XR devices.
- If the AutoPick Bridge Group Name check box is unchecked, enter an bridge group name in the **Bridge Group Name** text field.
- The AutoPick Bridge Group Name and Bridge Group Name attributes only appear if Configure Bridge Domain was enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 36 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID during service request creation.

If this check box is unchecked, you are prompted to specify a VLAN ID during service request creation (see the next step).

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.
- The AutoPick Bridge Domain/VLAN ID attribute appears for both Cisco 7600 and ASR 9000 devices. It will be displayed only for non-EVC links.

Step 37 If the AutoPick Bridge Domain/VLAN ID check box is unchecked, enter an ID number in the **Bridge Domain/VLAN ID** text field.

Usage notes:

- If AutoPick Bridge Domain/VLAN ID is checked, this field is non-editable.
- When a VLAN ID is manually allocated, Prime Provisioning verifies the VLAN ID to see if it lies within Prime Provisioning's VLAN ID pool. If the VLAN ID is in the pool but not allocated, the VLAN ID is allocated to the service request. If the VLAN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VLAN ID. If the VLAN ID lies outside of the Prime Provisioning VLAN ID pool, Prime Provisioning does not perform any verification about whether the VLAN ID allocated. The operator must ensure the VLAN ID is available.
- The Bridge Domain/VLAN ID text field appears for both Cisco 7600 and ASR 9000 devices. It will be displayed only for non-EVC links.

Step 38 Check the **AutoPick Bridge Domain Name** check box to have Prime Provisioning autopick the bridge domain name during service request creation.

If this check box is unchecked, you are prompted to specify a bridge domain name during service request creation (see the next step).

Usage notes:

- The AutoPick Bridge Domain Name attribute appears only for Cisco ASR 9000 devices.
- The AutoPick Bridge Domain Name attribute only appears if Configure Bridge Domain was enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 39 If the AutoPick Bridge Domain Name check box is unchecked, enter a bridge domain name in the **Bridge Domain Name** text field.

Usage notes:

- Bridge Domain Name field appears only for Cisco ASR 9000 devices.
- The Bridge Domain Name attribute only appears if Configure Bridge Domain was enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 40 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#) for additional information on pseudowire class support for IOS XR devices.
- If Use PseudoWireClass is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning.
- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

- The Use PseudoWireClass and PseudoWireClass attributes only appear if Configure Bridge Domain was not enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 41 For **L2VPN Group Name** choose one of the following from the drop-down list:

- **ISC**
- **VPNSC**

Usage notes:

- This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- The L2VPN Group Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- L2VPN Group Name is only applicable for IOS XR devices.
- The L2VPN Group Name attribute only appears if Configure Bridge Domain was not enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 42 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

Usage notes:

- If no value is specified for the **E-Line Name**, Prime Provisioning autogenerates a default name as follows:
 - For PSEUDOWIRE core connectivity type, the format is:
DeviceName--VC_ID
 - For LOCAL core connectivity type, the format is:
DeviceName--VLAN_ID

If the default name is more than 32 characters, the device names are truncated.

- The E-Line Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- E-Line Name is only applicable for IOS XR devices.
- The E-Line Name attribute only appears if Configure Bridge Domain was not enabled in the EVC Service Request Editor window earlier in the service request workflow.

Step 43 Click **OK** to save the Standard UNI settings and return to the EVC SR window.

The value in the Link Attributes column now displays as “Changed,” signifying that the link settings have been updated. You can edit the link attributes now or at a future time by clicking on the Changed link and modifying the settings in the Standard UNI Details window.

See [Modifying the EVC Service Request, page 3-54](#) for details on editing the link attributes.

Step 44 To add another link click the **Add** button and set the attributes for the new link as in the previous steps in this section.

Step 45 To delete a link, check the check box in the first column of the row for that link and click the **Delete** button.

Step 46 If you want to set up links with L2 access nodes for this service request, see [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

- Step 47** When you have completed setting the attributes in the EVC Service Request Editor window, click the **Save** button at the bottom of the window to save the settings and create the EVC service request.
- If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.
- For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).
-

Setting Links with L2 Access Nodes (Pseudowire and Local Connect only)

The Links with L2 Access Nodes section of the EVC Service Request Editor window allows you to set up links with L2 (Ethernet) access nodes. These are similar to direct connect links, except that they have L2/Ethernet access nodes beyond the N-PE (towards the CE). Therefore, NPCs are involved. The steps for setting up links with L2 access nodes are similar to those covered in the section [Setting Direct Connect Links, page 3-42](#). See that section for detailed steps on the following common operations:

- Adding and deleting links.
- Selecting the N-PE.
- Choosing the UNI interface.
- Setting the link as an EVC link.
- Editing the standard and EVC link attributes.

The main difference in setting up links with L2 access does is specifying the NPC details.

To set the NPC details for links with L2 access nodes, perform the following steps.

-
- Step 1** The first step in the process of adding a link using NPCs is selecting the U-PE/PE-AGG device, rather than the N-PE.
- If only one NPC exists for the chosen interface, that NPC is autopopulated in the Circuit Details column, and you need not choose it explicitly.
- If more than one NPC is available, click **Select one circuit** in the Circuit Selection column. The NPC window appears, enabling you to choose the appropriate NPC.
- Step 2** Click **OK**.
- Each time you choose a PE and its interface, the NPC that was set up from this PE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.
- If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC.
- Step 3** For details about editing link attributes, adding or deleting links, or using the EVC check box, see the corresponding steps in the section [Setting Direct Connect Links, page 3-42](#).
- Step 4** When you have completed setting the attributes in the EVC Service Request Editor window, click the **Save** button at the bottom of the window to save the settings and create the EVC service request.
- If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.

For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).

Setting VPLS Neighbor Links (VPLS only)

If a VPLS policy has been selected, the bottom window will show VPLS Neighbor Links. If you select two or more N-PEs under Direct Connect Links, you will be able to discover any VPLS enabled neighbors.

To choose the desired path in a Multisegment Pseudowire topology, do the following:

-
- Step 1** Configure the pseudowire by clicking the **Configure Pseudowire** link under VPLS Neighbor Links.
- Step 2** In the pop-up window, click the **Calculate Path** button.
- This displays a path diagram using the shortest path between the previously selected N-PEs. Any existing MPLS-TP tunnels between them will be given priority.
- Step 3** Add (or remove) path constraints by clicking the plus (or minus) icons to the right:
- **Required NE/Link**—Specify network elements or links that traffic must pass through for the path.
 - **Excluded NE/Link**—Specify network elements or links that traffic must *not* pass through for the path.
- Step 4** Once you have decided which path you want to use, click **Save** to complete the create service request operation.

The Service Request Manager window opens.

If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.

For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#). For information about the Service Request Manager elements and operations, see [Chapter 8, “Managing Service Requests.”](#)

Modifying the EVC Service Request

You can modify an EVC service request if you must change or modify the links or other settings of the service request.

To modify an EVC service request, perform the following steps.

-
- Step 1** Choose **Operate > Service Request Manager**.
- The Service Request Manager window appears, showing service requests available in Prime Provisioning.
- Step 2** Check a check box for a service request.
- Step 3** Click **Edit**.

EVC Service Request Editor window appears.

Step 4 Modify any of the attributes, as desired.

See the sections start with [“Setting the Service Request Details”](#) section on page 3-36 for detailed coverage of setting attributes in this window.



Note Once the VC ID, VPLS VPN ID, and VLAN ID have been set in a service request they cannot be modified.

Step 5 To add a template/data file to an attachment circuit, see the section [Using Templates and Data Files with an EVC Ethernet Service Request](#), page 3-55.

Step 6 When you are finished editing the EVC service request, click **Save**.

For additional information about saving an EVC service request, see [Saving the EVC Service Request](#), page 3-55.

Using Templates and Data Files with an EVC Ethernet Service Request

Prime Provisioning does not support configuration of all the available CLI commands on a device being managed by the application. In order to configure such commands on the devices, you can use Prime Provisioning Template Manager functionality. Templates can be associated at the policy level on a per-device role basis. Templates can be overridden at service request level, if the policy-level setting permits the operator to do so.

To associate templates and data files in a service request select any link in the Service Request Editor window and click the **Template** button at the bottom of the window.



Note If the template feature has not been enabled in the associated policy then the Template button will not be available for selection.

The SR Template Association window appears. In this window, you can associate templates at a per-device level. The SR Template Association window lists the devices comprising the link, the device roles, and the template(s)/data file(s) associated with the devices. In this case, the template(s)/data file(s) have not yet been set up.

For further instructions on how to associate templates and data files with a service request, see [Using Templates with Service Requests](#), page 9-24.

Saving the EVC Service Request

To save an EVC Ethernet service request, perform the following steps.

Step 1 When you have finished setting the attributes for the EVC Ethernet service request, click **Save** to create the service request.

If the EVC service request is successfully created, you will see the Service Request Manager window. The newly created EVC Ethernet service request is added with the state of REQUESTED.

- Step 2** If, however, the EVC Ethernet service request creation failed for some reason (for example, a value chosen is out of bounds), you are warned with an error message.
- In such a case, you should correct the error and save the service request again.
- Step 3** If you are ready to deploy the EVC Ethernet service request, see [Deploying Service Requests, page 8-9](#).

Creating an EVC ATM-Ethernet Interworking Policy

This section contains an overview of EVC ATM-Ethernet Interworking support in Prime Provisioning, as well as the basic steps to create an EVC ATM-Ethernet Interworking policy. It contains the following subsections:

- [Defining the EVC Ethernet Policy, page 3-19](#)
- [Setting the Service Options, page 3-20](#)
- [Setting the ATM Interface Attributes, page 3-60](#)
- [Setting the EVC Attributes, page 3-23](#)
- [Setting the Interface Attributes, page 3-29](#)
- [Enabling Template Association, page 3-34](#)

For information on creating EVC ATM-Ethernet service requests, see [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#).



Note

For a general overview of EVC support in Prime Provisioning, see the chapter “Layer 2 Concepts” in the *Cisco Prime Provisioning 6.3 Administration Guide*.

Defining the EVC ATM-Ethernet Interworking Policy

You must define an EVC ATM-Ethernet Interworking policy before you can provision a service. A policy can be shared by one or more service requests that have similar service requirements.

A policy is a template of most of the parameters needed to define an EVC service request. After you define it, an EVC policy can be used by all the EVC service requests that share a common set of characteristics. You create a new EVC policy whenever you create a new type of service or a service with different parameters. EVC policy creation is normally performed by experienced network engineers.

To define an EVC ATM-Ethernet Interworking policy, you start by setting the service type attributes. To do this, perform the following steps.

- Step 1** Choose **Service Design > Create Policy**.
- The Policy Editor window appears.
- Step 2** Choose **EVC** from the Policy Type drop-down list.
- The Policy Editor window appears.
- Step 3** Enter a **Policy Name** for the EVC ATM-Ethernet Interworking policy.
- Step 4** Choose the **Policy Owner** for the EVC policy.
- There are three types of EVC policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this policy.

This ownership has relevance when the Prime Provisioning Role-Based Access Control (RBAC) comes into play. For example, an EVC policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy. Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 5 Click **Select** to choose the owner of the EVC policy.

The policy owner was established when you created customers or providers during Prime Provisioning setup. If the ownership is global, the Select function does not appear.

Step 6 Choose the **Policy Type**.

The choices are:

- **ETHERNET**—See [Creating an EVC Ethernet Policy, page 3-19](#).
- **ATM**—See [Creating an ATM Policy, page 4-19](#).
- **ATM-Ethernet Interworking**—This section.
- **TDM Circuit Emulation**—See [Creating a CEM TDM Policy, page 4-7](#).



Note

This section describes creating the ATM-Ethernet Interworking policy type. For information on using the EVC ETHERNET policy type, see [Creating an EVC Ethernet Policy, page 3-19](#).

Step 7 Click **Next**.

The Service Options window appears.

Step 8 Continue with the steps contained in the next section, [Setting the Service Options, page 3-20](#).

Setting the Service Options

This section describes how to set the service options for the EVC policy.

To set the EVC service options, perform the following steps.

Step 1 Check the **CE Directly Connected to EVC** check box if the CEs are directly connected to the N-PE. This check box is not checked by default.



Note

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this EVC policy can modify the editable parameter during EVC service request creation.

Usage notes:

- If the check box is checked, a service request created using this policy can have only directly connected links. No Ethernet access nodes will be involved.

- If the check box is unchecked, a service request created using this policy might or might not have Ethernet access nodes in the links.
- When a CE is directly connected to the N-PE, NPCs are not applicable to the link while creating service requests.
- When a CE is not directly connected to the N-PE, NPCs are used during service request creation, as per standard Prime Provisioning behavior. There is no change in NPC implementation to support EVC functionality.

Step 2 Check the **All Links Terminate on EVC** check box if all links need to be configured with EVC features. This check box is not checked by default. Usage notes:

- If the check box is checked, a service request created using such policy will have all links using the EVC feature.
- If the check box is unchecked, zero or more links can use the EVC feature. This ensures that existing platforms can still be used in one or more links while delivering the services. This allows the possibility of a link with EVC support being added in the future.



Note If the check box is unchecked, in the service request creation process the user must indicate whether or not the created link is EVC or non-EVC.

- If no links are expected to use the EVC feature even in the future (for example, if the provider is not planning to upgrade to the EVC infrastructure for the service that is being created), existing Prime Provisioning policy types (L2VPN or VPLS) can be used instead of EVC.

Step 3 Choose an **MPLS Core Connectivity Type** from the drop-down list.



Note The core option supports MPLS only. There is no L2TPv3 support for this service.

The choices are:

- **PSEUDOWIRE**—Choose this option to allow connectivity between two N-PEs across the MPLS core. This option does not limit the service to point-to-point (E-Line). This is because even with the PSEUDOWIRE option selected, there can still be multiple CEs connected to a bridge domain on one or both sides of the pseudowire.
- **LOCAL**—Choose this option for local connect cases in which there is no connectivity required across the MPLS core.

Local connect supports the following scenarios:

- All interfaces on the N-PE are EVC-capable and using the EVC infrastructure. This is configured by associating all of the customer traffic on these interfaces to a bridge domain. This consumes a VLAN ID on the N-PE (equal to the bridge domain ID).
- Some interfaces on the N-PE are EVC-capable, while others are switch-port-based. In such cases, all of the customer traffic on the interfaces that are configured with the EVC infrastructure are associated to a bridge domain. The traffic on the non-EVC interfaces (and all the access nodes/interfaces beyond this N-PE) are configured with the Service Provider VLAN ID, where the Service Provider VLAN ID is the same as the bridge domain ID for the EVC-based services.
- Only two interfaces on the N-PE are involved, and both are based on EVC-capable line cards. In the first case, the operator might choose not to configure the bridge domain option. In this case, the **connect** command that is used for the local connects are used, and the global VLAN

is conserved on the device. If the operator chooses to configure with the bridge domain option, both interfaces are associated to a bridge domain ID, so that additional local links can be added to the service in future. This consumes a VLAN ID (bridge domain ID) on the N-PE.

- **VPLS**—This option is not supported for EVC ATM-Ethernet Interworking policies and services requests.

**Note**

Attributes available in subsequent windows of the policy workflow dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE or LOCAL). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

**Note**

Also, some attributes are supported only on IOS or IOS XR platforms. Attributes apply to both platforms, unless otherwise noted. All platform-specific attributes are visible in the policy workflow windows. Later, when a service request is created based on the policy (and specific devices are associated with the service request), platform-specific attributes are filtered from service request windows, depending on the device type (IOS or IOS XR).

- Step 4** Check the **Configure With Bridge Domain** check box to determine bridge domain characteristics. The behavior of the Configure With Bridge-Domain option works in tandem with the choice you selected in the MPLS Core Connectivity Type option, as follows.
- **PSEUDOWIRE** as the MPLS Core Connectivity Type. There are two cases:
 - A. With EVC:
 - If **Configure With Bridge Domain** is checked, the policy configures pseudowires under SVIs associated to the bridge domain.
 - If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under the service instance. This conserves the global VLAN.
 - B. Without EVC:
 - If **Configure With Bridge Domain** is checked, the policy configures pseudowires as in L2VPN services (with SVIs).
 - If **Configure With Bridge Domain** is unchecked, the policy configures pseudowires directly under subinterfaces.

Only pseudowires can be either configured directly under service instance of the corresponding EVC-capable interface or under SVIs associated to the bridge domain.
 - **LOCAL** as the MPLS Core Connectivity Type:
 - If **Configure With Bridge Domain** is checked, the policy allows either point-to-point or multipoint local connect services.
 - If **Configure With Bridge Domain** is unchecked, Prime Provisioning allows only point-to-point local connects without bridge domain.
- Step 5** Click **Next**.
ATM Interface Attribute window appears.
- Step 6** Continue with the steps contained in the next section, [Setting the ATM Interface Attributes, page 3-60](#).

Setting the ATM Interface Attributes

This section describes how to set the ATM Interface attributes for the EVC ATM-Ethernet Interworking policy.

To set the ATM interface attributes, perform the following steps.

-
- Step 1** Choose the **Transport Mode** from the drop-down list.
- The choices are:
- **VP**—Virtual path mode. This is the default.
 - **VC**—Virtual circuit mode.
- Step 2** Choose the **ATM Encapsulation** from the drop-down list.
- **AAL5SNAP**
- Step 3** Click **Next**.
- The EVC Attribute window appears.
- Step 4** Continue with the steps contained in the next section, [Setting the EVC Attributes, page 3-23](#).
-

Setting the EVC Attributes

This section describes how to set the EVC attributes for the EVC ATM-Ethernet Interworking policy.

EVC attributes are organized under the following categories:

- Service Attributes
- VLAN Match Criteria
- VLAN Rewrite Criteria

The following sections describe how to set the options under each category.

Setting the Service Attributes

To set the EVC service attributes, perform the following steps.

-
- Step 1** Check the **AutoPick Service Instance ID** check box to specify that the service instance ID will be autogenerated and allocated to the link during service request creation.
- If the check box is unchecked, while setting the Prime Provisioning link attributes during service request creation, Prime Provisioning will prompt the operator to specify the service instance ID.
- Usage notes:
- The service instance ID represents an Ethernet Flow Point (EFP) on an interface in the EVC infrastructure. The service instance ID is locally significant to the interface. This ID has to be unique only at the interface level. The ID must be a value from 1 to 8000.
 - There are no resource pools available in Prime Provisioning from which to allocate the service instance IDs.

- It is the responsibility of the operator creating the service request to maintain the uniqueness of the ID at the interface level.

Step 2 Check the **AutoPick Service Instance Name** check box to have Prime Provisioning autogenerate a service instance name when you create a service request based on the policy. The autogenerated value is in the following pattern: *CustomerName_ServiceRequestJobID*.

If the check box is unchecked, then you can enter a value during service request creation.

Step 3 Check the **Enable PseudoWire Redundancy** check box to enable pseudowire redundancy (alternative termination device) under certain conditions.

Usage notes:

- Enable Pseudo Wire Redundancy is only available if the MPLS Core Connectivity Type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options](#), page 3-20).

Step 4 Check the **AutoPick VC ID** check box to have Prime Provisioning autopick the VC ID during service request creation.

If this check box is unchecked, the operator will be prompted to specify a VC ID during service request creation.

Usage notes:

- When AutoPick VC ID is checked, Prime Provisioning allocates a VC ID for pseudowires from the Prime Provisioning-managed VC ID resource pool.

Step 5 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID for the service request during service request creation.

If this check box is unchecked, the operator will be prompted to specify a VLAN ID during service request creation.

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain/VLAN ID is picked from the existing Prime Provisioning VLAN pool. Once the VLAN ID is assigned in the service request, Prime Provisioning makes the VLAN ID unavailable for subsequent service requests.
- In the case of manual VLAN ID allocation, Prime Provisioning does not manage the VLAN ID if the ID lies outside the range of an Prime Provisioning-managed VLAN pool. In this case, the operator must ensure the uniqueness of the ID in the Ethernet access domain. If an operator specifies a VLAN ID that is within the range of an Prime Provisioning-managed VLAN pool and the VLAN ID is already in use in the access domain, Prime Provisioning displays an error message indicating that the VLAN ID is in use.

Note on Access VLAN IDs

An access VLAN ID is of local significance to the EVC-capable ports. It should not be confused with the global VLANs. This can be visualized as a partitioning of the Ethernet access network beyond the EVC ports into several subEthernet access domains (one each for an EVC-capable port).

However, all the service interfaces on the Ethernet access nodes beyond the EVC ports will have this very same VLAN ID for a link. This ID must be manually specified by the operator when setting the link attributes during service request creation. The operator must ensure the uniqueness of the ID across the EVC-demarcated Ethernet access domain.

These VLAN IDs are not managed by Prime Provisioning by means of locally-significant VLAN pools. But once a VLAN ID is assigned for a link in the service request, Prime Provisioning makes the VLAN unavailable for subsequent service requests within the Ethernet access domain demarcated by the EVC. Likewise, if a manually-specified VLAN is already in use in the access domain delimited by the EVC,

Prime Provisioning will display an error message indicating that the new VLAN ID being specified is already in use on the NPC. The operator will be prompted to specify a different VLAN ID, which will be provisioned on the L2 access nodes.

- Step 6** Continue with the steps contained in the next section, [Setting the VLAN Matching Criteria Attributes](#), page 3-26.

Setting the VLAN Matching Criteria Attributes

Prior to the introduction of the EVC capability, service providers could either deploy service-multiplexed services (ERS/ERMS or EVPL/EVCS) or service-bundled services on a single port. Both could not be supported simultaneously due to the limitations in the infrastructure, which only allowed matching the outer-most VLAN tag.

One of the key benefits of EVC support in Prime Provisioning is to provide a flexible means to examine the VLAN tags (up to two levels) of the incoming frames and associate them to appropriate Ethernet Flow Points (EFPs). This allows service providers to deploy simultaneously both the service-multiplexed and service-bundled services on a single port.

To set the EVC VLAN matching criteria attributes, perform the following steps.

-
- Step 1** Check the **Both Tags** check box to enable service requests created with the policy to match both the inner and outer VLAN tags of the incoming frames.
- If you do not check this check box, service requests created with the policy will match only the outer VLAN tag of the incoming frames.
- Checking the Both Tags attribute causes the Inner VLAN Ranges attribute (covered in the next steps) to appear in the EVC Attribute window.
- Step 2** Check the **Inner VLAN Ranges** check box to enable the range of inner VLAN tags to be specified during service request creation.
- If the check box is unchecked, the range of inner VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.
- Step 3** Check the **Outer VLAN Ranges** check box to enable the range of outer VLAN tags to be specified during service request creation.
- If the check box is unchecked, the range of outer VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.
- Step 4** Check the **AutoPick Outer VLAN** check box to have Prime Provisioning autopick the outer VLAN ID from a previously created outer VLAN ID resource pool during service request creation.
- If this check box is unchecked, the operator will be prompted to specify an outer VLAN ID during service request creation.



Note

Use of the AutoPick Outer VLAN attribute requires that two elements have already been set up in Prime Provisioning. One is an Interface Access Domain, which is a logical element that groups the physical ports of an N-PE device. The other is an EVC Outer VLAN resource pool, which is used by the Interface Access Domain. For instructions on how to set up these elements, see the sections [Setting Up Resources](#), page 2-40, and [Resource Pools](#), page 2-44.

Usage notes:

- AutoPick Outer VLAN can be used for interfaces that support EVC functionality.
- AutoPick Outer VLAN consumes a VLAN ID on the interface that supports EVC.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 5 Continue with the steps contained in the next section, [Setting the VLAN Rewrite Criteria Attributes](#), page 3-27.

Setting the VLAN Rewrite Criteria Attributes

Together with VLAN matching criteria, VLAN rewrite makes the EVC infrastructure very powerful and flexible. The following VLAN rewrite options are supported:

- Pop one or two tags.
- Push one or two tags.
- Translation (1:1, 2:1, 1:2, 2:2).

Be aware of the following considerations when setting the VLAN rewrite criteria attributes:

- Only one kind of rewrite can be done on every CE-facing EVC link.
- All VLAN rewrites are done using the **symmetric** keyword on the ingress traffic (for example, **rewrite ingress tag pop 2 symmetric**).
- For any service instance, only one type of rewrite option (pop, push, or translate) is allowed per instance. For example, if pop out is enabled, push inner, push outer, translate inner, and translate outer are not available.

To set the EVC VLAN rewrite criteria attributes, perform the following steps.

-
- Step 1** Check the **Pop Outer** check box to pop the outer VLAN ID tag of the incoming frames that fulfill the match criteria.
- If this check box is unchecked, the outer tag of the incoming traffic is not popped.
- Step 2** Check the **Pop Inner** check box to pop the inner VLAN ID tag of the incoming frames that fulfill the match-criteria.
- If this check box is unchecked, the inner tag is not popped. Note that, if Pop Inner is checked, Pop Outer is automatically checked.
- Step 3** Check the **Push Outer** check box to impose an outer VLAN ID tag onto the incoming frames that fulfill the match criteria.
- If this check box is unchecked, no outer tag is imposed on the incoming frames.

Usage notes:

- If Push Outer is checked, all service requests created with the policy push a dot1q outer tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an outer tag with a value from 1 to 4096.
- This attribute is available regardless of the number of tags used in the match criteria. Whether the incoming traffic is double tagged or single tagged, if Push Outer is enabled, all corresponding service requests push an outer tag. All subsequent nodes consider only the outer-most two tags (if EVC-capable) or just one tag (not EVC-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Provisioning-managed VLAN ID pools.

Step 4 Check the **Push Inner** check box to impose an inner VLAN ID tag onto the incoming frames that fulfill the match criteria.

This operation pushes both an inner and an outer tag onto the incoming packet, not just an inner tag. If this check box is unchecked, no inner tag is imposed on the incoming frames.

Usage notes:

- If Push Inner is checked, all service requests created with the policy push a dot1q inner tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an inner tag with a value from 1 to 4096.
- If Push Inner is checked, Push Outer is automatically checked.
- This attribute is available regardless of the number of tags used in the match criteria. Regardless of whether the incoming traffic is double tagged or single tagged, if Push Inner is enabled, all corresponding service requests push an inner tag. All subsequent nodes consider only the outer-most two tags (if EVC-capable) or just one tag (not EVC-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Provisioning-managed VLAN ID pools.

Step 5 Check the **Translate Outer** check box to allow the operator to specify a target outer VLAN ID during service request creation.

The outer tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no outer tag translation is performed. See [Table 3-4](#).

Step 6 Check the **Translate Inner** check box to allow the operator to specify a target inner VLAN ID during service request creation.

The inner tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no inner tag translation is performed. See [Table 3-4](#).



Note

[Table 3-4](#) summarizes the realization of different VLAN translations available in the EVC infrastructure. The second and third columns (Match Outer Tag and Match Inner Tag) refer to policy settings. The last two columns (Translate Outer Tag and Translate Inner Tag) indicate the VLAN translation that occurs on the incoming frames.

Table 3-4 VLAN Translation Summary Table

Type	Match Outer Tag	Match Inner Tag	Translate Outer Tag	Translate Inner Tag	Push Outer Tag
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

Step 7 Click **Next**.

The Interface Attribute window appears.

Step 8 Continue with the steps contained in the next section, [Setting the Interface Attributes, page 3-29](#).

Setting the Interface Attributes

This step of creating the EVC ATM-Ethernet Interworking policy involves setting the interface attributes, as shown in the Interface Attribute window. The attributes you can configure in this window are grouped under the following categories:

- UNI Information
- VLAN
- Pseudowire
- ACL
- Security
- UNI Storm Control
- Protocol

In some cases, checking an attribute causes additional attributes to appear in the GUI. This is covered in the steps that follow.

**Note**

If the CE is directly connected to an N-PE, only speed, duplex, UNI shutdown, and other generic options are presented. In this case, port security, storm control, L2 protocol tunneling, and other advanced features are not supported due to the current platform limitations. If these features are needed for a service, the service provider must deploy Layer 2 Ethernet access nodes beyond the EVC to support these requirements.

**Note**

Attributes available in the Interface Attributes window dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE or LOCAL) in the Service Options window (see [Setting the Service Options, page 3-20](#)). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

To set the EVC interface attributes, perform the following steps.

Step 1 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

**Note**

When the UNI is configured on an N-PE device running IOS XR, the Standard UNI Port attribute is not supported. All the CLIs related to Standard UNI Port and UNI Port Security are ignored in this case.

Step 2 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 3 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable, in order to support modification on a per-service request basis.

Step 4 Enter a **Link Media** (optional) of None, auto-select, rj45, or sfp.

Step 5 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 6 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 7 Choose an **Encapsulation** type.

The choices are:

- **DOT1QTRUNK**—Configures the UNI as a trunk with 802.1q encapsulation. If the UNI belongs to a directly connected and EVC link, this setting signifies that the incoming frames are 802.1q encapsulated and that they match the VLAN ID configured for the link. This specific topology does not involve a trunk UNI as such.
- **DOT1QTUNNEL**—Configures the UNI as an 802.1q tunnel (also known as a dot1q tunnel or Q-in-Q) port.
- **ACCESS**—Configures the UNI as an access port.

Step 8 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation. Translates an incoming customer VLAN to another.
- **2:1**—2:1 VLAN translation. Converts both inner and outer VLANs to a single VLAN.
- **1:2**—1:2 VLAN translation. Pushes one more provider VLAN.
- **2:2**—2:2 VLAN translation. Translates both inner and outer VLANs to two other VLANs.



Note For more details on how VLAN translation is supported in EVC ATM-Ethernet services, see the coverage of the VLAN Translation attribute in [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#).

Step 9 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#) for additional information on pseudowire class support for IOS XR devices.
- If **Use PseudoWireClass** is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning.
- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 10 For **L2VPN Group Name** choose one of the following from the drop-down list:

- **ISC**
- **VPNSC**

Usage notes:

- This attribute is used for provisioning the L2VPN group name on IOS XR devices.

**Note**

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- L2VPN Group Name is only applicable for IOS XR devices.

Step 11 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

Usage notes:

- If no value is specified for the **E-Line Name** in either the policy or the service request based on the policy, Prime Provisioning autogenerates a default name as follows:
 - For PSEUDOWIRE core connectivity type, the format is:
DeviceName--VC_ID
 - For LOCAL core connectivity type, the format is:
DeviceName--VLAN_ID

If the default name is more than 32 characters, the device names are truncated.

- E-Line Name is only applicable for IOS XR devices.

Step 12 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default.

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 13 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Provisioning generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Provisioning generates forwarding commands under the service instance.

For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the policy workflow in the EVC Policy Editor - Service Options window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- Prime Provisioning supports a hybrid configuration for EVC service requests. In a hybrid configuration, the forwarding commands (such as xconnect) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- For examples of these cases, see configlet examples [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\), page 3-212](#) and [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\), page 3-213](#).

- N-PE Pseudo-wire on SVI is applicable for all connectivity types, but a hybrid SVI configuration is possible only for pseudowire connectivity.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. All the xconnect commands are configured on L2 subinterfaces/service instance.
- [Table 3-5](#) shows various use cases for hybrid configuration for EVC service requests.

Table 3-5 Use Cases for Hybrid Configuration for EVC Service Requests

Use Bridge Domain	EVC	N-PE Pseudowire on SVI	CLIs Generated
True	True	True	<ul style="list-style-type: none"> • xconnect under VLAN interface. • Service instance under main interface.
True	True	False	<ul style="list-style-type: none"> • xconnect under service instance. • Service instance under main interface.
False	True	N/A	<ul style="list-style-type: none"> • xconnect under service instance. • Service instance under main interface.
True	False	True	xconnect under VLAN interface.
True	False	False	xconnect under subinterface.
False	False	False	xconnect under subinterface.

Step 14 Check the **Use Existing ACL Name** check box if you want to assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 15 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 17 Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- For **Aging**, enter the length of time the MAC address can stay on the port security table.

- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 18 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 19 Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

For each protocol that you choose, enter the shutdown threshold and drop threshold for that protocol:

- a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- b. **cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 20 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In Cisco Prime Provisioning 6.3, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500 to 1546.

- For the Cisco 7600 Ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500 to 9216. However, Cisco Prime Provisioning 6.3 uses 9216 in both cases.
- For the Cisco 7600 SVI (interface VLAN), the MTU size is 1500 to 9216.

Step 21 If you want to enable template association for this policy, click the **Next** button.

See the section “[Enabling Template Association](#)” section on [page 3-34](#) for information about this feature.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 22 To save the EVC policy, click **Finish**.

To create a service request based on an EVC ATM-Ethernet Interworking policy, see [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#).

Enabling Template Association

The Prime Provisioning template feature gives you a means to download free-format CLIs to a device. If you enable templates, you can create templates and data files to download commands that are not currently supported by Prime Provisioning.

Step 1 To enable template association for the policy, click the **Next** button in the Interface Attribute window (before clicking **Finish**).

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#).

Step 2 When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 3 To save the EVC ATM-Ethernet Interworking policy, click **Finish**.

To create a service request based on an EVC ATM-Ethernet Interworking policy, see [Managing an EVC ATM-Ethernet Interworking Service Request, page 3-70](#).

Managing an EVC ATM-Ethernet Interworking Service Request

This section provides information on how to provision an EVC ATM-Ethernet Interworking service request. It contains the following subsections:

- [Overview, page 3-71](#)
- [Creating an EVC Service Request, page 3-36](#)
- [Setting the Service Request Details, page 3-36](#)
- [Modifying the EVC Service Request, page 3-54](#)
- [Using Templates and Data Files with an EVC Ethernet Service Request, page 3-55](#)
- [Saving the EVC Service Request, page 3-55](#)

Overview

An EVC ATM-Ethernet Interworking service request allows you to configure interfaces on an N-PE to support the EVC features described in [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#). To create an EVC ATM-Ethernet Interworking service request, an EVC ATM-Ethernet Interworking service policy must already be defined, as described in [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#). Based on the predefined EVC policy, an operator creates an EVC service request, with or without modifications to the policy, and deploys the service. One or more templates can also be associated to the N-PE as part of the service request.

ATM-Ethernet interworking is supported through the following configurations:

- ATM Transport Mode (VC)
 - ATM-Ethernet Pseudowire
 - ATM-ATM Local connect
 - ATM-Ethernet Local connect
- ATM Transport Mode (VP)
 - ATM-ATM Local connect

The following steps are involved in creating an EVC ATM-Ethernet Interworking service request:

- Choose an existing EVC ATM-Ethernet Interworking policy.
- Choose a VPN.

**Note**

When working with VPN objects in the context of EVC policies and service requests, only the VPN name and customer attributes are relevant. Other VPN attributes related to MPLS and VPLS are ignored.

- Specify a bridge domain configuration (if applicable).
- Specify a service request description.
- Specify automatic or manual allocation of the VC ID or VPLS VPN ID.
- Add direct connect links (if applicable).
- Add links with L2 access nodes (if applicable).
- Choose the N-PE and UNI interface for links.
- For links with L2 access nodes, choose a Named Physical Circuit (NPC) if more than one NPC exists from the N-PE or the UNI interface.
- Edit the link attributes.
- Modify the service request.

- Save the service request.

For sample configlets for EVC ATM-Ethernet Interworking scenarios, see [Sample Configlets, page 3-177](#).

Creating an EVC ATM-Ethernet Interworking Service Request

To create an EVC ATM-Ethernet Interworking service request, perform the following steps.

-
- Step 1** Choose **Operate > Service Request Manager**.
The Service Request Manager window appears.
- Step 2** Click **Create**.
The Service Request Editor window appears.
- Step 3** From the policy picker, choose an EVC ATM-Ethernet Interworking policy from the policies previously created (see [Creating an EVC ATM-Ethernet Interworking Policy, page 3-56](#)).
The EVC Service Request Editor window appears. The new service request inherits all the properties of the chosen EVC ATM-Ethernet Interworking policy, such as all the editable and non-editable features and pre-set parameters.
- Step 4** Continue with the steps contained in the next section, [Setting the Service Request Details, page 3-36](#).
-

Setting the Service Request Details

After you have selected the EVC policy to be used as the basis of the service request, the EVC Service Request Editor window appears. It is divided into three main sections:

- Link Page
- Direct Connect Links (no NPCs)
- Links with L2 Access Nodes (involves NPCs)

This window enables you to specify options for the service request, as well as configure directly connected links and links with L2 access nodes. The options displayed in first section of the window change, depending on the MPLS Core Connectivity Type that was specified in the policy (pseudowire or local). For clarity, each of these scenarios is presented in a separate section below, to highlight the different window configurations and behavior of the displayed options.

Proceed to the appropriate section, as determined by the MPLS Core Connectivity Type for the policy:

- [Pseudowire Core Connectivity, page 3-37](#)
- [Local Core Connectivity, page 3-40](#)

Instructions for setting up direct connect links and links with L2 access nodes are presented in later sections.

Pseudowire Core Connectivity

This section covers the case in which the MPLS Core Connectivity Type for the EVC ATM-Ethernet Interworking policy is PSEUDOWIRE.

To set the attributes in the first section of the EVC Service Request Editor window, perform the following steps.

**Note**

The **Job ID** and **SR ID** fields are read-only. When the service request is being created for the first time, the fields display a value of NEW. When an existing service request is being modified, the values of the fields indicate the respective IDs that the Prime Provisioning database holds within the editing flow of the service request.

**Note**

The **Policy** field is read-only. It displays the name of the policy on which the service request is based. Clicking on the read-only policy name displays a list of all the attribute values set within the policy.

Step 1 Click **Select VPN** to choose a VPN for use with this service request.

The Select VPN window appears with the VPNs defined in the system.

**Note**

The same VPN can be used by service requests with LOCAL and PSEUDOWIRE core types. If a VPN for a service request is used with VPLS core type, the same VPN cannot be used for service requests with LOCAL or PSEUDOWIRE core type.

Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**.

The EVC Service Request Editor window appears with the VPN name displayed.

Step 4 Check the **AutoPick VC ID** check box if you want Prime Provisioning to choose a VC ID.

If you do not check this check box, you will be prompted to provide the ID in the VC ID field, as covered in the next step.

When AutoPick VC ID is checked, Prime Provisioning allocates a VC ID for pseudowires from the Prime Provisioning-managed VC ID resource pool. In this case, the text field for the VC ID option is non-editable.

Step 5 If AutoPick VC ID was unchecked, enter a VC ID in the **VC ID** field.

Usage notes:

- The AutoPick VC ID attribute appears during the creation of an EVC pseudowire service request.
- The VC ID value must be an integer value corresponding to a VC ID.
- When a VC ID is manually allocated, Prime Provisioning verifies the VC ID to see if it lies within Prime Provisioning's VC ID pool. If the VC ID is in the pool but not allocated, the VC ID is allocated to the service request. If the VC ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VC ID. If the VC ID lies outside of the Prime Provisioning VC ID pool, Prime Provisioning does not perform any verification about whether or not the VC ID allocated. The operator must ensure the VC ID is available.
- The VC ID can be entered only while creating a service. If you are editing the service request, the VC ID field is not editable.

Step 6 Check the **Configure Bridge Domain** check box to determine bridge domain characteristics.

The behavior of the Configure Bridge Domain option works in tandem with the choice you selected in the MPLS Core Connectivity Type option in the EVC policy, which in this case is pseudowire core connectivity. There are two cases:

- With EVC:
 - If **Configure With Bridge Domain** is checked, the policy will configure pseudowires under SVIs associated to the bridge domain.
 - If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under the service instance. This will conserve the global VLAN.
- Without EVC:
 - If **Configure With Bridge Domain** is checked, the policy will configure pseudowires under SVIs.
 - If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under subinterfaces.

Pseudowires can be configured either directly under service instance of the corresponding EVC-capable interface or under SVIs associated to the bridge domain.

Step 7 Check the **Use Split Horizon** check box to enable split horizon with bridge domain.

Usage notes:

- The Use Split Horizon attribute is disabled by default.
- The Use Split Horizon attribute can be used only when the Configure Bridge Domain check box is checked (enabled).
- When Use Split Horizon is enabled, the **bridge domain** command in the CLI will be generated with split horizon. When it is disabled, the **bridge domain** command will be generated without split horizon.

Step 8 Click the “Click here” link of the **Description** attribute to enter a description label for the service request.

This is useful for searching the Prime Provisioning database for the particular service request.

A dialogue appears in which you can enter a description.

Step 9 To set up direct connect links, see the section [Setting Direct Connect Links, page 3-42](#).

Step 10 To set up links with L2 access nodes, see the section [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

Local Core Connectivity

This section covers the case in which the MPLS Core Connectivity Type for the EVC ATM-Ethernet Interworking policy is LOCAL.

To set the attributes in the first section of the EVC Service Request Editor window, perform the following steps.

Step 1 The **Job ID** and **SR ID** fields are read-only.

When the service request is being created for the first time, the fields display a value of NEW. When an existing service request is being modified, the values of the fields indicate the respective IDs that the Prime Provisioning database holds within the editing flow of the service request.

Step 2 The **Policy** field is read-only.

It displays the name of the policy on which the service request is based.

Step 3 Click **Select VPN** to choose a VPN for use with this service request.

The Select VPN window appears with the VPNs defined in the system.



Note The same VPN can be used by service requests with LOCAL and PSEUDOWIRE core types. If a VPN for a service request is used with VPLS core type, the same VPN cannot be used for service requests with LOCAL or PSEUDOWIRE core type.

Step 4 Choose a **VPN Name** in the Select column.

Step 5 Click **Select**.

The EVC Service Request Editor window appears with the VPN name displayed.

Step 6 Check the **Configure Bridge Domain** check box to determine bridge domain characteristics.

Usage notes:

- If Configure Bridge Domain is checked, all links will have the same bridge domain ID allocated from the VLAN pool on the N-PE. All non-EVC links will have the Service Provider VLAN as the bridge domain ID. On the other hand, if no EVC links are added, the Service Provider VLAN will be allocated first and this will be used as the bridge domain ID when EVC links are added.
- If Configure Bridge Domain is unchecked, a maximum of two links that terminate on the same N-PE can be added. (This uses the **connect** command available in the EVC infrastructure.) This is only supported for ATM-ATM local connect.



Note See the following comments for details on how Prime Provisioning autogenerates the connect name.

Because the device only accepts a maximum of 15 characters for the connect name, the connect name is generated using the following format:

CustomerNameTruncatedToMaxPossibleCharacters_ServiceRequestJobID

For example, if the customer name is NorthAmericanCustomer and the service request job ID is 56345, the autogenerated connect name would be NorthAmer_56345.

The CLI generated would be:

```
connect NorthAmer_56345 ATM7/0/5 11 ATM7/0/4 18
```

In this case, 11 and 18 are service instance VPIs.

- If the policy setting for Configure Bridge Domain is non-editable, the option in the service request will be read-only.

Step 7 Check the **Use Split Horizon** check box to enable split horizon with bridge domain.

Usage notes:

- The Use Split Horizon attribute is disabled by default.
- The Use Split Horizon attribute can be used only when the Configure Bridge Domain check box is checked (enabled).
- When Use Split Horizon is enabled, the **bridge domain** command in the CLI will be generated with split horizon. When it is disabled, the **bridge domain** command will be generated without split horizon.

Step 8 Click the “Click here” link of the **Description** attribute to enter a description label for the service request.

A dialogue appears in which you can enter a description.

- Step 9** To set up direct connect links, see the section [Setting Direct Connect Links, page 3-42](#).
- Step 10** To set up links with L2 access nodes, see the section [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

Setting up Links to the N-PE

The lower two sections of the EVC Service Request Editor window allow you to set up links to the N-PE. For direct connect links, the CE is directly connected to the N-PE, with no intermediate L2 access nodes. For links with L2 access nodes, there are intermediate devices present between the CE and NPE requiring NPCs to be created in Prime Provisioning.

The Direct Connect Links section of the window is where you set up links that directly connect to the N-PE. No NPCs are involved. ATM links are supported for direct connect links.

The Links with L2 Access Nodes section is where you set up links with L2 (Ethernet) access nodes. NPCs are involved.



Note ATM interfaces cannot be in L2 access nodes.

See the appropriate section, depending on which type of link you are setting up:

- [Setting Direct Connect Links, page 3-42](#)
- [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#)



Note Many of steps for setting up the two link types are the same. The basic workflow for setting up links, as well as the attributes to be set, are presented in the following section [Setting Direct Connect Links, page 3-42](#). Even if you are setting up links with L2 access nodes, it will be helpful to refer to the information presented in that section, as the section on L2 access nodes only covers the unique steps for such links.

Setting Direct Connect Links

To set up the direct connect links, perform the following steps. Most of these steps apply to links with L2 access nodes also.

- Step 1** Click **Add** to add a link.
- A new numbered row for the link attributes appears.
- Step 2** Click **Select N-PE** in N-PE column.
- The Select PE Device window appears. This window displays the list of currently defined PEs.
- The **Show PEs with** drop-down list shows PEs by Provider, PE Region Name, or by Device Name.
 - The **Find** button allows a search for a specific PE or a refresh of the window.
 - The **Rows per page** drop-down list allows the user to configure the number of entries displayed on the screen at one time.
- Step 3** In the **Select** column, choose the PE device name for the link.

Step 4 Click **Select**.

The EVC Service Request Editor window reappears displaying the name of the selected PE in the NPE column.

Step 5 Choose the UNI interface from the interface picker in the UNI column.**Note**

Prime Provisioning only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name, job ID, service request ID, service request type, translation type, and VLAN ID information.

**Note**

When the UNI is configured on an N-PE device running IOS XR, the Standard UNI Port attribute is not supported. All the CLIs related to Standard UNI Port and UNI Port Security are ignored in this case.

Step 6 Check the **EVC check box** to mark the link for configuring service instance for the links.**Note**

The EVC check box is mentioned at this stage because the setting of the check box alters the behavior of the link editing function available in the Link Attributes column. This is covered in the next steps.

**Note**

The EVC check box is unchecked by default. The default value for the check box can be changed by setting the value of the DCPL property Provisioning\ProvDrv\CheckFlexUniCheckBox.

Editing the Link Attributes

The next steps document the use of the **Edit** link in the Link Attributes column. (In the case where the link attributes have already been set, this link changes from **Edit** to **Change**.) The link editing workflow changes depending on the status of the EVC check box for the link. If the EVC check box is checked, the editing workflow involves setting attributes in two windows, for two sets of link attributes:

- The EVC Details
- Standard UNI Details

If the EVC check box for the link is not checked, only the Standard UNI Details window is presented.

In the steps that follow, both scenarios covered.

**Note**

If you are setting up an ATM link (by choosing an ATM interface as the UNI on the N-PE device, there is a different workflow. The check box in the EVC column dynamically disappears, and clicking the Edit link in the link attributes column brings up the ATM-Ethernet Attributes window. For information on using this window to set up an ATM link, see [Setting the ATM Link Attributes, page 3-86](#).

Step 7 Click **Edit** in the Link Attributes column to specify the UNI attributes.**EVC Details Window**

If the EVC check box is checked, the EVC Details window appears

All of the fields in the EVC Details window are enabled based on the policy settings. For example, if Both Tags is selected in the policy and is editable, then the Match Inner and Outer Tags check box will be selected and editable in this window. The behavior is similar for the other attributes in the EVC Details window

- Step 8** Check the **AutoPick Service Instance ID** check box to specify that the service instance ID will be autogenerated and allocated to the link during service request creation.

If the check box is unchecked, you must specify the service instance ID (see the next step).

Usage notes:

- The service instance ID represents an Ethernet Flow Point (EFP) on an interface in the EVC infrastructure. The service instance ID is locally significant to the interface. This ID has to be unique only at the interface level. The ID must be a value from 1 to 8000.
- There are no resource pools available in Prime Provisioning from which to allocate the service instance IDs.
- In the case of a manually provided service instance ID, it is the responsibility of the operator to maintain the uniqueness of the ID at the interface level.
- This attribute is not displayed for IOS XR devices.

- Step 9** If the AutoPick Service Instance ID check box is not checked, enter an appropriate value for the service instance ID in the **Service Instance ID** field.

- Step 10** Check the **AutoPick Service Instance Name** check box to specify that the service instance name will be autogenerated.

If the check box is unchecked, you can specify the service instance name (see the next step).

Usage notes:

- If the check box is checked, the Service Instance Name text field is disabled.
- The service instance name is autogenerated in the following pattern:
CustomerName_ServiceRequestJobID.
- For example configlets, see [EVC \(No AutoPick Service Instance Name, No Service Instance Name\)](#), [page 3-215](#), [EVC \(User-Provided Service Instance Name, Pseudowire Core Connectivity\)](#), [page 3-216](#), and [EVC \(User-Provided Service Instance Name, Local Core Connectivity\)](#), [page 3-217](#).
- This attribute is not displayed for IOS XR devices.

- Step 11** If the AutoPick Service Instance Name check box is not checked, enter an appropriate value for the service instance ID in the **Service Instance Name** field.

Usage notes:

- The text string representing the service instance name must be 40 characters or less and contain no spaces. Other special characters are allowed.
- If AutoPick Service Instance Name is unchecked and no service instance name is entered in the text field, then Prime Provisioning does not generate the global **ethernet evc evcname** command in the device configuration generated by the service request.

- Step 12** Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID for the service request during service request creation.

If this check box is unchecked, the you must specify a bridge domain VLAN ID (see the next step).

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.

- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.
- This attribute is not displayed for IOS XR devices.

Step 13 If the AutoPick Bridge Domain/VLAN ID check box is unchecked, enter an appropriate value in the **Bridge Domain/VLAN ID** field.



Note This configuration applies in conjunction with the Configure Bridge Domain option in the EVC Service Request Editor window. If the option is not enabled in that window, then AutoPick Bridge Domain/VLAN ID check box is redundant and not required.

When a VLAN ID is manually allocated, Prime Provisioning verifies the VLAN ID to see if it lies within Prime Provisioning's VLAN ID pool. If the VLAN ID is in the pool but not allocated, the VLAN ID is allocated to the service request. If the VLAN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VLAN ID. If the VLAN ID lies outside of the Prime Provisioning VLAN ID pool, Prime Provisioning does not perform any verification about whether the VLAN ID allocated. The operator must ensure the VLAN ID is available.

Step 14 Check the **AutoPick Bridge Domain/VLAN ID Secondary N-PE** check box to have Prime Provisioning autopick the bridge domain VLAN ID for the secondary N-PE of a dual-homed ring during service request creation.

If this check box is unchecked, the you must specify a secondary bridge domain VLAN ID for the secondary N-PE (see the next step).

Usage notes:

- This attribute is only applicable in the case of a dual-homed ring (a ring that terminates on two different N-PEs). Prime Provisioning supports having a separate bridge domain VLAN ID for the secondary N-PE.
- In a dual-homed ring, if the two N-PEs are in different access domains, Prime Provisioning allocates the bridge domain VLAN IDs from both primary and secondary N-PE access domains. When both are in the same Access Domain, Prime Provisioning allocates a common VLAN ID from the Access Domain to which these belong.
- AutoPick Bridge Domain/VLAN ID Secondary N-PE consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.
- This attribute is not displayed for IOS XR devices.

Step 15 If the AutoPick Bridge Domain/VLAN ID Secondary N-PE check box is unchecked, enter an appropriate value in the **Bridge Domain/VLAN ID Secondary N-PE** field.

Step 16 Check the **Match Inner and Outer Tags** check box to enable service requests created with the policy to match both the inner and outer VLAN tags of the incoming frames.

If you do not check this check box, service requests created with the policy will match only the outer VLAN tag of the incoming frames.

Checking the Match Inner and Outer Tags attribute causes the Inner VLAN ID and Outer VLAN ID fields (covered in the next steps) to appear.

Step 17 If the Match Inner and Outer Tags check box is checked, enter the inner and outer VLAN tags in the **Inner VLAN ID** and **Outer VLAN ID** fields.

Usage notes:

- You can specify single values, single ranges, multiples values, multiple ranges, or combinations of these. Examples:

- 10
- 10, 15,17
- 10-15
- 10-15,17-20
- 10,20-25
- If the Inner VLAN Ranges attribute is set to true in the policy, the Inner VLAN ID field can take a range of inner VLAN tags.
- If the Outer VLAN Ranges attribute is set to true in the policy, the Outer VLAN ID field can take a range of Outer VLAN tags.

Step 18 If the Match Inner and Outer Tags check box is unchecked, enter the outer VLAN tag in the **Outer VLAN ID** field.

**Note**

The VLAN specified in Outer VLAN ID will be provisioned on the rest of the L2 access nodes (if the link has any), including the customer-facing UNI.

**Note**

You may also have Prime Provisioning autopick the outer VLAN ID as covered in the next step.

Step 19 Check the **AutoPick Outer VLAN** check box to have Prime Provisioning autopick the outer VLAN ID from a previously created outer VLAN ID resource pool.

If this check box is unchecked, the operator will be prompted to specify an outer VLAN ID.

**Note**

Use of the AutoPick Outer VLAN attribute requires that two elements have already been set up in Prime Provisioning. One is an Interface Access Domain, which is a logical element that groups the physical ports of an N-PE device. The other is an EVC Outer VLAN resource pool, which is used by the Interface Access Domain. For instructions on how to set up these elements, see the sections [Setting Up Resources, page 2-40](#), and [Resource Pools, page 2-44](#).

Usage notes:

- AutoPick Outer VLAN can be used for interfaces that support EVC functionality
- AutoPick Outer VLAN consumes a VLAN ID on the interface that supports EVC.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 20 In the VLAN Rewrite section of the window, choose a **Rewrite Type** from the drop-down list.

The choices are:

- **Pop**
- **Push**
- **Translate**

The subsequent attributes in the GUI change depending on the choice of Rewrite Type, as covered in the next steps.

Step 21 If Pop is the Rewrite Type, two check boxes appear:

- a. Check the **Pop Outer Tag** check box to pop the outer VLAN ID tag of the incoming frames that fulfill the match criteria. If this check box is unchecked, the outer tag of the incoming traffic will not be popped.
- b. Check the **Pop Inner Tag** check box to pop the inner VLAN ID tag of the incoming frames that fulfill the match-criteria. If this check box is unchecked, the inner tag will not be changed.

Note that if Pop Inner Tag is checked, Pop Outer Tag is automatically checked.

Step 22 If Push is the Rewrite Type, two text boxes appear:

- a. In the text box **Outer VLAN ID**, enter an outer VLAN ID tag that will be imposed on the incoming frames that fulfill the match criteria. All service requests created with this setting push a dot1q outer tag on the incoming frames matching the match criteria. If a value is not provided, the push operation is ignored and not configured on the device.
- b. In the text box **Inner VLAN ID**, enter an inner VLAN ID tag that will be imposed on the incoming frames that fulfill the match criteria. All service requests created with this setting push a dot1q inner tag on the incoming frames matching the match criteria. The Inner VLAN tag cannot be pushed without an Outer VLAN tag. That is, when pushing an Inner VLAN tag, the Outer VLAN tag also must be defined.

Step 23 If Translate is the Rewrite Type, a **Translation Type** drop-down list appears.

The choices available in this list vary depending on the setting of the Match Inner and Outer Tags attribute (set in a previous step).

- a. If the Match Inner and Outer Tags check box is checked (true), choose a translation type of **1:1**, **1:2**, **2:1**, or **2:2** from the Translation Type drop-down list.
 - If you choose 1:1 or 2:1, enter a value in the **Outer VLAN ID** text box that appears. The outer tag of all the incoming frames that fulfill the match criteria will be translated to this ID.
 - If you choose 1:2 or 2:2, enter values in the **Outer VLAN ID** and **Inner VLAN ID** text boxes that appear. The outer and inner tags of all the incoming frames that fulfill the match criteria will be translated to these IDs.
- b. If the Match Inner and Outer Tags check box is unchecked (false), choose a translation type of **1:1** or **1:2** from the Translation Type drop-down list.
 - If you choose 1:1, enter a value in the **Outer VLAN ID** text box that appears. The outer tag of all the incoming frames that fulfill the match criteria will be translated to this ID.
 - If you choose 1:2, enter values in the **Outer VLAN ID** and **Inner VLAN ID** text boxes that appear. The outer and inner tags of all the incoming frames that fulfill the match criteria will be translated to these IDs.

Step 24 Clicked **Next** to save the settings in the EVC Details window.

The Standard UNI Details window appears.

Step 25 Continue with setting the standard UNI link attributes in the next steps.

Editing the Standard UNI Attributes

The following steps cover setting the attributes in the Standard UNI Details window. In the case of a link which is not set as an EVC link (by not checking the EVC check box in the Service Request Details window), editing the link attributes begins with this window.

**Note**

The attributes that appear in the Standard UNI Details window are dynamically configured by Prime Provisioning. Some of the attributes covered in the steps below might not appear in the window, depending on the policy and service request settings or the link type. For example, if the MPLS core connectivity type of the EVC policy is local, the pseudowire-related attributes will not appear. Also, setting the link as EVC or non-EVC will change the attributes that appear in the window. In addition, attributes are filtered based on device type (IOS or IOS XR). These cases are noted in the steps, for reference.

Step 26 The **N-PE/U-PE Information** and **Interface Name** fields display the PE device and interface name selected in previous steps.

These fields are read-only.

Step 27 Choose an **Encapsulation** type from the drop-down list.

The choices are:

- **DOT1QTRUNK**—Configures the UNI as a trunk with 802.1q encapsulation. If the UNI belongs to a directly connected and EVC link, this setting signifies that the incoming frames are 802.1q encapsulated and that they match the VLAN ID configured for the link. This specific topology does not involve a trunk UNI as such.
- **DOT1QTUNNEL**—Configures the UNI as an 802.1q tunnel (also known as a dot1q tunnel or Q-in-Q) port.
- **ACCESS**—Configures the UNI as an access port.

This attribute allows you to deploy different types of UNI encapsulation on different links of a service.

Usage notes:

- In the case of direct connect links for which EVC is enabled (by checking the EVC check box in the EVC Service Request Editor window), the choices for the Encapsulation type are DOT1Q and DEFAULT.

Step 28 In the **PE/UNI Interface Description** field, enter a description for the interface, if desired.

Step 29 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation (for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time).

Step 30 Specify the type of **VLAN Translation** for the service request by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.
- **1:2**—1:2 VLAN translation.
- **2:2**—2:2 VLAN translation.

Usage notes:

- The VLAN Translation attribute does not appear for direct connect links if the EVC check box is enabled. It does appear for the following combinations:
 - Direct connect links with EVC check box disabled.
 - L2 access nodes with EVC check box enabled or disabled.

- Choosing a selection other than No causes other fields to appear in the GUI, which you can set based on your configuration:
 - **CE VLAN**—Provide a value between 1 and 4096.
 - **Auto Pick**—Check this check box to have Prime Provisioning autopick the outer VLAN from the VLAN resource pool.
 - **Outer VLAN**—If Auto Pick is unchecked, provide a value between 1 and 4096.
 - **Select where 2:1 or 2:2 translation takes place**—Specify the device where the 2:1 or 2:2 VLAN translation will take place. If you choose Auto, the VLAN translation takes place at the device closest to the UNI port.
- VLAN translation, and all standard UNI and port security attributes are applicable for links with L2 access. If the UNI is on an N-PE, these attributes will not appear.
- When the VLAN translation takes place on a U-PE or PE-AGG device, the VLAN translation command is configured on the NNI interface of the selected device. When the VLAN translation takes place on an NP-E, the VLAN translation command is configured on the UNI interface of the device.
- When there are two NNI interfaces in a ring-based environment, VLAN translation is applied for both of these NNI interfaces.
- 1:1 and 2:1 VLAN translations are supported with the same syntax as for non-EVC (switchport-based N-PE syntax) terminating attachment circuits.

Step 31 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Provisioning generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Provisioning generates forwarding commands under the service instance.

For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the service request workflow in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with scanned under SVI, even if N-PE pseudo-wire on SVI is enabled.
- Prime Provisioning supports a hybrid configuration for EVC service requests. In a hybrid configuration, the forwarding commands (such as scanned) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- N-PE Pseudo-wire on SVI is applicable for all connectivity types (PSEUDOWIRE or LOCAL), but a hybrid SVI configuration is possible only for pseudowire connectivity.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- For examples of these cases, see configlet examples [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\)](#), page 3-212 and [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\)](#), page 3-213.

- For additional information on the N-PE Pseudo-wire on SVI attribute, see the corresponding coverage in the EVC policy section in the section [Setting the Interface Attributes, page 3-29](#).
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. All the xconnect commands are configured on L2 subinterfaces/service instance.

Step 32 Check the **Use Existing PW Class** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- If Use Existing PW Class is checked, an additional attribute, **Existing PW Class Name**, appears in the GUI. Enter the name of a pseudowire class which already exists in the device.
- If Use Existing PW Class is checked, the PW Tunnel Selection and Interface Tunnel attributes will disappear from the window. This is to prevent Prime Provisioning from generating the pseudowire class.
- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Pseudowire Core Connectivity, page 3-37](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 33 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

Usage notes:

- Checking the PW Tunnel Selection check box activates the Interface Tunnel attribute field (see the next step).
- This attribute only appears if the MPLS core connectivity type is set as pseudowire in the EVC policy.

Step 34 If you checked the PW Tunnel Selection check box, enter the TE tunnel ID in the **Interface Tunnel** text field.

Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. During service request creation, Prime Provisioning does not check the validity of the tunnel ID number. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 35 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#) for additional information on pseudowire class support for IOS XR devices.
- If Use PseudoWireClass is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning.
- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Setting the Service Options, page 3-20](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 36 Check the **AutoPick Bridge Group Name** check box to have Prime Provisioning autopick the bridge group name during service request creation.

If this check box is unchecked, you are prompted to specify a bridge group name during service request creation (see the next step).

Usage notes:

- This attribute only displays for IOS XR devices.
- If the AutoPick Bridge Group Name check box is unchecked, enter an bridge group name in the **Bridge Group Name** text field.

Step 37 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID during service request creation.

If this check box is unchecked, you are prompted to specify a VLAN ID during service request creation (see the next step).

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.
- The AutoPick Bridge Domain/VLAN ID attribute appears for both Cisco 7600 and ASR 9000 devices. It will be displayed only for non-EVC links.

Step 38 If the AutoPick Bridge Domain/VLAN ID check box is unchecked, enter an ID number in the **Bridge Domain/VLAN ID** text field.

Usage notes:

- If AutoPick Bridge Domain/VLAN ID is checked, this field is non-editable.
- When a VLAN ID is manually allocated, Prime Provisioning verifies the VLAN ID to see if it lies within Prime Provisioning's VLAN ID pool. If the VLAN ID is in the pool but not allocated, the VLAN ID is allocated to the service request. If the VLAN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VLAN ID. If the VLAN ID lies outside of the Prime Provisioning VLAN ID pool, Prime Provisioning does not perform any verification about whether the VLAN ID allocated. The operator must ensure the VLAN ID is available.
- The Bridge Domain/VLAN ID text field appears for both Cisco 7600 and ASR 9000 devices. It will be displayed only for non-EVC links.

Step 39 For **L2VPN Group Name** choose one of the following from the drop-down list:

- **ISC**
- **VPNSC**

Usage notes:

- This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- L2VPN Group Name is only applicable for IOS XR devices.

Step 40 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

Usage notes:

- If no value is specified for the **E-Line Name**, Prime Provisioning autogenerated a default name as follows:

- For PSEUDOWIRE core connectivity type, the format is:

DeviceName--VC_ID

- For LOCAL core connectivity type, the format is:

DeviceName--VLAN_ID

If the default name is more than 32 characters, the device names are truncated.

- E-Line Name is only applicable for IOS XR devices.

Step 41 Click **OK** to save the Standard UNI settings and return to the EVC SR window.

The value in the Link Attributes column now displays as “Changed,” signifying that the link settings have been updated. You can edit the link attributes now or at a future time by clicking on the Changed link and modifying the settings in the Standard UNI Details window.

See [Modifying the EVC Service Request, page 3-54](#), for details on editing the link attributes.

Step 42 To add another link click the **Add** button and set the attributes for the new link as in the previous steps in this section.

Step 43 To delete a link, check the check box in the first column of the row for that link and click the **Delete** button.

Step 44 If you want to set up links with L2 access nodes for this service request, see [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

Step 45 When you have completed setting the attributes in the EVC Service Request Editor window, click the **Save** button at the bottom of the window to save the settings and create the EVC service request.

If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.

For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).

Setting the ATM Link Attributes

This section describes how to set up a direct connect link as an ATM link.

To set up the ATM link, perform the following steps.

Step 1 In the Direct Connect Links section of the EVC Service Request Editor window, specify the device for which you would like to set up an ATM link.

Step 2 Choose an ATM interface for the UNI.



Note ATM interfaces are displayed in the interface picker in the UNI column only if the EVC service request is based on an ATM-Ethernet Interworking policy type.

When you choose an ATM interface, the check box in the EVC column dynamically disappears from the GUI.

Step 3 In the Link Attributes column, click the **Edit** link of the device on which you want to add an ATM link. The ATM UNI Details window appears.

All of the fields in the ATM UNI Details window are enabled based on the policy settings.

Step 4 Choose the **Transport Mode** from the drop-down list.

The choices are:

- **VP**—Virtual path mode. This is the default.
- **VC**—Virtual circuit mode.

Step 5 Choose the **ATM Encapsulation** from the drop-down list.

- **AAL5SNAP**

Step 6 To specify the ATM virtual channel descriptor (VCD)/subinterface number, enter a value in the **ATM VCD/Sub-Interface #** field.

The value can be from 1 to 2147483647.

Step 7 To specify the ATM virtual path identifier (VPI), enter a value in the **ATM VPI** field.

The value can be from 0 to 255.

Step 8 To specify the ATM virtual channel identifier (VCI), a value in the **ATM VCI** field.

The value can be from 32 to 65535.

Step 9 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation (for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time).

Step 10 Check the **Use Existing PW Class** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- If Use Existing PW Class is checked, an additional attribute, **Existing PW Class Name**, appears in the GUI. Enter the name of a pseudowire class which already exists in the device.
- If Use Existing PW Class is checked, the PW Tunnel Selection and Interface Tunnel attributes will disappear from the window. This is to prevent Prime Provisioning from generating the pseudowire class.
- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see [Pseudowire Core Connectivity, page 3-37](#)).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 11 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Provisioning generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Provisioning generates forwarding commands under the service instance.

For an EVC link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the service request workflow in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- For an ATM link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (in the EVC Service Request Editor window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE pseudo-wire on SVI is enabled.
- Prime Provisioning supports a hybrid configuration for EVC service requests. In a hybrid configuration, the forwarding commands (such as xconnect) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- N-PE Pseudo-wire on SVI is applicable for all connectivity types (PSEUDOWIRE or LOCAL), but a hybrid SVI configuration is possible only for pseudowire connectivity.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- For examples of these cases, see configlet examples [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\)](#), page 3-212 and [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\)](#), page 3-213.
- For additional information on the N-PE Pseudo-wire on SVI attribute, see the corresponding coverage in the EVC policy section in the section [Setting the Interface Attributes](#), page 3-29.
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. All the xconnect commands are configured on L2 subinterfaces/service instance.

Step 12 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

Usage notes:

- Checking the PW Tunnel Selection check box activates the Interface Tunnel attribute field (see the next step).
- This attribute only appears if the MPLS core connectivity type is set as pseudowire in the EVC policy.

Step 13 If you checked the PW Tunnel Selection check box, enter the TE tunnel ID in the **Interface Tunnel** text field.

Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. During service request creation, Prime Provisioning does not check the validity of the tunnel ID number. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 14 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Provisioning autopick the VLAN ID during service request creation.

If this check box is unchecked, you are prompted to specify a VLAN ID during service request creation (see the next step).

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain VLAN ID is picked from the existing Prime Provisioning VLAN pool.

Step 15 If the AutoPick Bridge Domain/VLAN ID check box is unchecked, enter an ID number in the **Bridge Domain/VLAN ID** text field.

Usage notes:

- If AutoPick Bridge Domain/VLAN ID is checked, this field is non-editable.

- When a VLAN ID is manually allocated, Prime Provisioning verifies the VLAN ID to see if it lies within Prime Provisioning's VLAN ID pool. If the VLAN ID is in the pool but not allocated, the VLAN ID is allocated to the service request. If the VLAN ID is in the pool and is already in use, Prime Provisioning prompts you to allocate a different VLAN ID. If the VLAN ID lies outside of the Prime Provisioning VLAN ID pool, Prime Provisioning does not perform any verification about whether the VLAN ID allocated. The operator must ensure the VLAN ID is available.

Step 16 Click **OK** to save the ATM UNI Details settings and return to the EVC Service Request Editor window.

The value in the Link Attributes column now displays as "Changed," signifying that the link settings have been updated. You can edit the link attributes now or at a future time by clicking on the Changed link and modifying the settings in the Standard UNI Details window.

See [Modifying the EVC Service Request, page 3-54](#) for details on editing the link attributes.

Step 17 To add another link click the **Add** button and set the attributes for the new link as in the previous steps in this section.

Step 18 To delete a link, check the check box in the first column of the row for that link and click the **Delete** button.

Step 19 If you want to set up links with L2 access nodes for this service request, see [Setting Links with L2 Access Nodes \(Pseudowire and Local Connect only\), page 3-53](#).

Step 20 When you have completed setting the attributes in the EVC Service Request Editor window, click the **Save** button at the bottom of the window to save the settings and create the EVC service request.

If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.

For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).

Setting Links with L2 Access Nodes

The Links with L2 Access Nodes section of the EVC Service Request Editor window allows you to set up links with L2 (Ethernet) access nodes. These are similar to direct connect links, except that they have L2/Ethernet access nodes beyond the N-PE (towards the CE). Therefore, NPCs are involved.



Note

ATM links are not supported in L2 access nodes. ATM links must be set up as direct connect links. For more information, see [Setting the ATM Link Attributes, page 3-86](#).

The steps for setting up links with L2 access nodes are similar to those covered in the section [Setting Direct Connect Links, page 3-42](#). See that section for detailed steps on the following common operations:

- Adding and deleting links.
- Selecting the N-PE.
- Choosing the UNI interface.
- Setting the link as an EVC link.
- Editing the standard and EVC link attributes.

The main difference in setting up links with L2 access does is specifying the NPC details.

To set the NPC details for links with L2 access nodes, perform the following steps.

-
- Step 1** The first step in the process of adding a link using NPCs is selecting the U-PE/PE-AGG device, rather than the N-PE.
- If only one NPC exists for the chosen interface, that NPC is autopopulated in the Circuit Details column, and you need not choose it explicitly.
- If more than one NPC is available, click **Select one circuit** in the Circuit Selection column. The NPC window appears, enabling you to choose the appropriate NPC.
- Step 2** Click **OK**.
- Each time you choose a PE and its interface, the NPC that was set up from this PE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.
- If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC.
- Step 3** For details about editing link attributes, adding or deleting links, or using the EVC check box, see the corresponding steps in the section [Setting Direct Connect Links, page 3-42](#).
- Step 4** When you have completed setting the attributes in the EVC Service Request Editor window, click the **Save** button at the bottom of the window to save the settings and create the EVC service request.
- If any attributes are missing or incorrectly set, Prime Provisioning displays a warning in the lower left of the window. Make any corrections or updates needed (based on the information provided by Prime Provisioning), and click the **Save** button.
- For information on modifying an EVC service request see the section [Modifying the EVC Service Request, page 3-54](#). For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).
-

Modifying the EVC Service Request

You can modify an EVC service request if you must change or modify the links or other settings of the service request.

To modify an EVC service request, perform the following steps.

-
- Step 1** Choose **Operate > Service Request Manager**.
- The Service Request Manager window appears, showing service request available in Prime Provisioning.
- Step 2** Check a check box for a service request.
- Step 3** Click **Edit**.
- EVC Service Request Editor window appears.
- Step 4** Modify any of the attributes, as desired.
- See the sections start with [Setting the Service Request Details, page 3-36](#), for detailed coverage of setting attributes in this window.

**Note**

Once the VC ID, VPLS VPN ID, and VLAN ID have been set in a service request they cannot be modified.

- Step 5** To add a template/data file to an attachment circuit, see the section [Using Templates and Data Files with an EVC Ethernet Service Request, page 3-55](#).
- Step 6** When you are finished editing the EVC service request, click **Save**.
For additional information about saving an EVC service request, see [Saving the EVC Service Request, page 3-55](#).

Using Templates and Data Files with an EVC Service Request

Prime Provisioning does not support configuration of all the available CLI commands on a device being managed by the application. In order to configure such commands on the devices, you can use Prime Provisioning Template Manager functionality. Templates can be associated at the policy level on a per-device role basis. Templates can be overridden at service request level, if the policy-level setting permits the operator to do so.

To associate templates and data files in a service request select any link in the EVC Service Request Editor window and click the **Template** button at the bottom of the window.

**Note**

If the template feature has not been enabled in the associated policy then the Template button will not be available for selection.

The SR Template Association window appears. In this window, you can associate templates at a per-device level.

The Template Association window lists the devices comprising the link, the device roles, and the template(s)/data file(s) associated with the devices. In this case, the template(s)/data file(s) have not yet been set up.

For further instructions on how to associate templates and data files with a service request, see [Using Templates with Service Requests, page 9-24](#).

Saving the EVC Service Request

To save an EVC service request, perform the following steps.

- Step 1** When you have finished setting the attributes for the EVC service request, click **Save** to create the service request.
If the EVC service request is successfully created, you will see the Service Request Manager window. The newly created EVC service request is added with the state of REQUESTED.
- Step 2** If, however, the EVC service request creation failed for some reason (for example, a value chosen is out of bounds), you are warned with an error message.
In such a case, you should correct the error and save the service request again.

Step 3 If you are ready to deploy the EVC service request, see [Deploying Service Requests, page 8-9](#).

Creating an L2VPN Policy

This section covers the basic steps to create an L2VPN policy. It contains the following subsections:

- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Defining an Ethernet ERS \(EVPL\) Policy with a CE, page 3-94](#)
- [Defining an Ethernet ERS \(EVPL\) Policy without a CE, page 3-98](#)
- [Defining an Ethernet EWS \(EPL\) Policy with a CE, page 3-102](#)
- [Defining an Ethernet EWS \(EPL\) Policy without a CE, page 3-107](#)
- [Defining a Frame Relay Policy with a CE, page 3-112](#)
- [Defining a Frame Relay Policy without a CE, page 3-114](#)
- [Defining an ATM Policy with a CE, page 3-116](#)
- [Defining an ATM Policy without a CE, page 3-118](#)

Defining an L2VPN Policy

You must define an L2VPN policy before you can provision a Prime Provisioning service. An L2VPN policy defines the common characteristics shared by the end-to-end wire attributes and Attachment Circuit (AC) attributes.

A policy is a template of most of the parameters needed to define an L2VPN service request. After you define it, an L2VPN policy can be used by all the L2VPN service requests that share a common set of characteristics. You create a new L2VPN policy whenever you create a new type of service or a service with different parameters. L2VPN policy creation is normally performed by experienced network engineers.

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is *not* set to editable, the service request creator cannot change the policy item.

You can also associate Prime Provisioning templates and data files with a policy. See [Chapter 9, “Managing Templates and Data Files”](#) for more about using templates and data files in policies.

It is also possible to create user-defined attributes within a policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#)

The four major categories of an L2VPN policy correspond to the four major services that L2VPN provides:

- Point-to-point Ethernet Relay Service (ERS). The Metro Ethernet Forum (MEF) name for this service is Ethernet Virtual Private Line (EVPL). For more information about terms used to denote L2VPN services in this guide, see the section “Layer 2 Terminology Conventions” in the L2VPN Concepts chapter in the [Cisco Prime Provisioning 6.3 Administration Guide](#).
- Point-to-point Ethernet Wire Service (EWS). The MEF name for this service is Ethernet Private Line (EPL).

- Frame Relay over MPLS (FRoMPLS)
- ATM over MPLS (ATMoMPLS)

To define an L2VPN policy in Prime Provisioning, perform the following steps.

Step 1 Choose **Service Design > Create Policy**.

The Policy Editor window appears.

Step 2 Choose **L2VPN** from the Policy Type drop-down list.

The Policy Editor window appears.

Step 3 Enter a **Policy Name** for the L2VPN policy.

Step 4 Choose the **Policy Owner** for the L2VPN policy.

There are three types of L2VPN policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this L2VPN policy.

This ownership has relevance when the Prime Provisioning Role-Based Access Control (RBAC) comes into play. For example, an L2VPN policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 5 Click **Select** to choose the owner of the L2VPN.

(If you choose Global ownership, the Select function is not available.) The Select Customer window or the Select Provider window appears and you can choose an owner of the policy and click **Select**.

Step 6 Choose the **Service Type** of the L2VPN policy.

There are four service types for L2VPN policies:

- L2VPN ERS (EVPL)
- L2VPN EWS (EPL)
- Frame Relay
- ATM

Subsequent sections cover setting up the policies for each of these services.

Step 7 Check the **CE Present** check box if you want Prime Provisioning to ask the service operator who uses this L2VPN policy to provide a CE router and interface during service activation.

The default is CE present in the service.

If you do not check the **CE Present** check box, Prime Provisioning asks the service operator, during service activation, only for the U-PE or the N-PE router and customer-facing interface.

Step 8 Click **Next**.

The next sections contain examples of setting policies for the service types, with and without a CE present.

Defining an Ethernet ERS (EVPL) Policy with a CE

This section describes defining an Ethernet ERS (EVPL) policy with CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **L2VPN ERS** for the Policy Type.

Step 2 Check the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.



Note

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

Step 5 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a U-PE or N-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 6 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 7 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

**Note**

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

- Step 8** Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.
- Step 9** Check the **Keep Alive** check box to configure keepalives on the UNI port.
- By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.
- Step 10** Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 11** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 12** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.
- If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 13** Check the **VC ID AutoPick** check box if you want Prime Provisioning to choose a VC ID.
- If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.
- Step 14** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.
- The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.
- Step 15** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.
- This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.
- Step 16** Choose an **L2VPN Group Name** from the drop-down list.
- The choices are:
- **ISC**
 - **VPNSC**
- This attribute is used for provisioning the L2VPN group name on IOS XR devices.

**Note**

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- Step 17** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the **p2p** name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 18 Enter a **Link Media** type (optional) of None, auto-select, rj45, or sfp.

Usage notes:

- The default is None.
- When this attribute is used, a new CLI will be generated in the UNI interface to define the media type.
- The Link Media attribute is supported only for ME3400 platforms.

Step 19 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 20 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this box is unchecked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 24 Choose a **UNI Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**



Note

Enter a UNI Port Type only if the encapsulation type is DEFAULT.

Step 25 Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- For **Aging**, enter the length of time the MAC address can stay on the port security table.
- For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.

- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 26 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 27 Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.



Note

The **N-PE Pseudo-wire on SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 28 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.



Note

For detailed coverage of setting up VLAN translation, see [Setting Up VLAN Translation for L2VPN ERS \(EVPL\) Services, page 3-172](#).

Step 29 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.



Note

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 30 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 31 Click **Finish**.

Defining an Ethernet ERS (EVPL) Policy without a CE

This section describes defining an Ethernet ERS (EVPL) policy without a CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **L2VPN ERS** for the Policy Type.

Step 2 Uncheck the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 5 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

**Note**

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

- Step 6** Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

- Step 7** Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

**Note**

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

- Step 8** Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

- Step 9** Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

- Step 10** Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 11** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 12** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID. If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

- Step 13** Check the **VC ID AutoPick** check box if you want Prime Provisioning to choose a VC ID.

If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

- Step 14** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

- Step 15** Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

Step 16 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 17 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

Step 18 Enter a **Link Media** type (optional) of None, auto-select, rj45, or sfp.

Usage notes:

- The default is None.
- When this attribute is used, a new CLI will be generated in the UNI interface to define the media type.
- The Link Media attribute is supported only for ME3400 platforms.

Step 19 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 20 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is unchecked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you unchecked the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 24 Choose a **UNI Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**



Note Enter a UNI Port Type only if the encapsulation type is DEFAULT.

- Step 25** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 26** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.
- Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.
- Step 27** Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.
- This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.



Note The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

- Step 28** Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.
- The choices are:
- **No**—No VLAN translation is performed. (This is the default.)
 - **1:1**—1:1 VLAN translation.
 - **2:1**—2:1 VLAN translation.



Note For detailed coverage of setting up VLAN translation, see [Setting Up VLAN Translation for L2VPN ERS \(EVPL\) Services](#), page 3-172.

- Step 29** Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

**Note**

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

- Step 30** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

- Step 31** Click **Finish**.

Defining an Ethernet EWS (EPL) Policy with a CE

This section describes defining an Ethernet EWS (EPL) policy with CE present.

Perform the following steps.

- Step 1** In the Service Information window of the Policy Editor, choose **L2VPN EWS** for the Policy Type.

- Step 2** Check the **CE Present** check box.

- Step 3** Click **Next**.

The Interface Type window appears.

- Step 4** Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

**Note**

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

**Note**

In previous releases, the only Layer 2 VPN support for EWS (EPL) was from EWS (EPL) to EWS (EPL). In ISC 4.1.2 and later, support is also from EWS (EPL) to Network to Network Interface (NNI) as a trunk port. To create this new type of service request, you need to create an EWS (EPL) “hybrid” policy by unchecking the standard UNI flag. When using the EWS (EPL) hybrid policy for service request creation, check the **Standard UNI Port flag** for the EWS (EPL) side of the connection and uncheck the standard UNI flag for the NNI side of the connection.

**Note**

In the case of hybrid services, UNI on an N-PE running IOS XR is not supported.

Step 5 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a U-PE or N-PE interface based on the service provider’s POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 6 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.

Step 7 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

**Note**

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

- Step 8** Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.
- Step 9** Check the **Keep Alive** check box to configure keepalives on the UNI port.
- By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.
- Step 10** Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 11** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 12** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.
- If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 13** Check the **VC ID AutoPick** check box if you want Prime Provisioning to choose a VC ID.
- If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.
- Step 14** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.
- This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#) for additional information on pseudowire class support for IOS XR devices.
- Step 15** Choose an **L2VPN Group Name** from the drop-down list.
- The choices are:
- **ISC**
 - **VPNSC**
- This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- Step 16** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.
- This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.
- Step 17** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.
- The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID. If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 19** Enter a **Link Media** type (optional) of None, auto-select, rj45, or sfp.
- Usage notes:
- The default is None.
 - When this attribute is used, a new CLI will be generated in the UNI interface to define the media type.
 - The Link Media attribute is supported only for ME3400 platforms.
- Step 20** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 21** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 22** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 23** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note**

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

- Step 24** Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.
- This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.
- Step 25** Check the **UNI Port Security** check box if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 26** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm. Enter a threshold value for each type of traffic.

The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

- Step 27** Check the **Protocol Tunneling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

For each protocol that you choose, enter the shutdown threshold and drop threshold for that protocol:

- a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- b. **cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

- Step 28** Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.



Note

The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

- Step 29** Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In Cisco Prime Provisioning 6.3, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Cisco Prime Provisioning 6.3 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

- Step 30** Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.



Note

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 31 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 32 Click **Finish**.

Defining an Ethernet EWS (EPL) Policy without a CE

This section describes how to define an Ethernet EWS (EPL) policy without a CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **L2VPN EWS** for the Policy Type.

Step 2 Uncheck the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)

- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 5 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.



Note

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.



Note

In previous releases, the only Layer 2 VPN support for EWS (EPL) was from EWS (EPL) to EWS (EPL). In ISC 4.1.2 and later, support is also from EWS (EPL) to Network to Network Interface (NNI) as a trunk port. To create this new type of service request, you need to create an EWS (EPL) “hybrid” policy by unchecking the standard UNI flag. When using the EWS (EPL) hybrid policy for service request creation, check the **Standard UNI Port flag** for the EWS (EPL) side of the connection and uncheck the standard UNI flag for the NNI side of the connection.



Note

In the case of hybrid services, UNI on an N-PE running IOS XR is not supported.

Step 6 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.

Step 7 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.



Note

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

Step 8 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 9 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

- Step 10** Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is not checked by default.

- Step 11** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is not checked by default.

- Step 12** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

- Step 13** Check the **VC ID AutoPick** check box if you want Prime Provisioning to choose a VC ID.

If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

- Step 14** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

- Step 15** Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- Step 16** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

- Step 17** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

- Step 18** Enter a **Link Media** type (optional) of None, auto-select, rj45, or sfp.

Usage notes:

- The default is None.

- When this attribute is used, a new CLI will be generated in the UNI interface to define the media type.
- The Link Media attribute is supported only for ME3400 platforms.

Step 19 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 20 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 24 Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- For **Aging**, enter the length of time the MAC address can stay on the port security table.
- For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 25 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 26 Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

- Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

- b. **cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 27 Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.



Note

The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 28 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In Cisco Prime Provisioning 6.3, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Cisco Prime Provisioning 6.3 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 29 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback

address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

**Note**

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 30 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 31 Click **Finish**.

Defining a Frame Relay Policy with a CE

This section describes how to define a Frame Relay policy with CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **Frame Relay** for the Policy Type.

Step 2 Check the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 5 Choose the **Interface Type** for the **CE** from the drop-down list.

The choices are:

- **ANY**
- **Serial**
- **MFR**
- **POS**
- **Hssi**
- **BRI**

Step 6 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 7 Choose the CE Encapsulation type.

The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**



Note

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

Step 8 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

Step 9 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

Step 10 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 11 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 12 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 13 Click **Finish**.

Defining a Frame Relay Policy without a CE

This section describes how to define a Frame Relay policy without a CE present. Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **Frame Relay** for the Policy Type.

Step 2 Uncheck the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 5 Choose the N-PE/U-PE **Interface Type** for the **CE** from the drop-down list.

The choices are:

- **ANY**
- **Serial**
- **MFR**
- **POS**
- **Hssi**
- **BRI**

Step 6 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 7 Choose the N-PE/U-PE **Encapsulation** type.

The choices are:

- **FRAME RELAY**

- **FRAME RELAY IETF**

**Note**

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

- Step 8** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

- Step 9** Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.

**Note**

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

- Step 10** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

- Step 11** Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

- Step 12** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 13 Click **Finish**.

Defining an ATM Policy with a CE

This section describes how to define an ATM policy with CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **ATM** for the Policy Type.

Step 2 Check the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Choose the **Transport Mode** from the drop-down list.

The choices are:

- **VP**—Virtual path mode. This is the default.
- **VC**—Virtual circuit mode.
- **PORT**—Port mode. (Only supported for the IOS XR 3.7 platform.) Usage notes:
 - If you choose PORT as the transport mode, the attributes **ATM VCD/Sub-interface #** and **ATM VPI** will be disabled in the Link Attributes window of the service request based on this policy.
 - If you choose PORT as the transport mode, three attributes for setting timer values will appear in the Link Attributes window of the service request based on this policy. These attributes are **Timer1**, **Timer2**, and **Timer3**. They are used to add timer values. The permissible range for these values is 50 to 4095. This feature is supported only for an N-PE as a UNI device.
 - If you choose PORT as the transport mode, two attributes for setting cell packing will appear in the Link Attributes window of the service request based on this policy. These attributes are **Maximum no. of cells to be packed** and **Cell packing timer**. This feature is supported only for an N-PE as a UNI device.

Step 5 Choose the **CE Interface Type** from the drop-down list.

The choices are:

- **ANY**
- **ATM**
- **Switch**

Step 6 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 7 Choose a **CE Encapsulation**.

The choices are:

- **AAL5SNAP**
- **AAL5MUX**
- **AAL5NLPID**
- **AAL2**



Note

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

Step 8 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 9 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

Step 10 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

Step 11 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 12 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback

address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

Step 13 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 14 Click **Finish**.

Defining an ATM Policy without a CE

This section describes how to define an ATM policy without a CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **ATM** for the Policy Type.

Step 2 Uncheck the **CE Present** check box.

Step 3 Click **Next**.

The Interface Type window appears.

Step 4 Choose the **Transport Mode** from the drop-down list.

The choices are:

- **VP**—Virtual path mode. This is the default.
- **VC**—Virtual circuit mode.
- **PORT**—Port mode. (Only supported for the IOS XR 3.7 platform.) Usage notes:
 - If you choose PORT as the transport mode, the attributes **ATM VCD/Sub-interface #** and **ATM VPI** will be disabled in the Link Attributes window of the service request based on this policy.
 - If you choose PORT as the transport mode, three attributes for setting timer values will appear in the Link Attributes window of the service request based on this policy. These attributes are **Timer1**, **Timer2**, and **Timer3**. They are used to add timer values. The permissible range for these values is 50 to 4095. This feature is supported only for an N-PE as a UNI device.
 - If you choose PORT as the transport mode, two attributes for setting cell packing will appear in the Link Attributes window of the service request based on this policy. These attributes are **Maximum no. of cells to be packed** and **Cell packing timer**. This feature is supported only for an N-PE as a UNI device.

Step 5 Choose the **N-PE/U-PE Interface Type** from the drop-down list.

The choices are:

- ANY
- ATM
- Switch

Step 6 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 7 Choose a **PE Encapsulation**.

The choices are:

- AAL5SNAP
- AAL5MUX
- AAL5NLPID
- AAL5
- AAL0



Note

If the Interface Type is ANY, Prime Provisioning will not ask for an **Encapsulation** type in the policy.

Step 8 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 9 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Provisioning. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes, page 3-15](#), for additional information on pseudowire class support for IOS XR devices.

Step 10 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- ISC
- VPNSC

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note

The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 3-18](#).

Step 11 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, Prime Provisioning generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.

- Step 12** Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. Prime Provisioning uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, Prime Provisioning does not check the validity of the value. That is, Prime Provisioning does not verify the existence of the tunnel.

- Step 13** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

- Step 14** Click **Finish**.

Managing an L2VPN Service Request

This section covers the basic steps to provision an ERS (EVPL), EWS (EPL), ATM, or Frame Relay L2VPN service. It contains the following subsections:

- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Creating an EVC Service Request, page 3-36](#)
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request with a CE, page 3-122](#)
- [Creating an EWS \(EPL\) L2VPN Service Request with a CE, page 3-124](#)
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request without a CE, page 3-125](#)
- [Creating an EWS \(EPL\) L2VPN Service Request without a CE, page 3-127](#)
- [Modifying the EVC Service Request, page 3-54](#)
- [Saving the L2VPN Service Request, page 3-131](#)

Introducing L2VPN Service Requests

An L2VPN service request consists of one or more end-to-end wires, connecting various sites in a point-to-point topology. When you create a service request, you enter several parameters, including the specific interfaces on the CE and PE routers.

You can also associate Prime Provisioning templates and data files with a service request. See [Chapter 9, “Managing Templates and Data Files”](#) for more about using templates and data files in service requests.

It is also possible to create user-defined attributes within a policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#)

To create a service request, a Service Policy must already be defined, as described in [Creating a VPLS Policy, page 3-131](#).

Based on the predefined L2VPN policy, an operator creates an L2VPN service request, with or without modifications to the L2VPN policy, and deploys the service. Service creation and deployment are normally performed by regular network technicians for daily operation of network provisioning.

**Note**

Not all of the attributes defined in an L2VPN policy might be applicable to a service request. For specific information, see L2VPN policy attribute descriptions in [Creating an L2VPN Policy, page 3-92](#).

The following steps are involved in creating a service request for Layer 2 connectivity between customer sites:

- Choose a CE Topology for ERS (EVPL)/Frame Relay/ATM services.
- Choose the endpoints (CE and PE) that must be connected. For each end-to-end Layer 2 connection, Prime Provisioning creates an end-to-end wire object in the repository for the service request.
- Choose a CE or PE interface.
- Choose a Named Physical Circuit (NPC) for the CE or PE.
- Edit the end-to-end connection.
- Edit the link attributes.
- (Optional) Associate templates and data files to devices in the service request.

For sample configlets for L2VPN scenarios, see [Sample Configlets, page 3-177](#).

Creating an L2VPN Service Request

To create an L2VPN service request, perform the following steps.

-
- Step 1** Choose **Operate > Create Service Request**.
The Service Request Editor window appears.
- Step 2** From the policy picker choose an L2VPN policy from the policies previously created (see [Creating an L2VPN Policy, page 3-92](#)).
The L2VPN Service Request editor window appears.
The new service request inherits all the properties of the chosen L2VPN policy, such as all the editable and non-editable features and pre-set parameters.
- Step 3** To continue creating an L2VPN service request, go to one of the following sections:

- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request with a CE, page 3-122.](#)
- [Creating an EWS \(EPL\) L2VPN Service Request with a CE, page 3-124.](#)
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request without a CE, page 3-125.](#)
- [Creating an EWS \(EPL\) L2VPN Service Request without a CE, page 3-127.](#)

Creating an ERS (EVPL), ATM, or Frame Relay L2VPN Service Request with a CE

This section includes detailed steps for creating an L2VPN service request with a CE present for ERS (EVPL), ATM, and Frame Relay policies. If you are creating an L2VPN service request for an EWS (EPL) policy, go to [Creating an EWS \(EPL\) L2VPN Service Request with a CE, page 3-124.](#)

After you choose an L2VPN policy, the L2VPN Service Request Editor window appears.

Perform the following steps.

Step 1 Create the L2VPN service request for the policy.

The L2VPN Service Request Editor window appears.

Step 2 Choose a **Topology** from the drop-down list.

If you choose **Full Mesh**, each CE will have direct connections to every other CE.

If you choose **Hub and Spoke**, then only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other.



Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two endpoints. For example, with four endpoints, Prime Provisioning automatically creates six links with full mesh topology. With hub and spoke topology, however, Prime Provisioning creates only three links.

Step 3 Click **Add Link**.

You specify the CE endpoints using the Attachment Tunnel Editor.



Note All the services that deploy point-to-point connections (ERS/EVPL, EWS/EPL, ATMoMPLS, and FRoMPLS) must have at least two CEs specified.

Step 4 Click **Select CE** in the CE column.

The Select CPE Device window appears. This window displays the list of currently defined CEs.

- From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.
- You can use the **Find** button to either search for a specific CE, or to refresh the display.
- You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Step 5 In the Select column, choose a CE for the L2VPN link.

Step 6 Click **Select**.

The Service Request Editor window appears displaying the name of the selected CE in the CE column.

Step 7 Choose the CE interface from the interface picker.

**Note**

When you provision an L2VPN ERS (EVPL) service, when you choose a UNI for a particular device, Prime Provisioning determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests relying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

**Note**

Prime Provisioning only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.

Step 8 If only one NPC exists for the Chosen CE and CE interface, that NPC is autopopulated in the Circuit Selection column and you need not choose it explicitly. If more than one NPC is available, click **Select one circuit** in the Circuit Selection column.

The Select NPC window appears, enabling you to choose the appropriate NPC.

Step 9 Click **OK**.

Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.

If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC.

Step 10 Continue to specify additional CEs, as in previous steps.

Prime Provisioning creates the links between CEs based on the Topology that you chose.

Step 11 Click **OK**.

For ERS (EVPL), ATM, and Frame Relay, the EndToEndWire window appears.

Step 12 The VPN for this service request appears in the **VPN** field.

If there is more than one VPN, click **Select VPN** to choose a VPN. The Select VPN window appears.

Step 13 Choose a **VPN Name** and click **Select**.

The L2VPN Service Request Editor window appears with the VPN name displayed.

Step 14 If necessary, click **Add AC** in the Attachment Circuit2 (AC2) column, and repeat Steps 3 to 10 for AC2. The EndToEndWire window displays the complete end-to-end wire.

Step 15 Specify remaining items in the EndToEndWire window as necessary for your configuration:

- You can choose any of the **blue** highlighted values to edit the end-to-end wire.
- You can edit the AC link attributes to change the default policy settings. After you edit these fields, the **blue** link changes from Default to Changed. For more information, see the section [Modifying the EVC Service Request, page 3-54](#).
- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

- You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.
- The ID number is system-generated identification number for the circuit.
- The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.
- If the policy was set up for you to define a VC ID manually, enter it into the empty **VC ID** field. If policy was set to “auto pick” the VC ID, Prime Provisioning will supply a VC ID, and this field will not be editable. In the case where you supply the VC ID manually, if the entered value is in the provider’s range, Prime Provisioning validates if the entered value is available or allocated. If the entered value has been already allocated, Prime Provisioning generates an error message saying that the entered value is not available and prompts you to re-enter the value. If the entered value is in the provider’s range, and if it is available, then it is allocated and is removed from the VC ID pool. If the entered value is outside the provider’s range, Prime Provisioning displays a warning saying that no validation could be performed to verify if it is available or allocated.
- You can also click **Add Link** to add an end-to-end wire.
- You can click **Delete Link** to delete an end-to-end wire.

Step 16 When you are finished editing the end-to-end wires, click **Save**.

The service request is created and saved into Prime Provisioning.

Creating an EWS (EPL) L2VPN Service Request with a CE

This section includes detailed steps for creating an L2VPN service request with a CE present for EWS (EPL). If you are creating an L2VPN service request for an ERS (EVPL), ATM, or Frame Relay policy, go to [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request with a CE, page 3-122](#).

Perform the following steps.

Step 1 Create the L2VPN service request for EWS (EPL) with CE.

The L2VPN Service Request Editor window appears.

Step 2 Click **Select VPN** to choose a VPN for use with this CE.

The Select VPN window appears with the VPNs defined in the system.

Step 3 Choose a **VPN Name** in the Select column.

Step 4 Click **Select**.

The L2VPN Service Request Editor window appears with the VPN name displayed.

Step 5 Click **Add Link**.

- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Request Editor window. The maximum length for this field is 256 characters.
- You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.
- The ID number is system-generated identification number for the circuit.

- The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.
- Step 6** Click **Add AC** in the Attachment Circuit1 (AC1) column.
The Customer and Link Selection window appears.
- Step 7** Click **Select CE**.
The Select CPE Device window appears.
This window displays the list of currently defined CEs.
- a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.
 - b. You can use the **Find** button to either search for a specific CE, or to refresh the display.
 - c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.
- Step 8** In the Select column, choose a CE for the L2VPN link.
- Step 9** Click **Select**.
- Step 10** In the Customer and Link Selection window, choose a CE interface from the interface picker.
- Step 11** If only one NPC exists for the Chosen CE and CE interface, that NPC is autopopulated in the Circuit Selection column and you need not choose it explicitly.

If more than one NPC is available, click **Select one circuit** in the Circuit Selection column. The Select NPC window appears, enabling you to choose the appropriate NPC. Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.
- Step 12** Click **OK**.
The EndToEndWire window appears displaying the name of the selected CE in the AC1 column.
- Step 13** Click the Edit link in the AC1 Attributes column to edit the attributes of the attachment circuit if desired.
The Link Attributes window appears. Edit the attributes as desired. For more information, see the section [Modifying the EVC Service Request, page 3-54](#).
- Step 14** Click **OK**.
- Step 15** Repeat Steps 6 through 14 for **AC2**.
- Step 16** In the L2VPN Service Request Editor, click **Save**.
The EWS (EPL) service request is created and saved in Prime Provisioning.

Creating an ERS (EVPL), ATM, or Frame Relay L2VPN Service Request without a CE

This section includes detailed steps for creating an L2VPN service request without a CE present for ERS (EVPL), ATM, and Frame Relay policies. If you are creating an L2VPN service request for an EWS (EPL) policy, go to [Creating an EWS \(EPL\) L2VPN Service Request without a CE, page 3-127](#).

Perform the following steps.

- Step 1** Create the L2VPN service request for ERS (EVPL) without a CE.
The L2VPN Service Request Editor window appears.

Step 2 Choose a **Topology** from the drop-down list.

If you choose **Full Mesh**, each CE will have direct connections to every other CE. If you choose **Hub and Spoke**, then only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other.



Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two endpoints. For example, with four endpoints, Prime Provisioning automatically creates six links with full mesh topology. With hub and spoke topology, however, Prime Provisioning creates only three links.

Step 3 Click **Add Link**.

Step 4 Specify the N-PE/PE-AGG/U-PE endpoints, as covered in the following steps.

Step 5 Click **Select U-PE/PE-AGG/N-PE** in the U-PE/PE-AGG/N-PE column.

The Select PE Device window appears.

This window displays the list of currently defined PEs.

- a. The **Show PEs with** drop-down list shows PEs by customer name, by site, or by device name.
- b. The **Find** button allows a search for a specific PE or a refresh of the window.
- c. The **Rows per page** drop-down list allows the page to be set to 5, 10, 20, 30, 40, or All.

Step 6 In the **Select** column, choose the PE device name for the L2VPN link.

Step 7 Click **Select**.

The L2VPN Service Request Editor window appears displaying the name of the selected PE in the N-PE/PE-AGG/U-PE column.

Step 8 Choose the UNI interface from the interface picker.



Note When you provision an L2VPN ERS (EVPL) service, when you choose a UNI for a particular device, Prime Provisioning determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.



Note Prime Provisioning only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.


Step 9 If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column.

The Select NPC window appears.

If only one NPC exists for the Chosen PE and PE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly.





Note If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

- Step 10** Choose the name of the NPC from the **Select** column.
- Step 11** Click **OK**.
- Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.
- Step 12** If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column.
- The Select NPC Details window appears and lists the circuit details for this NPC.
- Step 13** After you specify all the PEs, Prime Provisioning creates the links between PEs based on the Topology that you chose.
- Step 14** Click **OK**.
- For ERS (EVPL), ATM, and Frame Relay, the EndToEndWire window appears.
- Step 15** The VPN for this service request appears in the Select VPN field.
- If there is more than one VPN, click **Select VPN** to choose a VPN.
- Step 16** Specify remaining items in the EndToEnd Wire window, as necessary for your configuration:
- You can choose any of the **blue** highlighted values to edit the end-to-end wire.
 - You can edit the AC link attributes to change the default policy settings. After you edit these fields, the **blue** link changes from Default to Changed. For more information, see the section [Modifying the EVC Service Request, page 3-54](#).
 - You can also click **Add Link** to add an end-to-end wire.
 - You can click **Delete Link** to delete an end-to-end wire.
-  **Note** If you are attempting to decommission a service request to which a template has been added, see [Decommissioning Service Requests, page 8-12](#), for information on the proper way to do this.
- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.
 - You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.
 - The ID number is system-generated identification number for the circuit.
 - The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.
- Step 17** When you are finished editing the end-to-end wires, click **Save**.
- The service request is created and saved into Prime Provisioning.

Creating an EWS (EPL) L2VPN Service Request without a CE

This section includes detailed steps for creating an L2VPN service request without a CE present for EWS (EPL). If you are creating an L2VPN service request for an ERS (EVPL), ATM, or Frame Relay policy, see [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request without a CE, page 3-125](#).

-
- Step 1** Create the L2VPN service request for EWS (EPL) without a CE.
The L2VPN Service Request Editor window appears.
- Step 2** Click **Select VPN** to choose a VPN for use with this PE.
The Select VPN window appears with the VPNs defined in the system.
- Step 3** Choose a **VPN Name** in the Select column.
- Step 4** Click **Select**.
The EndToEndWire window appears with the VPN name displayed.
- Step 5** Click **Add AC** in the Attachment Circuit 1(AC1) column.
The Customer and Link Selection window appears.
- Step 6** Click **Select N-PE/PE-AGG/U-PE** in the N-PE/PE-AGG/U-PE column.
The Select PE Device window appears.
This window displays the list of currently defined PEs.
- a. From the **Show PEs with** drop-down list, you can display PEs by Customer Name, by Site, or by Device Name.
 - b. You can use the **Find** button to either search for a specific PE, or to refresh the display.
 - c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.
- Step 7** In the Select column, choose a PE for the L2VPN link.
- Step 8** Click **Select**.
The Customer and Link Selection window appears.
- Step 9** Choose a PE interface from the interface picker.
-
-  **Note** Prime Provisioning only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.
-
- Step 10** If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled. In this case, skip to Step 13.
- Step 11** If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column.
The Select NPC window appears.
-
-  **Note** If only one NPC exists for the Chosen PE and PE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly.
-
- Step 12** If applicable, choose the name of the NPC from the Select column.
- Step 13** Click **OK**.

**Note**

Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.

Step 14 Click **OK**.

The L2VPN Service Request window appears displaying the name of the selected PE in the Attachment Circuit1 (AC1) column.

Step 15 Click the **Edit** link in the AC1 Attributes and edit the attributes, if desired.

For more information, see the section [Modifying the EVC Service Request, page 3-54](#).

Step 16 Repeat Steps 5 through 14 for Attachment Circuit2.**Step 17** Specify remaining items in the EndToEndWire window, as necessary for your configuration.

- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.
- You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.
- The ID number is system-generated identification number for the circuit.
- The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 18 Click **Save**.

The EWS (EPL) service request is created and saved in Prime Provisioning.

Modifying the L2VPN Service Request

This section describes how to edit the L2VPN service request attributes. This is also where you can associate templates and data files to devices that are part of the attachment circuits.

Perform the following steps.

Step 1 Choose **Operate > Service Request Manager**.

The L2VPN Service Request window appears.

Step 2 Check a check box for a service request.**Step 3** Click **Edit**.

The EndToEndWire window appears.

Step 4 Modify any of the attributes, as desired:

- The VPN for this service request appears in the Select VPN field. If this request has more than one VPN, click **Select VPN** to choose a VPN.
- You can choose any of the [blue](#) highlighted values to edit the end-to-end wire.

- You can edit the AC link attributes to change the default policy settings. After you edit these fields, the [blue](#) link changes from Default to Changed.
- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.
- You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.
- The Circuit ID is created automatically, based on the VLAN data for the circuit.
- If the policy was set up for you to define a VC ID manually, enter it into the empty **VC ID** field. If policy was set to “auto pick” the VC ID, Prime Provisioning will supply a VC ID, and this field will not be editable. In the case where you supply the VC ID manually, if the entered value is in the provider’s range, Prime Provisioning validates if the entered value is available or allocated. If the entered value has been already allocated, Prime Provisioning generates an error message saying that the entered value is not available and prompts you to re-enter the value. If the entered value is in the provider’s range, and if it is available, then it is allocated and is removed from the VC ID pool. If the entered value is outside the provider’s range, Prime Provisioning displays a warning saying that no validation could be performed to verify if it is available or allocated.
- You can also click **Add Link** to add an end-to-end wire.
- You can click **Delete Link** to delete an end-to-end wire.



Note If you are attempting to decommission a service request to which a template has been added, see [Decommissioning Service Requests, page 8-12](#) for information on the proper way to do this.

- The ID number is system-generated identification number for the circuit.
- The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 5 To edit AC attributes, click the **Default** link in the appropriate AC Attributes column.

The Link Attributes window appears.

Step 6 Edit any of the link attributes, as desired.

Step 7 To add a template and data file to an attachment circuit, choose a Device Name, and click **Add** under Templates.

The Add/Remove Templates window appears.




Note To add a template to an attachment circuit, you must have already created the template. For detailed steps to create templates, see [Overview, page 9-1](#). For more information on how to use templates and data files in service requests, see [Chapter 9, “Managing Templates and Data Files.”](#)

Step 8 Click **Add**.

The Template Data File Chooser window appears.

Step 9 In the left pane, navigate to and select a template.

The associated data files are listed in rows in the main window.

- Step 10** Check the data file that you want to add and click **Accept**.
The Add/Remove Templates window appears with the template displayed.
- Step 11** Choose a Template name.
- Step 12** Under Action, use the drop-down list and choose **APPEND** or **PREPEND**.
Append tells Prime Provisioning to append the template generated CLI to the regular Prime Provisioning (non-template) CLI. Prepend is the reverse and does not append the template to the Prime Provisioning CLI.
- Step 13** Choose **Active** to use this template for this service request.
If you do not choose Active, the template is not used.
- Step 14** Click **OK**.
The Link Attributes with the template added appears.
-  **Note** For more information about using templates and data files in service requests, see [Chapter 9, “Managing Templates and Data Files.”](#)
- Step 15** Click **OK**.
The L2VPN Service Request window appears showing the link in the AC Attachment Circuit column has changed from Default to Changed.
- Step 16** When you are finished editing the end-to-end wires, click **Save**.

Saving the L2VPN Service Request

To save an L2VPN service request, perform the following steps.

- Step 1** When you are finished specifying the link attributes for all the attachment circuits, click **Save** to finish the L2VPN service request creation.
If the L2VPN service request is successfully created, you will see it listed in the Service Request Manager window. The newly created L2VPN service request is added with the state of REQUESTED.
- Step 2** If, however, the L2VPN service request creation failed for some reason (for example, a value chosen is out of bounds), you are warned with an error message. In such a case, you should correct the error and save the service request again.

For information on deploying L2VPN service requests, see [Deploying Service Requests, page 8-9](#).

Creating a VPLS Policy

This section contains the basic steps to create a VPLS policy. It contains the following subsections:

- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Defining an Ethernet ERS \(EVPL\) Policy with a CE, page 3-94](#)

- [Defining an MPLS/ERMS \(EVP-LAN\) Policy without a CE, page 3-136](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy with a CE, page 3-139](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy without a CE, page 3-143](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy with a CE, page 3-147](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy without a CE, page 3-150](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy with a CE, page 3-153](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy without a CE, page 3-156](#)

Defining a VPLS Policy

You must define a VPLS policy before you can provision a service. A VPLS policy defines the common characteristics shared by the Attachment Circuit (AC) attributes.

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is *not* set to editable, the service request creator cannot change the policy item.

You can also associate Prime Provisioning templates and data files with a policy. See [Chapter 9, “Managing Templates and Data Files”](#) for more about using templates and data files in policies.

It is also possible to create user-defined attributes within a policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#)

VPLS policies correspond to the one of the core types that VPLS provides:

- MPLS core type—provider core network is MPLS enabled
- Ethernet core type—provider core network uses Ethernet switches

and to one of the service types that VPLS provides:

- Ethernet Relay Multipoint Service (ERMS). The Metro Ethernet Forum name for ERMS is Ethernet Virtual Private LAN (EVP-LAN). For more information about terms used to denote VPLS services in this guide, see the section “Layer 2 Terminology Conventions” in the L2VPN Concepts chapter in the *Cisco Prime Provisioning 6.3 Administration Guide*.
- Ethernet Multipoint Service (EMS). The MEF name for EMS is Ethernet Private LAN (EP-LAN).

A policy is a template of most of the parameters needed to define a VPLS service request. After you define it, a VPLS policy can be used by all the VPLS service requests that share a common set of characteristics.

You create a new VPLS policy whenever you create a new type of service or a service with different parameters. VPLS policy creation is normally performed by experienced network engineers.

To define a VPLS policy in the Prime Provisioning, perform the following steps.

-
- Step 1** Choose **Service Design > Create Policy**.
The Policy Editor window appears.
- Step 2** Choose **VPLS** from the Policy Type drop-down list.
The Policy Editor window appears.
- Step 3** Enter a **Policy Name** for the VPLS policy.

Step 4 Choose the **Policy Owner** for the VPLS policy.

There are three types of VPLS policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this VPLS policy.

This ownership has relevance when the Prime Provisioning Role-Based Access Control (RBAC) comes into play. For example, a VPLS policy that is customer owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 5 Click **Select** to choose the owner of the VPLS policy.

The policy owner was established when you created customers or providers during Prime Provisioning setup. If the ownership is global, the Select function does not appear.

Step 6 Choose the **Core Type** of the VPLS policy.

There are two core types for VPLS policies:

- MPLS—running on an IP network
- Ethernet—all PEs are on an Ethernet provider network

Step 7 Choose the **Service Type** of the VPLS policy.

There are two service types for VPLS policies:

- Ethernet Relay Multipoint Service (ERMS). (The MEF name for ERMS is EVP-LAN.)
- Ethernet Multipoint Service (EMS). (The MEF name for EMS is EP-LAN.)

Step 8 Check the **CE Present** check box if you want Prime Provisioning to ask the service operator who uses this VPLS policy to provide a CE router and interface during service activation.

The default is CE present in the service.

If you do not check the **CE Present** check box, Prime Provisioning asks the service operator, during service activation, only for the PE router and customer-facing interface.

Defining an MPLS/ERMS (EVP-LAN) Policy with a CE

This section describes how to define a VPLS policy with an MPLS core type and an ERMS (EVP-LAN) service type with CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.

Step 2 For Core Type, choose **MPLS**.

Step 3 For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.

Step 4 Check the **CE Present** check box.

Step 5 Click **Next**.

The Interface Type window appears.

Step 6 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a CE, N-PE, PE-AGG, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 7 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 8 Choose a CE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

Step 9 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 10 Check **UNI Shutdown** box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 13 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Choose a **Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

Step 19 Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 24 Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 25 Check the **UNI Port Security** check box if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.

- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses. Click the **Edit** button to enter the addresses.

Step 26 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.



Note

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an MPLS/ERMS (EVP-LAN) Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an ERMS (EVP-LAN) service type without a CE present.

Perform the following steps.

- Step 1** In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.
- Step 2** For Core Type, choose **MPLS**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.
- Step 4** Uncheck the **CE Present** check box.
- Step 5** Click **Next**.

The Interface Type window appears.

Step 6 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 7 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 8 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 9 Choose a CE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

Step 10 Check **UNI Shutdown** box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 13 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Choose a **Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

Step 19 Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 24 Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 25 Check the **UNI Port Security** check box if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.

- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 26 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.



Note

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an MPLS/EMS (EP-LAN) Policy with a CE

This section describes defining a VPLS policy with an MPLS core type and an EMS (EP-LAN) service type with CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.

Step 2 For Core Type, choose **MPLS**.

Step 3 For Service Type, choose **Ethernet Multipoint Service (EMS)**.

Step 4 Check the **CE Present** check box.

Step 5 Click **Next**.

The Interface Type window appears.

Step 6 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 7 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 8 Choose a CE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**



Note

When creating a service request based on the MPLS/EMS (EP-LAN) with CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

Step 9 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 10 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 13 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

- Step 14** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

- Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

- Step 19** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

- Step 20** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the **Failed Deploy** state because this size is not accepted, you must adjust the size until the service request is deployed.

Prime Provisioning supports ranges for different platforms, as specified below. The range is 1500 to 9216.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Prime Provisioning uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

- Step 21** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

- Step 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

- Step 24** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 25** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.
- Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.
- Step 26** Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.
- For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:
- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
 - CDP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
 - Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
 - VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
 - Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
 - STP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
 - Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an MPLS/EMS (EP-LAN) Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an EMS (EP-LAN) service type without a CE present.

Perform the following steps.

Step 1 In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.

Step 2 For Core Type, choose **MPLS**.

Step 3 For Service Type, choose **Ethernet Multipoint Service (EMS)**.

Step 4 Uncheck the **CE Present** check box.

Step 5 Click **Next**.

The Interface Type window appears.

Step 6 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a N-PE, U-PE, or PE-AGG interface based on the service provider’s POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**

- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 7 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 8 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 9 Choose a N-PE/U-PE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**



Note

When creating a service request based on the MPLS/EMS (EP-LAN) without CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

Step 10 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 13 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 16 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 17 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

Step 18 Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 19 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 20 Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the **Failed Deploy** state because this size is not accepted, you must adjust the size until the service request is deployed.

Prime Provisioning supports, ranges for different platforms, as specified below. The range is 1500 to 9216.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Prime Provisioning uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 24 Check the **UNI Port Security** check box if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

- Step 25** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.
- Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.
- Step 26** Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.
- For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:
- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
 - CDP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
 - Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
 - VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
 - Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
 - STP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
 - Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

- Step 27** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

- Step 28** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an Ethernet/ERMS (EVP-LAN) Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERMS (EVP-LAN) service type with CE present.

Perform the following steps.

-
- Step 1** In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.
- Step 4** Check the **CE Present** check box.
- Step 5** Click **Next**.
- The Interface Type window appears.
- Step 6** Choose an **Interface Type** from the drop-down list.
- You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider’s POP design. The interfaces are:
- **ANY** (Any interface can be chosen.)
 - **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
 - **Ethernet**
 - **FastEthernet**
 - **GE-WAN**
 - **GigabitEthernet**
 - **TenGigabitEthernet**
 - **TenGigE**
- The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.
- Step 7** Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).
- This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.
- Step 8** Choose a CE **Encapsulation** type.
- The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

Step 9 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 10 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 13 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Choose a **Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

Step 19 Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

- Step 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

- Step 24** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

- Step 25** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

- Step 26** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

- Step 27** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

- Step 28** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an Ethernet/ERMS (EVP-LAN) Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERMS (EVP-LAN) service type without a CE present.

Perform the following steps.

-
- Step 1** In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.
- Step 4** Uncheck the **CE Present** check box.
- Step 5** Click **Next**.
- The Interface Type window appears.
- Step 6** Choose an **Interface Type** from the drop-down list.
- You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider’s POP design. The interfaces are:
- **ANY** (Any interface can be chosen.)
 - **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
 - **Ethernet**
 - **FastEthernet**
 - **GE-WAN**
 - **GigabitEthernet**
 - **TenGigabitEthernet**
 - **TenGigE**
- The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.
- Step 7** Check the **Standard UNI Port** check box to enable port security.
- This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.
- Step 8** Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).
- This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.

Step 9 Choose a CE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, Prime Provisioning shows another field for the UNI port type.

Step 10 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 13 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Choose a **Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

Step 19 Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note**

Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 24 Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 25 Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 26 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an Ethernet/EMS (EP-LAN) Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an EMS (EP-LAN) service type with a CE present.

Perform the following steps.

-
- Step 1** In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.
- Step 4** Check the **CE Present** check box.
- Step 5** Click **Next**.
- The Interface Type window appears.
- Step 6** Choose an **Interface Type** from the drop-down list.
- You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider’s POP design.
- The interfaces are:
- **ANY** (Any interface can be chosen.)
 - **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
 - **Ethernet**
 - **FastEthernet**
 - **GE-WAN**
 - **GigabitEthernet**
 - **TenGigabitEthernet**
- The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.
- Step 7** Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).
- This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.
- Step 8** Choose a CE **Encapsulation** type.
- The choices are:

- **DOT1Q**
- **DEFAULT**

**Note**

When creating a service request based on the Ethernet/EMS (EP-LAN) with CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

- Step 9** Check the **Standard UNI Port** check box to enable port security.
- This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.
- Step 10** Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.
- Step 11** Check the **Keep Alive** check box to configure keepalives on the UNI port.
- By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.
- Step 12** Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 13** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).
- This check box is checked by default.
- Step 14** Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.
- This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.
- Step 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.
- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID.
- If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 19** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.
- The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.
- Step 20** Enter the **System MTU** in bytes.
- The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.
- In Cisco Prime Provisioning 6.3, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Cisco Prime Provisioning 6.3 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 21 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 22 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 23 Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 24 Check the **UNI Port Security** check box if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- For **Aging**, enter the length of time the MAC address can stay on the port security table.
- For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Step 25 Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Step 26 Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- CDP Threshold**—Enter the number of packets per second to be received before the interface is shut down.

- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **STP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.



Note

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.



Note

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Defining an Ethernet/EMS (EP-LAN) Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an EMS (EP-LAN) service type without a CE present. Perform the following steps.

- Step 1** In the Service Information window of the Policy Editor, choose **VPLS** for the Policy Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.

Step 4 Uncheck the **CE Present** check box.

Step 5 Click **Next**.

The Interface Type window appears.

Step 6 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 7 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 8 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 9 Choose a N-PE/U-PE **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**



Note

When creating a service request based on the Ethernet/EMS (EP-LAN) without CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

Step 10 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 11 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 12 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 13** Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 14** Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

- Step 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

- Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Provisioning to choose a VLAN ID. If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

- Step 19** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

- Step 20** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. Prime Provisioning does not perform an integrity check for this customized value. If a service request goes to the **Failed Deploy** state because this size is not accepted, you must adjust the size until the service request is deployed. Prime Provisioning supports ranges for different platforms, as specified below. The range is 1500 to 9216.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, Prime Provisioning uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

- Step 21** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and Prime Provisioning automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note Prime Provisioning does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

- Step 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

- Step 24** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 25** Check the **Enable Storm Control** check box to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.
- Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.
- Step 26** Check the **Protocol Tunnelling** check box if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.
- For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:
- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
 - CDP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
 - Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
 - VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
 - Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
 - STP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
 - stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
 - Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Using Templates with Service Requests, page 9-24](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Note**

An additional window appears the policy workflow before the Template Association window. This window allows you to create user-defined attributes within the policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#) If you are not using this feature, click **Next** to proceed to the Template Association window, or else click **Finish** to save the policy.

Step 28 Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Managing a VPLS Service Request

This section contains the basic steps to provision a VPLS service. It contains the following subsections:

- [Configuring Device Settings to Support Prime Provisioning, page 3-7](#)
- [Creating an EVC Service Request, page 3-36](#)
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request with a CE, page 3-122](#)
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request without a CE, page 3-125](#)
- [Modifying the VPLS Service Request, page 3-165](#)
- [Using the Bridge Domain ID Attribute, page 3-166](#)
- [Saving the EVC Service Request, page 3-55](#)

Introducing VPLS Service Requests

A VPLS service request consists of one or more attachment circuits, connecting various sites in a multipoint topology. When you create a service request, you enter several parameters, including the specific interfaces on the CE and PE routers and UNI parameters.

You can also associate Prime Provisioning templates and data files with a service request. See [Chapter 9, “Managing Templates and Data Files”](#) for more about using templates and data files in service requests.

It is also possible to create user-defined attributes within a policy (and service requests based on the policy). For background information on how to use the additional information feature, see [Appendix F, “Adding Additional Information to Services.”](#)

To create a service request, a service policy must already be defined, as described in [Creating a VPLS Policy, page 3-131](#). Based on the predefined VPLS policy, an operator creates a VPLS service request, with or without modifications to the VPLS policy, and deploys the service. The service request must be the same service type (ERMS/EVP-LAN or EMS/EP-LAN) as the policy selected. Service creation and deployment are normally performed by regular network technicians for daily operation of network provisioning.

The following steps are involved in creating a service request for Layer 2 connectivity between customer sites:

- Choose a VPLS policy.
- Choose a VPN. For more information, see [Defining VPNs, page 3-9](#).
- Add a link.
- Choose a CE or UNI interface.
- Choose a Named Physical Circuit (NPC) if more than one NPC exists from the CE or the UNI interface.
- Edit the link attributes.

For sample configlets for VPLS scenarios, see [Sample Configlets, page 3-177](#).

Creating a VPLS Service Request

To create a VPLS service request, perform the following steps.

-
- Step 1** Choose **Operate > Create Service Request**.
The Service Request Editor window appears.
- Step 2** From the policy picker, choose a VPLS policy from the policies previously created (see [Creating a VPLS Policy, page 3-131](#)).
The L2VPN Service Request editor window appears.
The new service request inherits all the properties of that VPLS policy, such as all the editable and noneditable features and preset parameters.
- Step 3** To continue creating a VPLS service request, go to one of the following sections:
- [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request with a CE, page 3-122](#).
 - [Creating an ERS \(EVPL\), ATM, or Frame Relay L2VPN Service Request without a CE, page 3-125](#).
-

Creating a VPLS Service Request with a CE

This section includes detailed steps for creating a VPLS service request with a CE present. In this example, the service request is for an VPLS policy over an MPLS core with an ERMS (EVP-LAN) service type and CE present.

Perform the following steps.

-
- Step 1** Choose the appropriate VPLS policy.
The Edit VPLS Link window appears.

Step 2 Click **Select VPN** to choose a VPN for use with this CE.

The Select VPN window appears with the VPNs defined in the system. Only VPNs with the same service type (ERMS/EVP-LAN or EMS/EP-LAN) as the policy you chose appear.



Note

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this check box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

Step 3 Choose a **VPN Name** in the Select column.

Step 4 Click **Select**.

The Edit VPLS Link window appears with the VPN name displayed.

Step 5 Click **Add Link**.

The window updates, allowing you specify the CE endpoints.

Step 6 You can enter a description for the service request in the **Description** field.

The description will show up in this window and also in the Description column of the VPLS Service Requests window. The maximum length for this field is 256 characters.

Step 7 Click **Select CE** in the CE column.

The Select CPE Device window appears.

This window displays the list of currently defined CEs.

- a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.
- b. You can use the **Find** button to either search for a specific CE, or to refresh the display.
- c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Step 8 In the Select column, choose a CE for the VPLS link.

Step 9 Click **Select**.

The Edit VPLS Link window appears displaying the name of the selected CE in the CE column.

Step 10 Choose the CE interface from the interface picker.



Note

When you provision an ERMS (EVP-LAN) service (and when you choose a UNI for a particular device), Prime Provisioning determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

Step 11 Click **Select one circuit** in the Circuit Selection column.

The Select NPC window appears. If only one NPC exists for the chosen CE and CE interface, that NPC is automatically populated in the Circuit Selection column and you need not choose it explicitly.

Step 12 Choose the name of the NPC from the Select column.

Step 13 Click **OK**.

Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.

- Step 14** If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC.
- Step 15** The Circuit ID is created automatically, based on the VLAN data for the circuit.
- Step 16** To edit values that were set by the VPLS policy, that is, the values that were marked “editable” during the VPLS policy creation, click the **Edit** link in the Link Attributes column for a link. The Edit VPLS window appears.

**Note**

For more information on setting attributes in this window, see [Modifying the EVC Service Request, page 3-54](#).

**Note**

For information on the Bridge Domain ID attribute, which shows up in some VPLS service request scenarios, see [Modifying the VPLS Service Request, page 3-165](#).

- Step 17** Continue to specify additional CEs, as in previous steps, if desired.
- Step 18** Click **OK**.
- Step 19** Click **Save**.

The service request is created and saved into Prime Provisioning.

Creating a VPLS Service Request without a CE

This section includes detailed steps for creating a VPLS service request without a CE present. In this example, the service request is for an VPLS policy over an MPLS core with an EMS (EP-LAN) service type and no CE present.

Perform the following steps.

- Step 1** Choose the appropriate VPLS policy. The Edit VPLS Link window appears.
- Step 2** Click **Select VPN** to choose a VPN for use with this PE. The Select VPN window appears with the VPNs defined in the system. Only VPNs with the same service type (ERMS/EVP-LAN or EMS/EP-LAN) as the policy you chose appear.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Provisioning will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this check box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see [Setting Up Logical Inventory, page 2-53](#).

- Step 3** Choose a **VPN Name** in the Select column.

Step 4 Click **Select**.

The Edit VPLS Link window appears with the VPN name displayed.

Step 5 Click **Add Link**.

The Edit VPLS Link window updates, allowing you specify the U-PE/PE-AGG/U-PE endpoints. You can add one or more links in the window.

Step 6 You can enter a description for the service request in the first **Description** field.

The description will show up in this window and also in the Description column of the VPLS Service Requests window. The maximum length for this field is 256 characters.

Step 7 Click **Select N-PE/PE-AGG/U-PE** in the N-PE/PE-AGG/U-PE column.

The Select PE Device window appears.

This window displays the list of currently defined PEs.

- a. The **Show PEs with** drop-down list shows PEs by customer name, by site, or by device name.
- b. The **Find** button allows a search for a specific PE or a refresh of the window.
- c. The **Rows per page** drop-down list allows the page to be set to 5, 10, 20, 30, 40, or All.

Step 8 In the **Select** column, choose the PE device name for the VPLS link.**Step 9** Click **Select**.

The Edit VPLS Link window appears displaying the name of the selected N-PE/PE-AGG/U-PE in the N-PE/PE-AGG/U-PE column

Step 10 Choose the UNI interface from the interface picker.**Note**

When you provision an ERMS (EVP-LAN) service (and when you choose a UNI for a particular device), Prime Provisioning determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

Step 11 If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column.

The Select NPC window appears. If only one NPC exists for the chosen PE and PE interface, that NPC is automatically populated in the Circuit Selection column and you need not choose it explicitly.

**Note**

If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

Step 12 Choose the name of the NPC from the **Select** column.**Step 13** Click **OK**.

Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection**. This means that you do not have to further specify the PE to complete the link.

Step 14 If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column.

The NPC Details window appears and lists the circuit details for this NPC.

The Circuit ID is created automatically, based on the VLAN data for the circuit.

Step 15 To edit values that were set by the VPLS policy, that is, the values that were marked “editable” during the VPLS policy creation, click the **Edit** link in the Link Attributes column for a link.

**Note**

For more information on setting attributes in this window, see [Modifying the EVC Service Request, page 3-54](#).

**Note**

For information on the Bridge Domain ID attribute, which shows up in some VPLS service request scenarios, see [Modifying the VPLS Service Request, page 3-165](#).

Step 16 Continue to specify additional PEs, as in previous steps, if desired.

Step 17 Click **Save**.

The VPLS service request is created and saved into Prime Provisioning.

Modifying the VPLS Service Request

You can modify a VPLS service request if you must change or modify the VPLS links. This is also where you can associate templates and data files to a link.

Perform the following steps.

Step 1 Choose **Operate > Service Request Manager**.

Step 2 Check a check box for a service request.

Step 3 Click **Edit**.

The Edit VPLS Link window appears.

Step 4 Specify items in the window as necessary for your configuration:

- Choose any of the [blue](#) highlighted values to edit the VPLS links.
- Click **Add Link** to add a VPLS link.
- Click **Delete Link** to delete a VPLS link.

**Note**

If you are attempting to decommission a service request to which a template has been added, see [Decommissioning Service Requests, page 8-12](#), for information on the proper way to do this.

- You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.
- The Circuit ID is created automatically, based on the VLAN data for the circuit.

Step 5 To modify the link attributes, click **Edit** in the Link Attributes column as shown in the VPLS link editor. The Edit VPLS window appears.

Step 6 Edit the link attributes as desired.

**Note**

If you did not choose **VLANI D AutoPick** in the VPLS policy, you are prompted to provide the VLAN in a **Provider VLAN ID** field.

**Note**

For information on the Bridge Domain ID attribute, which shows up in some VPLS service request scenarios, see [Modifying the VPLS Service Request, page 3-165](#).

- Step 7** To add a template and data file to a link, choose a Device Name, and click the **Add** link in the Templates column.

The Add/Remove Templates window appears.

**Note**

To add a template to a link, you must have already created the template. For detailed steps to create templates, see [Overview, page 9-1](#). For more information on how to use templates and data files in service requests, see [Chapter 9, “Managing Templates and Data Files.”](#)

- Step 8** Click **Add**.

The Template Data File Chooser window appears.

- Step 9** In the left pane, navigate to and select a template.

The associated data files are listed in rows in the main window.

- Step 10** Check the data file that you want to add and click **Accept**.

The Add/Remove Templates window appears with the template displayed.

- Step 11** Choose a Template name.

- Step 12** Under Action, use the drop-down list and choose **APPEND** or **PREPEND**.

Append tells Prime Provisioning to append the template generated CLI to the regular Prime Provisioning (non-template) CLI. Prepend is the reverse and does not append the template to the Prime Provisioning CLI.

- Step 13** Choose Active to use this template for this service request.

If you do not choose Active, the template is not used.

- Step 14** Click **OK**.

The Edit VPLS window appears with the template added.

- Step 15** Click **OK**.

The Edit VPLS Link window appears.

- Step 16** When you are finished editing the VPLS links, click **Save**.

Using the Bridge Domain ID Attribute

The Bridge Domain ID attribute appears in the Link Attributes window of some VPLS service request scenarios.

To use the Bridge Domain ID attribute, enter an ID number in the **Bridge Domain ID** text field to enable bridge domain functionality for the VPLS service request.

Acceptable values are 1 to 4294967295.

Usage notes:

- The Bridge Domain ID attribute is only available for the following service request scenarios:

- Ethernet/ERMS (EVP-LAN) with a CE
- Ethernet/ERMS (EVP-LAN) without a CE
- Ethernet/EMS (EP-LAN) with a CE
- Ethernet/EMS (EP-LAN) without a CE
- The Bridge Domain ID attribute is only supported for the Cisco GSR 12406 running IOS 12.0(32)SY6 and functioning in an N-PE role. This attribute will show up in a service request only for this platform; otherwise, the attribute will be filtered from the Link Attributes window of the service request.
- The following points apply to service requests based on this policy:
 - When an N-PE (GSR platform) is used as a UNI device, the standard UNI attributes are not displayed in the Link Attributes window of the service request workflow.
 - When a U-PE (non-GSR platform) is used as a UNI device, all standard UNI attributes are displayed in the Link Attributes window of the service request workflow.
 - For VPLS EMS services, a U-PE (non-GSR platform) should be used in the same circuit which is terminating on a GSR device (N-PE). In other words, an NPC circuit should be used to provision VPLS EMS on GSR devices.

Saving the VPLS Service Request

To save a VPLS service request, perform the following steps.

-
- Step 1** When you are finished setting all the attributes for the attachment circuits, click **Save** to finish the VPLS service request creation.
- If the VPLS service request is successfully created, you will see a list of service requests in the Service Request Manager window. The newly created VPLS service request is added with the state of REQUESTED.
- Step 2** If, however, the VPLS service request creation failed for some reason (for example, a value chosen is out of bounds), you are warned with an error message.
- In such a case, you should correct the error and save the service request again.
-

Deploying, Monitoring, and Auditing Service Requests

To apply L2VPN, VPLS, or EVC policies to network devices, you must deploy the service request. When you deploy a service request, Prime Provisioning compares the device information in the Repository (the Prime Provisioning database) with the current device configuration and generates a configlet. Additionally, you can perform various monitoring and auditing tasks on service requests. These common tasks that apply to all types of Prime Provisioning service requests are covered in [Chapter 8, “Managing Service Requests.”](#) See that chapter for more information on these tasks.

This section covers specific issues related to managing service request tasks for EVC, L2VPN and VPLS services.

Pre-Deployment Changes

You can change the Dynamic Component Properties Library (DCPL) parameter **actionTakenOnUNIVlanList** before you deploy an EVC, L2VPN, or VPLS service request. This will be necessary if the **trunk allowed vlan** list is not present on the User Network Interface (UNI).

To make this change, perform the following steps.

-
- Step 1** Choose **Administration > Hosts**.
- Step 2** Choose the host that you want to change.
- Step 3** Click **Config**.
The Host Configuration window appears.
- Step 4** In the DCPL properties panel, choose **Provisioning > Service > shared > actionTakenOnUNIVlanList**.
The Attribute details appear.
- Step 5** In the **New Value** drop-down list, choose one of the following:
- **prune** to have Prime Provisioning create the minimum VLAN list. This is the default.
 - **abort** to have Prime Provisioning stop the L2VPN or VPLS service request provisioning with the error message: **trunk allowed vlan list is absent on ERS UNI**.
 - **nochange** to have Prime Provisioning allow all VLANs.
- Step 6** Click **Set Property**.
-

Using Autodiscovery for L2 Services

All discovery steps are integrated in a discovery workflow, controlled from the Prime Provisioning GUI. This is accessed in Prime Provisioning through **Inventory > Discovery**. The following discovery features are supported:

- File-based device discovery is supported.
- Rules-based device role assignment is supported.
- Discovery progress messages and logs are viewable in the GUI to keep track of various discovery stages.
- Bulk creation of Provider, Customer, Site, and Region objects is available through an XML data file.

For detailed steps on using the autodiscovery feature in Prime Provisioning, see [Appendix E, “Inventory - Discovery.”](#)

Provisioning VPLS Autodiscovery on Devices using EVC Service Requests

This section describes how enable the VPLS autodiscovery in Prime Provisioning. It contains the following sections:

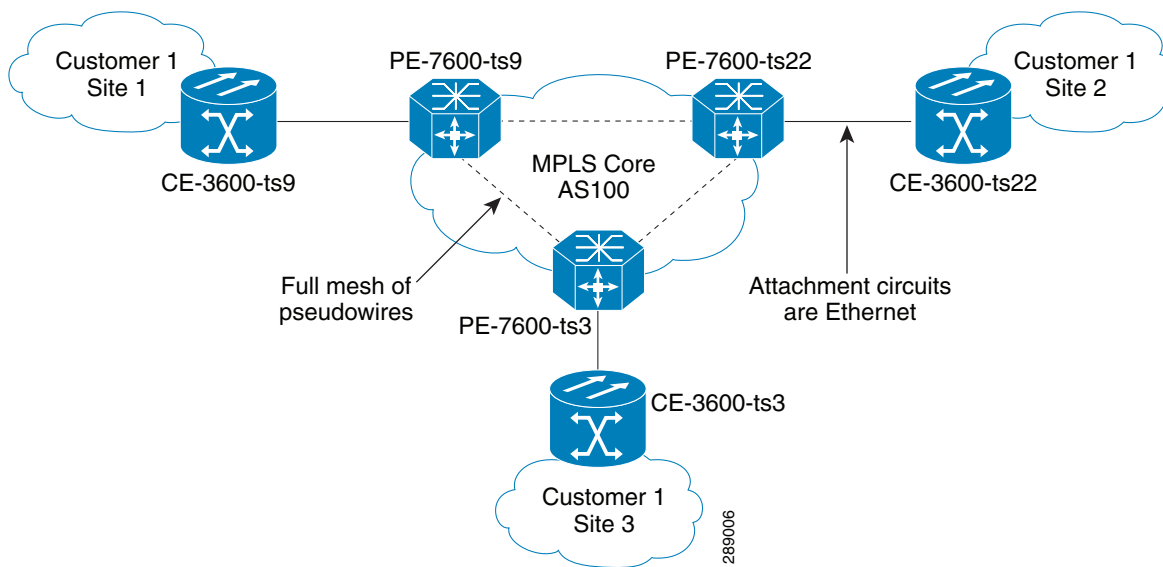
- [Overview, page 3-169](#)
- [Limitations and Restrictions for VPLS Autodiscovery, page 3-170](#)
- [Preconfiguring PE Devices to Support VPLS Autodiscovery, page 3-170](#)
- [Enabling VPLS Autodiscovery in the EVC Workflow, page 3-171](#)
- [Sample Configlets, page 3-171](#)

Overview

Earlier implementations of VPLS in IOS and IOS XR required manual configuration of each VPLS PE neighbor when devices were added or removed from the VPLS domain. VPLS auto discovery eliminates the need to manually configure the VPLS neighbors. It discovers PEs within the same VPLS domain and automatically detects when PEs are added or removed from the domain.

[Figure 3-1](#) shows an example VPLS topology that will be referenced in this section. The three PE devices constitute the neighbors in the VPLS domain. As PEs are added or removed from the domain, VPLS autodiscovery keeps the PE configurations updated.

Figure 3-1 VPLS Autodiscovery Topology Example



To provision VPLS autodiscovery on PE devices in the VPLS domain, you must perform two basic tasks:

- You must preconfigure some configlets on the devices before they are provisioned by Prime Provisioning. You must do this manually or through the use of templates. See [Preconfiguring PE Devices to Support VPLS Autodiscovery, page 3-170](#).
- You must enable VPLS autodiscovery within the EVC service request(s) used to provision the PE(s) in the VPLS domain.

The rest of this section documents limitations and restrictions of VPLS autodiscovery, describes the steps you must perform in the workflow to enable it, and provides sample configlets generated on IOS and IOS XR devices.

Limitations and Restrictions for VPLS Autodiscovery

Keep in mind the following limitations and restrictions when using VPLS autodiscovery Prime Provisioning.

- To use VPLS autodiscovery, all PE devices in the VPLS domain must be have VPLS autodiscovery enabled. Mixed topologies (that is, some PEs configured with VPLS autodiscovery enabled and some without) are not supported. The VPLS discovery mode should be enabled for all service requests under the same virtual forwarding interface (VFI).
- Some preconfiguration on the PEs in the VPLS domain is required. See [Preconfiguring PE Devices to Support VPLS Autodiscovery, page 3-170](#).
- Split horizon should be enabled for when using VPLS autodiscovery.
- VPLS autodiscovery can only be configured in Prime Provisioning using EVC Ethernet service requests for which the MPLS Core Connectivity Type is set as VPLS. The feature is not supported for other Prime Provisioning service requests and/or connectivity types.
- The same discovery mechanism must be used to build a pseudowire between two PE peers. It is not valid for both auto discovered and manually configured pseudowires in the same VFI to go to the same peer PE. For example, it is not valid for PE1 to be manually configured for PE2 and PE2 be dynamically configured to discover PE1.
- Once the VPLS discovery mode is provisioned (as manual or autodiscovery) in the service required, it cannot be modified.
- VPLS autodiscovery is only supported for full-mesh topologies, not hub and spoke topologies like hierarchical VPLS (H-VPLS).
- VPLS autodiscovery is not supported with inter-autonomous system configurations.

Preconfiguring PE Devices to Support VPLS Autodiscovery

The following configlets must be preconfigured on IOS and IOS XR devices before provisioning VPLS autodiscovery on them. The configlets are required to setup MP-iBGP peering with other PEs and to enable VPLS L2VPN community information exchange with other PEs in the same VPLS domain.

```
! 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
!
```

Enabling VPLS Autodiscovery in the EVC Workflow

To enable VPLS discovery in the EVC Ethernet workflow, perform the following steps.

-
- Step 1** In the EVC Ethernet policy or service request workflow, set the **MPLS Core Connectivity Type** to **VPLS**.
- When the core connectivity is VPLS, the Discovery Mode attribute dynamically appears in the Service Request Details section of the EVC Service Request Editor window. This window describes the VPLS connectivity between the attachment circuits. VPLS connectivity allows the creation of a multipoint connection between two customer sites, using direct connect links or L2 access links.
- Step 2** Choose the **Discovery Mode** type in the EVC Service Request Editor window.
- The choices are:
- **Manual**— When the Manual option is selected, the **vfi** command will be configured as in legacy with the **manual** option. This is the same for both IOS and IOS XR devices. The signaling protocol implemented is LDP.
 - **Auto Discovery**— When the Auto Discovery option is selected, the **vfi** command will be configured with the **autodiscovery** option, and the **neighbor** command is not required.
- For examples of the resulting configlets generated by these choices, see [Sample Configlets, page 3-171](#).
- Step 3** Save the service request and deploy it on the device(s) in the VPLS domain.
-

Sample Configlets

This section provides sample configlets generated by Prime Provisioning for both IOS and IOS XR devices for VPLS autodiscovery.

Sample Configlet for IOS Device

```
! 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
```

Sample Configlet for IOS XR Device

```
l2vpn
bridge group abc
bridge-domain east
vfi vfname
```

```
vpn-id 678
autodiscovery bgp
rd auto
route-target 456:567
```

**Note**

For IOS XR devices, the Route Target value must be saved while creating the VPN.

Setting Up VLAN Translation for L2VPN ERS (EVPL) Services

This section provide supplemental information about how to set up VLAN translation for L2VPN ERS (EVPL) services. It contains the following subsections:

- [VLAN Translation Overview, page 3-172](#)
- [Setting Up VLAN Translation, page 3-172](#) [Figure 3-1](#)
- [Platform-Specific Usage Notes, page 3-176](#)

**Note**

For helpful information to be aware of before you create policies and services using VLAN translation, review [Platform-Specific Usage Notes, page 3-176](#).

VLAN Translation Overview

VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. There are two types of VLAN translation—one is 1-to-1 translation (1:1), and the other one is 2-to-1 translation (2:1). This feature is available for L2VPN ERS (EVPL) (with and without a CE). The behavior of L2VPN ERS (EVPL) service remains the same, even though it is true that it is possible now for one Q-in-Q port to be shared by both EWS (EPL) and ERS (EVPL) service. VLAN translation is only for an Ethernet interface, not for other types of interfaces, such as ATM and Frame Relay.

With 1:1 VLAN translation, the VLAN of the incoming traffic (CE VLAN) is replaced by another VLAN (PE VLAN). It means the service provider is now able to handle the situation where incoming traffic from two different customers share the same CE VLAN. The SP can map these two CE VLANs to two different PE VLANs, and customer traffic will not be mixed.

With 2:1 VLAN translation, the double tagged (Q-in-Q) traffic at the U-PE UNI port can be mapped to different flows to achieve service multiplexing. The translation is based on the combination of the CE VLAN (inner tag) and the PE VLAN (outer tag). Without this translation, all the traffic from a Q-in-Q port can only go to one place because it is switched only by the outer tag.

Setting Up VLAN Translation

The following sections described how to create and manage policies and service requests to support VLAN translation:

- [Creating a Policy, page 3-173](#)
- [Creating a Service Request, page 3-173](#)
- [Modifying a Service Request, page 3-175](#)

- [Deleting a Service Request, page 3-175](#)

Creating a Policy

VLAN translation is specified during policy creation for L2VPN for ERS (EVPL) (with and without a CE). The L2VPN (Point to Point) Editor window contains a new option called **VLAN Translation**.

There are three options for VLAN translation:

- **No**—This is the default choice. No VLAN translation is performed.



Note If you choose **No** and you do not want to deal with any behavior related to VLAN translation during service request creation, then uncheck the **Editable** check box. This is the recommendation when you choose no VLAN translation.

- **1:1**—1:1 VLAN translation. The VLAN of the incoming traffic (CE VLAN) is replaced by another VLAN (PE VLAN). The specification of the VLAN translation is done during the creation of the service request for the policy, as covered in [Creating a Service Request, page 3-173](#).
- **2:1**—2:1 VLAN translation. The double tagged (Q-in-Q) traffic at the U-PE UNI port can be mapped to different flows to achieve service multiplexing. When you choose 2:1 VLAN translation, the L2VPN (Point to Point) Editor window dynamically changes to enable you to choose where the 2:1 VLAN translation takes place.

The choices for where 2:1 VLAN translation takes place are:

- **Auto** (This is the default choice.)
- **U-PE**
- **PE-AGG**
- **N-PE**

If you choose **Auto**, the 2:1 VLAN translation takes place at the device closest to the UNI port. The other choices come into play only when there is more than one place that 2:1 VLAN translation can be done. If there is only one place where the translation can be done, the choice is ignored.

The actual VLAN values are specified when you create a service request based on this policy. See [Creating a Service Request, page 3-173](#).

Creating a Service Request

When you create a service request based on an L2VPN ERS (EVPL) policy, the VLAN options can be changed if they were set to be editable in the policy. You can overwrite the policy information for the VLAN translation type and the place where translation occurs. This flexibility allows the following provisioning:

- One AC can have 2:1 VLAN translation, while the other AC can have no VLAN translation or 1:1 VLAN translation.
- The VLAN translation for one AC can be on the UNI box, while the translation for the other AC can be on the PE-AGG.



Note Note these modifications can happen only when a new service request is created. They are not allowed during the modification of an existing service request.

The specification of the VLAN translation happens during the creation of the service request within the Link Attributes window. At that point, you can specify which VLAN is translated to which VLAN. The Link Attributes window is accessed after the UNI port is selected on the Attachment Tunnel Editor window. Because you can set the VLAN translation type after the UNI selection, the UNI port display list does not exclude any type for the UNI port. This is because:

- The UNI port list has to include the regular trunk port, in case you later (on the Link Attributes window) decide to perform no VLAN translation or 1:1 VLAN translation.
- The UNI port list has to include an EWS (EPL) (Q-in-Q) port, in case you decide to do 2:1 VLAN translation.

Even though you have all the ports to start with for VLAN translation, you must choose specific types of ports, based on the type of VLAN translation. More specifically:

- For no VLAN translation and 1:1 VLAN translation, you must choose an empty port or a trunk port as the UNI.
- For 2:1 VLAN translation, you must choose an empty port or a Q-in-Q port as the UNI port.

To help determine the proper port to use, you can click the **Details** button on the Attachment Tunnel Editor window to display the port type and associated service with that port.

The following sections show how the VLAN translation is defined on the Link Attribute window for the different types of VLAN translation.

No VLAN Translation

When you choose no VLAN translation, no additional information needs to be provided.

1:1 VLAN Translation

When you choose 1:1 VLAN translation, the window dynamically changes.

In the empty field, you must enter which CE VLAN is to be translated from. The VLAN number must be a number from 1 to 4096.

The PE VLAN that the CE VLAN is to be translated to can be “auto picked” or manually entered. Check the **VLAN ID AutoPick** check box above (on the Link Attributes window) to have PE VLAN automatically assigned.

If you uncheck the **VLAN ID AutoPick** check box, the window displays a Provider VLAN ID, where you can manually enter the PE VLAN.

Upon completion of the service request creation, Prime Provisioning does an integrity check before saving the service request. For 1:1 VLAN translation, Prime Provisioning rejects the service request if the CE VLAN has been used for another 1:1 VLAN translation on the same port.

2:1 VLAN Translation

When choosing 2:1 VLAN translation, the window dynamically changes.



Note

If the UNI port has been provisioned with EWS (EPL) service, the outer VLAN value is grayed out.

In 2:1 VLAN translation, there are three VLANs involved:

- “A”—The CE VLAN to be translated from. You specify this in the “From CE VLAN field.” For out-of-range translation, a value of “*” (asterisk character) should be provided

- “B”—The PE VLAN that is the outer VLAN of the Q-in-Q port. You specify this in the “Outer VLAN” field. You can choose this VLAN manually by entering a value, or you can choose the **AutoPick** check box to have one automatically assigned.
- “C”—The PE VLAN that the “A” and “B” VLANs are translated to. You specify this in the “VLAN and Other Information” section above (on the Link Attributes window).

You must specify VLAN “A” (the CE VLAN) and VLAN “C” (the PE VLAN translated to). For VLAN “B” (the Q-in-Q outer VLAN), what to specify depends on the UNI port type:

- If it is an empty port, you must specify VLAN “B.”
- If it is an existing Q-in-Q port, then VLAN “B” has been defined, and it cannot be changed at this point.

Some additional comments on 2:1 VLAN translation:

- For 2:1 VLAN translation, if you build an ERS (EVPL) service on an empty port, then this UNI port will be provisioned as an ERS (EVPL) service. If you later add an EWS (EPL) service to the same port, the EWS (EPL) service will overwrite the previous ERS (EVPL) provisioning. The major difference between ERS (EVPL) and EWS (EPL) is the L2PT BPDU treatment. For ERS (EVPL), BPDU is blocked. For EWS (EPL), BPDU is tunneled.
- As an ERS (EVPL) service, the 2:1 VLAN translation can share the same port, just like a regular ERS (EVPL) port.
- An ERS (EVPL) 2:1 service can be added on top of an existing EWS (EPL) service.

Upon completion of the service request creation, Prime Provisioning does an integrity check before saving the service request. For 2:1 VLAN translation, Prime Provisioning rejects the service request if the CE VLAN and outer tag PE VLAN combination has been used for another 2:1 VLAN translation on the same port.

Modifying a Service Request

For both 1:1 and 2:1 VLAN translation, you can perform the following modifications on an existing service request:

- Change to a new CE VLAN to be translated from.
- All other normal changes for a service request are permitted.

However, the following modifications are not allowed:

- You cannot change the VLAN translation type for a given AC. For instance, you cannot change from 2:1 to 1:1 VLAN translation.
- You cannot change the place where 2:1 VLAN translation occurs.

Deleting a Service Request

During service request deletion, the following resources are released:

For 1:1 VLAN translation:

- The CE VLAN becomes available to be translated again.
- The PE VLAN is released.
- If the link being deleted is the last link on the UNI port, then this port is set to new.

For 2:1 VLAN translation:

- The CE VLAN becomes available to be translated again.

- The “translated to” PE VLAN is released.
- If the link being deleted is the last “CE-PE” pair on this UNI port, and there is no EWS (EPL) service on this port, then this port is set to new. In addition, the outer VLAN is released.

Platform-Specific Usage Notes

VLAN translation is available on 7600 and 3750 ME platforms. The 7600 and 3750 ME have different ways to support VLAN translation. Not only is the command syntax different, but so is the place where the VLAN translation is carried out. On the 7600, for 1:1 VLAN translation, the operation is done on the PFC card. For 2:1 VLAN translation, the operation is done on the uplink GE-WAN (OSM module). On the 3750 ME, however, both translations occur on the uplinks (ES ports).

VLAN Translation on the 3750

Be aware of the following points when performing VLAN translation on the 3750.

- The 3750 where VLAN translation occurs should be designated as a U-PE or PE-AGG role, not N-PE.
- VLAN translation on the up link (ES) port should be performed on the Gigabit 1/1/1 or Gigabit 1/1/2 port.
- If a 1:1 VLAN translation occurs on a ring that is made of 3750 PEs, all the 3750s use the ES port as uplink ports (the “east” and “west” ports) to connect other ring nodes.

VLAN Translation on the 7600

Be aware of the following points when performing VLAN translation on the 7600.

- 1:1 VLAN translation always occurs on the UNI port. However, not every Ethernet interface will support 1:1 VLAN translation. Such support is dependent on the line card.
- 2:1 VLAN translation always occurs on the GE-WAN port. The port must be an NNI uplink port.
- 2:1 VLAN translation only occurs on a 7600 that is a U-PE or a PE-AGG, not an N-PE. The reason is when the 2:1 VLAN translation is performed on the GE-WAN interface, this interface can no longer perform L3VPN and L2VPN service using the translated new VLAN. The L3/L2VPN service has to be provisioned on another (N-PE) box.

Failed Service Requests When Hardware Does Not Support VLAN Translation

For the 1:1 VLAN translation feature, a service request goes to the **Fail Deployed** state if the target hardware (line card) does not support the VLAN translation. The reason the service request goes to the **Fail Deployed** state instead of **Invalid** is that Prime Provisioning does not know beforehand whether a particular line card will accept or reject the VLAN translation CLI commands. In this case, Prime Provisioning attempts to push down the commands and the deployment fails. An **Invalid** status means Prime Provisioning detects something wrong (in advance) and aborts the provisioning task. No CLI is pushed down in that case. This is a general behavior of Prime Provisioning when a given hardware does not support a feature. In these cases, it is the user’s responsibility to select proper hardware to support the intended service.

Sample Configlets

This section provides sample configlets for L2VPN and Metro Ethernet service provisioning in Prime Provisioning. It contains the following subsections:

- [Overview, page 3-178](#)
- [ERS \(EVPL\) \(Point-to-Point\), page 3-179](#)
- [ERS \(EVPL\) \(Point-to-Point, UNI Port Security\), page 3-180](#)
- [ERS \(EVPL\) \(1:1 VLAN Translation\), page 3-181](#)
- [ERS \(EVPL\) \(2:1 VLAN Translation\), page 3-182](#)
- [ERS \(Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device\), page 3-183](#)
- [ERS \(EVPL\) \(NBI Enhancements for L2VPN, IOS Device\), page 3-184](#)
- [ERS \(EVPL\) or EWS \(EPL\) \(IOS XR Device\), page 3-185](#)
- [ERS \(EVPL\) and EWS \(EPL\) \(Local Connect on E-Line\), page 3-188](#)
- [ERS \(EVPL\), EWS \(EPL\), ATM, or Frame Relay \(Additional Template Variables for L2VPN, IOS and IOS XR Device\), page 3-189](#)
- [EWS \(EPL\) \(Point-to-Point\), page 3-190](#)
- [EWS \(EPL\) \(Point-to-Point, UNI Port Security, BPDU Tunneling\), page 3-191](#)
- [EWS \(EPL\) \(Hybrid\), page 3-193](#)
- [EWS \(EPL\) \(Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device\), page 3-196](#)
- [EWS \(EPL\) \(NBI Enhancements for L2VPN, IOS Device\), page 3-197](#)
- [ATM over MPLS \(VC Mode\), page 3-198](#)
- [ATM over MPLS \(VP Mode\), page 3-199](#)
- [ATM \(Port Mode, Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device\), page 3-200](#)
- [Frame Relay over MPLS, page 3-201](#)
- [Frame Relay \(DLCI Mode\), page 3-202](#)
- [VPLS \(Multipoint, ERMS/EVP-LAN\), page 3-203](#)
- [VPLS \(Multipoint, EMS/EP-LAN\), BPDU Tunneling\), page 3-204](#)
- [EVC \(Pseudowire Core Connectivity, UNI Port Security\), page 3-205](#)
- [EVC \(Pseudowire Core Connectivity, UNI, without Port Security, with Bridge Domain\), page 3-206](#)
- [EVC \(Pseudowire Core Connectivity, UNI, and Pseudowire Tunneling\), page 3-207](#)
- [EVC \(Pseudowire Core Connectivity, UNI, and Pseudowire Tunneling\), page 3-207](#)
- [EVC \(VPLS Core Connectivity, UNI Port Security\), page 3-208](#)
- [EVC \(VPLS Core Connectivity, no UNI Port Security\), page 3-209](#)
- [EVC \(Local Connect Core Connectivity, UNI Port Security\), page 3-210](#)
- [EVC \(Local Connect Core Connectivity, UNI, no Port Security, Bridge Domain\), page 3-211](#)
- [EVC \(Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI\), page 3-212](#)
- [EVC \(Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI\), page 3-213](#)
- [EVC \(No AutoPick Service Instance Name, No Service Instance Name\), page 3-215](#)

- EVC (User-Provided Service Instance Name, Pseudowire Core Connectivity), page 3-216
- EVC (User-Provided Service Instance Name, Local Core Connectivity), page 3-217
- EVC (User-Provided Service Instance Name, VPLS Core Connectivity), page 3-218
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Point-to-Point Circuit), page 3-219
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Multipoint Circuit), page 3-220
- EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit), page 3-221
- EVC (ATM-Ethernet Interworking, Local Core Connectivity, Multipoint Circuit), page 3-222
- EVC (ATM-Ethernet Interworking, Local Core Connectivity, Multipoint Circuit), page 3-223
- EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit), page 3-224
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit), page 3-225
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Multipoint Circuit), page 3-226
- EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit), page 3-227
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, with Bridge Domain), page 3-228
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, with Bridge Domain), page 3-229
- EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, no Bridge Domain), page 3-230

Overview

The configlets provided in this section show the CLIs generated by Prime Provisioning for particular services and features. Each configlet example provides the following information:

- Service
- Feature
- Devices configuration (network role, hardware platform, relationship of the devices and other relevant information)
- Sample configlets for each device in the configuration
- Comments



Note

The configlets generated by Prime Provisioning are only the delta between what needs to be provisioned and what currently exists on the device. This means that if a relevant CLI is already on the device, it does not show up in the associated configlet.



Note

The CLIs shown in bold are the most relevant commands.



Note

All examples in this section assume an MPLS core.

ERS (EVPL) (Point-to-Point)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL) (point-to-point).
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL.
Interface(s): FA8/17.
 - The U-PE is a Cisco 3750ME with 12.2(25)EY1, no port security.
Interface(s): FA1/0/4 – FA1/0/23.
 - L2VPN point-to-point.

Configlets

U-PE	N-PE
<pre> 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 bpduguard 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 </pre>	<pre> 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 </pre>

Comments

- The N-PE is a 7600 with an OSM or SIP-600 module.
- The U-PE is a generic Metro Ethernet (ME) switch. Customer BPDUs are blocked by the PACL.

ERS (EVPL) (Point-to-Point, UNI Port Security)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL) (point-to-point) with UNI port security.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, OSM. Interface(s): FA2/18.
 - The U-PE is a Cisco 3550 with IOS 12.2(25)SEC2. Port security is enabled. Interface(s): FA3/31– FA3/23.
 - L2VPN point-to-point.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> 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 </pre>

Comments

- The N-PE is a 7600 with an OSM or SIP-600 module.
- The U-PE is a generic Metro Ethernet (ME) switch. The customer BPDUs are blocked by the PACL.
- Various UNI port security commands are provisioned.
- A user-defined PACL entry is added to the default PACL.

ERS (EVPL) (1:1 VLAN Translation)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL) with 1:1 VLAN translation.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL
Interface(s): FA8/34.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. VLAN translation on the NNI port (uplink).
Interface(s): FA1/0/8 – GI1/1/1.
 - L2VPN point-to-point.

Configlets

U-PE	N-PE
<pre> ! 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 bpduguard 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 </pre>	<pre> 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 </pre>

Comments

- VLAN translation is only for L2VPN (point-to-point) ERS (EVPL).
- In this case, the 1:1 VLAN translation occurs on the U-PE, a 3750. It is provisioned on the NNI (uplink) port.
- The customer VLAN 123 is translated to the provider VLAN 778.

ERS (EVPL) (2:1 VLAN Translation)

- Configuration**

- Service: L2VPN/Metro Ethernet.
 - Feature: ERS (EVPL) with VLAN 2:1 translation. Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL
 - Interface(s): FA8/34.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. VLAN translation on the NNI port (uplink).
 - Interface(s): FA1/0/5 – GI1/1/1.
 - L2VPN point-to-point.

U-PE	N-PE
<pre> 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 </pre>	<pre> 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 </pre>

- Comments**

- VLAN translation is only for L2VPN (point-to-point) ERS (EVPL).
 - In this case, the 2:1 VLAN translation occurs on the U-PE, a 3750. It is provisioned on the NNI (uplink) port.
 - The customer VLAN 123 and the provider VLAN 234 (as part of Q -in-Q) are translated to a new provider VLAN 779.

ERS (Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL).
- Device configuration:
 - The N-PE is a CRS-1 with IOS XR 3.6.1 or later.
 - UNI on N-PE.
 - UNI on U-PE.

Configlets

U-PE	N-PE
<pre> ! vlan 700 exit ! interface FastEthernet1/0/2 switchport trunk encapsulation dot1q switchport trunk allowed vlan 700 switchport mode trunk switchport nonegotiate no keepalive mac access-group ISC-FastEthernet1/0/2 in no cdp enable spanning-tree bpdufilter enable ! ! interface GigabitEthernet1/0/1 switchport trunk encapsulation dot1q switchport trunk allowed vlan 700 switchport mode trunk keepalive 10 ! ! mac access-list extended ISC-FastEthernet1/0/2 deny any host 0100.0ccc.cccc deny any host 0100.0ccc.cccd deny any host 0100.0ccd.cdd0 deny any host 0180.c200.0000 permit any any ! </pre>	<pre> ! interface GigabitEthernet0/3/1/1.700 l2transport dot1q vlan 700 ! l2vpn pw-class PW_AD3-AD7_Customer1 encapsulation mpls transport-mode vlan preferred-path interface tunnel-te 1370 fallback disable ! ! xconnect group L2VPN_Customer1-Gold_class p2p GoldPkg_AD3-AD7_Customer1 interface GigabitEthernet0/3/1/1.700 neighbor 192.169.105.30 pw-id 1000 pw-class PW_AD3-AD7_Customer1 ! ! </pre>

Comments

- The N-PE is a CRS-1 with IOS XR 3.7.
- The pseudowire class feature is configured with various associated attributes like encapsulation, transport mode, preferred-path, and fallback option.
- The disable fallback option is required for IOS XR 3.6.1 and optional for IOS XR 3.7 and later.
- The E-Line name (**p2p** command) and L2VPN Group Name (**xconnect group** command) is user configured.

ERS (EVPL) (NBI Enhancements for L2VPN, IOS Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL).
- Device configuration:
 - The N-PE is a 12.2(18)SXF with IOS.
 - The U-PE is a 12.2(25)EY4with IOS.
 - UNI on N-PE.
 - UNI on U-PE.

Configlets

U-PE	N-PE
<pre> ! vlan 3200 exit ! interface FastEthernet1/0/2 no cdp enable no ip address duplex auto switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan none switchport trunk allowed vlan 3200 switchport nonegotiate switchport port-security aging type inactivity switchport port-security maximum 100 switchport port-security aging time 1000 switchport port-security violation protect switchport port-security storm-control unicast level 1.0 storm-control broadcast level 50.0 storm-control multicast level 50.0 shutdown keepalive spanning-tree bpdupfilter enable ! interface GigabitEthernet1/0/1 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 3200 ! </pre>	<pre> ! vlan 3300 exit ! interface FastEthernet1/0/24 no cdp enable no ip address duplex auto switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan none switchport trunk allowed vlan 3300 switchport nonegotiate switchport port-security aging type inactivity switchport port-security maximum 100 switchport port-security aging time 1000 switchport port-security violation protect switchport port-security storm-control unicast level 1.0 storm-control broadcast level 50.0 storm-control multicast level 50.0 shutdown keepalive spanning-tree bpdupfilter enable ! interface Vlan3300 no ip address xconnect 192.169.105.40 7502 encapsulation mpls no shutdown ! </pre>

Comments

None.

ERS (EVPL) or EWS (EPL) (IOS XR Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL) or EWS (EPL).
- Device configuration(s):
 - The N-PE is a CRS-1 with IOS XR 3.4.2.
 - UNI on N-PE. ERS (EVPL) only.
 - U-PE. EWS (EPL) or ERS (EVPL).

Configlets**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>

```

Comments

- In IOS XR, device configuration is specified in XML format.

- With respect to the XML schemas, different versions of IOS XR generate different XML configlets. However the configurations will be almost identical, except for changes in the XML schema.
- There are different cases to consider. For example, when a service request is decommissioned or modified, the XML configuration will slightly differ.

ERS (EVPL) and EWS (EPL) (Local Connect on E-Line)

- Configuration
- Service: L2VPN/Metro Ethernet.
 - Feature: ERS (EVPL) and EWS (EPL).
 - Device configuration:
 - The N-PE is a CRS-1 with IOS XR 3.6 or later.
 - The U-PE is a 12.2(18)SXF with IOS.

Configlets	U-PE	N-PE
		<pre>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 c1-test-12-crs1-1--0--559 interface GigabitEthernet0/0/0/2.559 interface GigabitEthernet0/0/0/4.559 ! ! !</pre>

- Comments
- The default E-Line name has changed for local connect configlets.
 - The format of the default E-line name is:
device_name_with_underscores--VCID--VLANID

ERS (EVPL), EWS (EPL), ATM, or Frame Relay (Additional Template Variables for L2VPN, IOS and IOS XR Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ERS (EVPL), EWS (EPL), ATM and Frame Relay.
- Device configuration:
 - The N-PE is a 12.2(18)SXF with IOS for ERS (EVPL), EWS (EPL), Frame Relay service.
 - The N-PE is a CRS-1 with IOS XR 3.6 or later for ERS (EVPL), EWS (EPL) service; and IOS XR 3.7 or later for ATM service (ATM port mode).
 - The U-PE is a 12.2(25)EY4 with IOS for ERS (EVPL) or EWS (EPL) service.

Configlets

U-PE	N-PE
(None)	<p>Template Content:</p> <pre>interface Loopback0 description LocalLoopbackAddress=\$L2VPNLocalLoopback LocalHostName=\$L2VPNLocalHostName RemoteLoopbackAddress=\$L2VPNRemoteLoopback RemoteHostName=\$L2VPNRemoteHostName</pre> <p>Configlets:</p> <pre>interface Loopback0 description LocalLoopbackAddress= 192.169.105.40 LocalHostName=c1-test-12-7600-2 RemoteLoopbackAddress=192.169.105.80 RemoteHostName= c1-test-12-7600-4</pre>

Comments

- These four variables are supported only on the N-PE.
- The values will be empty for all other device roles (U-PE, PE-AGG, and CE).

EWS (EPL) (Point-to-Point)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: EWS (EPL) (point-to-point).
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL.
Interface(s): FA8/17.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. No port security, no tunneling.
Interface(s): FA1/0/20 – FA1/0/23.
 - L2VPN point-to-point.
 - Q-in-Q UNI.

Configlets

U-PE	N-PE
<pre>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 bpduguard enable ! interface FastEthernet1/0/23 no ip address switchport trunk allowed vlan 774,787-788</pre>	<pre>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</pre>

Comments

- The N-PE is a 7600 with a OSM or SIP-600 module. Provisioning is the same as the ERS (EVPL) example.
- The U-PE is a generic Metro Ethernet (ME) switch.
- No PACL provisioned by default. BPDU can be tunneled if desired.
- The system MTU needs to set to 1522 to handle the extra 4 bytes of Q-in-Q frames.

EWS (EPL) (Point-to-Point, UNI Port Security, BPDU Tunneling)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: EWS (EPL) (point-to-point) with Port security, BPDU tunneling.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. No port security, with tunneling.
 - L2VPN point-to-point.
 - Q-in-Q UNI.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> 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 </pre>

Comments

- The N-PE is a 7600 with an OSM or SIP-600 module. Provisioning is the same as the ERS (EVPL) example.
- The U-PE is a generic Metro Ethernet (ME) switch.
- PACL with one user-defined entry.
- BPDUs (CDP, STP and VTP) are tunneled through the MPLS core.
- Storm control is enabled for unicast, multicast, and broadcast.

EWS (EPL) (Hybrid)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: EWS (EPL) hybrid. One side is EWS (EPL) UNI; the other side is ERS (EVPL) NNI.
- Device configuration:
 - The N-PE is a Cisco 7600 with 12.2(18)SXF, Sup720-3BXL.
Interface(s): FA8/17.
 - The U-PE is a Cisco 3750ME with 12.2(25)EY1. No port security, with tunneling.
Interface(s): FA1/0/20 – FA1/0/23.
 - L2VPN point-to-point.
 - Q-in-Q UNI.

**Note**

The first configlet example is the EWS (EPL) side (UNI). The second configlet is the ERS (EVPL) side (NNI).

Configlets (EWS)

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> 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 </pre>

Comments

- This is the EWS (EPL) side (UNI).
- N-PE is 7600 with an OSM or a SIP-600 module. Provisioning is the same as the ERS (EVPL).
- The U-PE is a generic Metro Ethernet (ME) switch.
- PACL with one user-defined entry.
- BPDUs (cdp, stp and vtp) are tunneled through the MPLS core.
- Storm control is enabled for unicast, multicast, and broadcast.

Configlets (ERS)

U-PE	N-PE
<pre> 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 </pre>	<pre> 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 </pre>

Comments

- This is the ERS (EVPL) side (NNI).
- The N-PE is a 7600 with an OSM or a SIP-600 module. Provisioning is the same as the ERS (EVPL).
- The U-PE is really a PE-AGG. It connects to the wholesale customer as an NNI. Both ports are regular NNI ports.

EWS (EPL) (Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: EWS (EPL).
- Device configuration:
 - The N-PE is a CRS-1 with IOS XR 3.6.1 or later.
 - UNI on U-PE.

Configlets

U-PE	N-PE
<pre> ! 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 bpdupfilter enable ! interface GigabitEthernet1/0/1 no ip address switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 700 switchport mode trunk ! </pre>	<pre> ! 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-12-12404-2--1000 interface GigabitEthernet0/3/1/1.700 neighbor 192.169.105.30 pw-id 1000 pw-class PW_AD7-AD3_Cutsomer2 ! </pre>

Comments

- The N-PE is a CRS-1 router with IOS XR 3.7.
- The pseudowire class feature is configured with various associated attributes like encapsulation, transport mode, preferred-path, and fallback option
- The disable fallback option is required for IOS XR 3.6.1 and optional for IOS XR 3.7 and later.
- The E-Line name (**p2p** command) and L2VPN Group Name (**xconnect group** command) is an Prime Provisioning-generated default value, if user input is not provided.

EWS (EPL) (NBI Enhancements for L2VPN, IOS Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: EWS (EPL).
- Device configuration:
 - The N-PE is a 12.2(18)SXF with IOS.
 - The U-PE is a 12.2(25)EY4with IOS.
 - UNI on N-PE.
 - UNI on U-PE.

Configlets

U-PE	N-PE
<pre> ! vlan 3201 exit ! interface FastEthernet1/0/2 no cdp enable no ip address duplex auto switchport switchport access vlan 3201 switchport mode dot1q-tunnel switchport nonegotiate switchport port-security aging type inactivity switchport port-security maximum 100 switchport port-security aging time 1000 switchport port-security violation protect switchport port-security storm-control unicast level 1.0 storm-control broadcast level 50.0 storm-control multicast level 50.0 shutdown keepalive spanning-tree bpdufilter enable ! interface GigabitEthernet1/0/1 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 3201 ! </pre>	<pre> ! vlan 3301 exit ! interface FastEthernet1/0/24 no cdp enable no ip address duplex auto switchport switchport access vlan 3301 switchport mode dot1q-tunnel switchport nonegotiate switchport port-security aging type inactivity switchport port-security maximum 100 switchport port-security aging time 1000 switchport port-security violation protect switchport port-security storm-control unicast level 1.0 storm-control broadcast level 50.0 storm-control multicast level 50.0 shutdown keepalive spanning-tree bpdufilter enable ! interface Vlan3301 no ip address xconnect 192.169.105.40 7502 encapsulation mpls no shutdown ! </pre>

Comments

None.

ATM over MPLS (VC Mode)

Configuration

- Service: L2VPN.
- Feature: ATM over MPLS (ATMoMPLS, a type of AToM) in VC mode.
- Device configuration:
 - The N-PE is a Cisco 7200 with IOS 12.0(28)S.
 - No CE.
 - No U-PE.
 - L2VPN point-to-point (ATMoMPLS).
 - C7200 (ATM2/0).

Configlets

U-PE	N-PE
(None)	<code>interface ATM2/0.34234 point-to-point</code> <code>pvc 213/423 12transport</code> <code>encapsulation aal5</code> <code>xconnect 99.99.4.99 89025 encapsulation</code> <code>mpls</code>

Comments

- The N-PE is any MPLS-enabled router.
- L2VPN provisioning is on the ATM VC connection.

ATM over MPLS (VP Mode)

Configuration

- Service: L2VPN.
- Feature: ATM over MPLS (ATMoMPLS, a type of AToM) in VP mode.
- Device configuration:
 - The N-PE is a Cisco 7200 with IOS 12.0(28)S.
Interface(s): ATM2/0.
 - No CE.
 - No U-PE.
 - L2VPN point-to-point (ATMoMPLS).

Configlets

U-PE	N-PE
(None)	<pre>pseudowire-class ISC-pw-tunnel-123 encapsulation mpls preferred-path interface tunnel123 disable-fallback ! interface ATM2/0 atm pvp 131 12transport xconnect 99.99.4.99 89024 pw-class ISC-pw-tunnel-123</pre>

Comments

- The N-PE is any MPLS-enabled router.
- L2VPN provisioning is on the ATM VP connection.
- The L2VPN pseudowire is mapped to a TE tunnel.

ATM (Port Mode, Pseudowire Class, E-Line, L2VPN Group Name, IOS XR Device)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: ATM.
- Device configuration:
 - The N-PE is a CRS-1 with IOS XR 3.7 or later for ATM service (port mode only).
 - UNI on N-PE.

Configlets

U-PE	N-PE
(None)	<pre> 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 ! </pre>

Comments

- The N-PE is a CRS-1 router.
- The pseudowire class feature is optional and not configured.
- The E-Line name (**p2p** command) and L2VPN Group Name (**xconnect group** command) are user configured.
- Only PORT mode is supported in IOS XR.
- This PORT mode will not generate any specific command, such as **pvp** or **pvc**, on IOS XR devices.
- The ATM interface is included under **xconnect**.

Frame Relay over MPLS

Configuration

- Service: L2VPN.
- Feature: Frame Relay over MPLS (FRoMPLS, a type of AToM).
- Device configuration:
 - The N-PE is a Cisco 7200 with IOS 12.0(28)S.
Interface(s): ATM2/0.
 - No CE.
 - No U-PE.
 - L2VPN point-to-point (ATMoMPLS).

Configlets

U-PE	N-PE
(None)	<pre>interface Serial1/1 exit ! connect C1_89001 Serial1/1 135 12transport xconnect 99.99.4.99 89001 encapsulation mpls</pre>

Comments

- The N-PE is any MPLS-enabled router.
- L2VPN provisioning is on the serial port for the Frame Relay connection.

Frame Relay (DLCI Mode)

Configuration

- Service: L2VPN over a L2TPv3 core.
- Feature: FR in DLCI mode.
- Device configuration:
 - The N-PE is a Cisco 7200 with IOS 12.0(28)S.
 - Interface(s): ATM2/0.
 - No CE.
 - No U-PE.
 - L2VPN point-to-point (ATMoMPLS).

Configlets

U-PE	N-PE
(None)	<pre>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</pre>

Comments

- The N-PE is any L2TPv3 enabled router.
- L2VPN provisioning is on the serial port for the Frame Relay connection.

VPLS (Multipoint, ERMS/EVP-LAN)

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: VPLS (multipoint) ERMS (EVP-LAN).
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BX.L
Interface(s): FA2/18.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. No port security, no tunneling.
Interface(s): FA1/0/21 – FA1/0/23.
 - VPLS Multipoint VPN with VLAN 767.

Configlets

U-PE	N-PE
<pre> 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 bpduguard 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 </pre>	<pre> 12 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 </pre>

Comments

- The N-PE is a 7600 with OSM or SIP-600 module.
- The VFI contains all the N-PEs (neighbors) that this N-PE talks to.
- The U-PE is a generic Metro Ethernet (ME) switch. The customer BPDUs are blocked by the PACL. The VPLS ERMS (EVP-LAN) UNI is the same as the L2VPN (point-to-point) ERS (EVPL) UNI.
- The SVI (interface 767) refers to the global VFI, which contains multiple peering N-PEs.

VPLS (Multipoint, EMS/EP-LAN), BPDU Tunneling

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: VPLS (multipoint) EMS (EP-LAN) with BPDU tunneling.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(18)SXF, Sup720-3BXL.
Interface(s): FA2/18.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY1. No port security, no tunneling.
Interface(s): FA1/0/12 – FA1/0/23.
 - VPLS Multipoint VPN, with VLAN 767.
 - Q-in-Q UNI.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter enable </pre>	<pre> 12 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 </pre>

Comments

- The N-PE is a 7600 with an OSM or SIP-600 module.
- The VFI contains all the N-PEs (neighbors) that this N-PE talks to.
- The VPLS EMS (EP-LAN) UNI is the same as L2VPN (point-to-point) EWS (EPL) UNI.
- The SVI is the same as VPLS ERS (EVP-LAN) SVI.

EVC (Pseudowire Core Connectivity, UNI Port Security)

Configuration

- Service: EVC/Metro Ethernet.
- Feature: EVC with pseudowire core connectivity, with UNI port security.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33)SRB3.
Interface(s): GI2/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY2. Port security is enabled.
Interface(s): FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpduguard 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 </pre>	<pre> interface GigabitEthernet4/0/1 no shut service instance 10 ethernet encapsulation dot1q 500 rewrite ingress tag push dot1q 555 symmetric xconnect 192.169.105.20 505 encapsulation mpls </pre>

Comments

- UNI on U-PE.
- Single match tag is performed.
- The rewrite operation **push** pushes the outer VLAN tag of 555.

EVC (Pseudowire Core Connectivity, UNI, without Port Security, with Bridge Domain)

Configuration

- Service: EVC/Metro Ethernet.
- Feature: EVC with pseudowire core connectivity, with UNI, without port security, and with bridge domain.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33)SRB3.
Interface(s): GI2/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25)EY2. Port security is enabled.
Interface(s): FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> vlan 100 interface GigabitEthernet2/0/0 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 </pre>

Comments

- UNI on U-PE.
- Single match tag is performed.
- The rewrite operation **push** pushes two tags.

EVC (Pseudowire Core Connectivity, UNI, and Pseudowire Tunneling)

Configuration

- Service: EVC/Metro Ethernet.
 - Feature: EVC with pseudowire core connectivity, with UNI, with pseudowire tunneling.
 - Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
- Interface(s): GI4/0/0 <--> GI2/0/0.

Configlets

U-PE	N-PE
(None)	<pre> pseudowire-class ISC-pw-tunnel-2147 encapsulation mpls preferred-path interface Tunnel2147 disable-fallback interface GigabitEthernet4/0/0 service instance 1 ethernet encapsulation dot1q 11 second-dot1q 41 rewrite ingress tag pop 2 symmetric xconnect pw-class ISC-pw-tunnel-2147 </pre>

Comments

- UNI on N-PE (the CE is directly connected).
- Match of both tags is performed.
- The rewrite operation pops both the inner and outer VLAN tags.

EVC (VPLS Core Connectivity, UNI Port Security)

Configuration

- Service: EVC/Metro Ethernet.
- Feature: EVC with VPLS core connectivity, with UNI port security.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GI4/0/1.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2. Port security is enabled.
Interface(s): FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> 12 vfi attest-226 manual vpn id 226 neighbor 192.169.105.20 encapsulation mpls vlan 200 bridge-domain 200 split-horizon interface GigabitEthernet4/0/1 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 </pre>

Comments

- UNI on U-PE.
- The rewrite operation translates the incoming VLAN tag 500 to 222.

EVC (VPLS Core Connectivity, no UNI Port Security)

Configuration

- Service: EVC/Metro Ethernet.
- Feature: EVC with VPLS core connectivity, without UNI port security.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GI4/0/1.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> 12 vfi attest1-458 manual vpn id 452 neighbor 192.169.105.20 encapsulation mpls vlan 200 bridge-domain 200 split-horizon interface GigabitEthernet4/0/1 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 </pre>

Comments

- UNI on U-PE.
- The rewrite operation translates the incoming VLAN tag 500 to two tags, 222 and 41.

EVC (Local Connect Core Connectivity, UNI Port Security)

Configuration

- Service: EVC/Metro Ethernet.
- Feature: EVC with local connect core connectivity, with UNI port security.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s):GI2/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2. Port security is enabled.
Interface(s): FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpduguard 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 </pre>	<pre> Connect Customer_1 GigabitEthernet4/0/1 10 GigabitEthernet4/0/10 25 interface GigabitEthernet4/0/1 no shut service instance 10 ethernet encapsulation dot1q 500 rewrite ingress tag push dot1q 555 symmetric interface GigabitEthernet4/0/10 no shut service instance 25 ethernet encapsulation dot1q 500 second-dot1q 501 rewrite ingress tag translate 2-to-1 dot1q 222 symmetric </pre>

Comments

- UNI on U-PE.
- Two tag matching operations are carried out.
- The rewrite operation translates two tags to a single tag.
- Two service instances are connected through the **connect** command.

EVC (Local Connect Core Connectivity, UNI, no Port Security, Bridge Domain)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with local connect core connectivity, with UNI, without port security, and with bridge domain.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s):GI2/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s):FA1/14– FA3/23.

Configlets

U-PE	N-PE
<pre> 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 bpdupfilter 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 </pre>	<pre> interface GigabitEthernet2/0/0 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 GigabitEthernet2/0/10 no shut service instance 15 ethernet encapsulation dot1q 24 rewrite ingress tag pop 1 symmetric bridge-domain 200 split-horizon </pre>

Comments

- UNI on U-PE.
- The rewrite operation maps/translates the incoming two tags into two different tags.
- The service instances here are connected through bridge domain.

EVC (Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with pseudowire core connectivity, with bridge domain, and with Pseudowire on SVI enabled on the N-PE.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/10.

Configlets

U-PE	N-PE
<pre> 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 </pre>	<pre> 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 </pre>

Comments

- None.

EVC (Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with pseudowire core connectivity, bridge domain disables, and with Pseudowire on SVI disabled on the N-PE.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/10.

Configlets

U-PE	N-PE
<pre> 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 </pre>	<pre> 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 </pre>

Comments

- None.

EVC (AutoPick Service Instance Name)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with AutoPick Service Instance Name enabled and the Service Instance Name input field left blank.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/2.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/14.

Configlets

U-PE	N-PE
<pre>! 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 mac access-group ISC-FastEthernet1/0/13 in</pre>	<pre>! vlan 3524 exit ! ethernet evc C1_1 ! interface GigabitEthernet7/0/0 service instance 3 ethernet C1_1 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</pre>

Comments

- The transport type is pseudowire.
- The autopick Service Instance Name will take the value *CustomerName_JobID*.

EVC (No AutoPick Service Instance Name, No Service Instance Name)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with AutoPick Service Instance Name not enabled and the Service Instance Name input field left blank.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/2.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/14.

Configlets

U-PE	N-PE
<pre> ! 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 </pre>	<pre> ! interface GigabitEthernet7/0/2 service instance 43 ethernet encapsulation dot1q 566 xconnect 1.1.1.1 453366 encapsulation mpls </pre>

Comments

- In this example, the user does not enable AutoPick Service Instance Name and also leaves the Service Instance Name input field blank.
- The global command **ethernet evc** is not generated, while the command **service instance 43 ethernet** is generated.
- There is no Service Instance Name available and the Service Instance ID is 43.

EVC (User-Provided Service Instance Name, Pseudowire Core Connectivity)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with pseudowire core connectivity and user-provided service instance name.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/10.

Configlets

U-PE	N-PE
<pre>! 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 mac access-group ISC-FastEthernet1/0/13 in</pre>	<pre>! vlan 3524 exit ! ethernet evc ServiceInst ! interface GigabitEthernet7/0/0 service instance 3 ethernet ServiceInst 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</pre>

Comments

- The transport type is PSEUDOWIRE.
- The user manually provided **ServiceInst** as the Service Instance Name. This is pushed onto the device, where the Service Instance ID is 3.

EVC (User-Provided Service Instance Name, Local Core Connectivity)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with local core connectivity and a user-provided service instance name.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet1/0/6, GigabitEthernet1/0/7.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/12, FastEthernet1/0/14.

Configlets

U-PE	N-PE
<pre> 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 </pre>	<pre> 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 </pre>

Comments

- The transport type is LOCAL.
- The user manually provided **service_int** as the Service Instance Name. This is pushed onto the device, where the Service Instance IDs are 5 and 33, respectively.

EVC (User-Provided Service Instance Name, VPLS Core Connectivity)

Configuration

- EVC/Metro Ethernet.
- Feature: EVC with VPLS core connectivity and user-provided service instance name.
- Device configuration:
 - The N-PE is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/0.
 - The U-PE is a Cisco 3750ME with IOS 12.2(25) EY2.
Interface(s): FastEthernet1/0/10.

Configlets

U-PE	N-PE
<pre> ! 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 mac access-group ISC-FastEthernet1/0/13 in </pre>	<pre> l2 vfi vpls-test manual vpn id 300 neighbor 22.22.22.22 encapsulation mpls ! vlan 500 ! ethernet evc ServiceInst ! interface GigabitEthernet7/0/0 service instance 10 ethernet ServiceInst encapsulation dot1q 400 rewrite ingress tag pop 1 symmetric bridge-domain 500 split-horizon ! interface vlan500 xconnect vfi vpls-test </pre>

Comments

- The transport type is VPLS.
- The user manually provided **ServiceInst** as the Service Instance Name. This is pushed onto the device, where the Service Instance ID is 10.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Point-to-Point Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity with an end-to-end circuit with multiple links. One link terminates on an ATM interface on N-PE 1, and the other link terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.370.
 - N-PE 2 is a Cisco 7600 with IOS 12.2(33) SRE.
Interface(s): GigabitEthernet4/0/2.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>! interface ATM1/0/0.370 point-to-point no atm enable-ilmi-trap pvc 0/370 12transport encapsulation aal5snap xconnect 192.169.105.10 123 pw-class inter-ether !</pre>	<pre>! ethernet evc 1-3_51 ! interface GigabitEthernet4/0/2 no ip address 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 !</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Multipoint Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity with a multipoint circuit. Link #1 terminates on an ATM interface on N-PE 1, link #2 terminates on an Ethernet interface on N-PE 1, and link #3 terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet7/0/4, ATM6/0/0.100.
 - The N-PE 2 is a Cisco 7600 with IOS 12.2(33) SRE.
Interface(s): GigabitEthernet7/0/5.

Configlets

N-PE 1 (ATM + Ethernet)	N-PE 2 (Ethernet)
<pre>! 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</pre>	<pre>! 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</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
 - Feature: EVC for ATM-Ethernet interworking with local core connectivity with a point-to-point circuit. The circuit terminates on different ATM interfaces on the same local N-PE.
 - Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
- Interface(s): ATM1/0/1, ATM4/1/0, ATM1/0/1.99, ATM4/1/0.98.

Configlets

N-PE 1 (ATM)	N/A
<pre>! 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 !</pre>	

Comments

- None.

EVC (ATM-Ethernet Interworking, Local Core Connectivity, Multipoint Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
 - Feature: EVC for ATM-Ethernet interworking with local core connectivity for multiple links that terminate on the same local N-PE. Link #1 terminates on an ATM interface, and link #2 terminates on an Ethernet interface.
 - Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
- Interface(s): ATM1/0/0.99, TenGigabitEthernet6/0/0, TenGigabitEthernet6/0/1.

Configlets

N-PE 1 (ATM + Ethernet)	N/A
<pre>! 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 !</pre>	

Comments

- None.

EVC (ATM-Ethernet Interworking, Local Core Connectivity, Multipoint Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with local core connectivity. Multiple links terminate on the same local N-PE. Link #1 terminates on an ATM interface, link #2 terminates on an ATM interface, and link #3 terminates on an ATM interface.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
 - Interface(s): ATM6/0/0.100, ATM6/0/1.101, ATM6/0/2.102.

Configlets

N-PE 1 (ATM)	N/A
<pre>! 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 !</pre>	

Comments

- None.

EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with local core connectivity. A point-to-point circuit terminates on different ATM interfaces on same local N-PE.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
 - Interface(s): ATM1/0/0, ATM1/0/1.

Configlets

N-PE 1 (ATM)	N/A
<pre>! 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</pre>	

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity for end-to-end circuit with multiple links. One link terminates on ATM interface on N-PE 1, and other link terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.370.
 - The N-PE 2 is a Cisco ASR 9000 with IOS XR 3.9.0.
Interface(s): GigabitEthernet0/0/0/4.458.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>! 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 !</pre>	<pre>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 ! ! !</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, Multipoint Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity with an end-to-end circuit with multiple links. One link is terminating on an ATM interface on N-PE 1, and the other (non-flex) link terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM4/1/0.8790.
 - The N-PE 2 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): GigabitEthernet4/0/17.600.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>interface ATM4/1/0.8790 point-to-point pvc 150/3454 12transport encapsulation aal5snap xconnect 192.169.105.10 760 pw-class ISC-pw-tunnel-1</pre>	<pre>interface GigabitEthernet4/0/17.600 encapsulation dot1Q 600 xconnect 192.169.105.20 760 pw-class ISC-pw-tunnel-1</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Local Core Connectivity, Point-to-Point Circuit)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with local core connectivity for point-to-point circuit. The circuit terminates on the same, local N-PE 1. One link terminates on an ATM interface, and the other (non-flex) link terminates on an Ethernet interface.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.444.
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): FastEthernet3/39.674.

Configlets

N-PE 1 (ATM + Ethernet)	N/A
<pre>! interface FastEthernet3/39.674 encapsulation dot1Q 674 ! interface ATM1/0/0.444 point-to-point pvc 44/4444 12transport encapsulation aal5snap ! connect Customer1_204 ATM1/0/0 44/4444 FastEthernet3/39.674 interworking ethernet</pre>	

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, with Bridge Domain)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity for end-to-end circuit with multiple links with bridge domain enabled. One link terminates on an ATM interface on N-PE 1, and the other link terminates on a flex Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.370.
 - The N-PE 2 is a Cisco ASR 9000 with IOS XR 3.9.0.
Interface(s): GigabitEthernet0/0/0/25.341.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>! 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</pre>	<pre>interface GigabitEthernet0/0/0/25.341 l2transport encapsulation dot1q 341 rewrite ingress tag push dot1q 430 second-dot1q 349 symmetric ! l2vpn bridge group tml bridge-domain CISCO interface GigabitEthernet0/0/0/25.341 ! neighbor 192.169.105.20 pw-id 32190 ! ! ! !</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, with Bridge Domain)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity for end-to-end circuit with multiple links. Bridge domain is enabled. One link terminates on an ATM interface on N-PE 1, and the other (non-flex) link terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.370.
 - The N-PE 2 is a Cisco ASR 9000 with IOS XR 3.9.0.
Interface(s): GigabitEthernet0/0/0/20.712.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>! 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 !</pre>	<pre>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 ! ! ! !</pre>

Comments

- None.

EVC (ATM-Ethernet Interworking, Pseudowire Core Connectivity, End-to-End Circuit, no Bridge Domain)

Configuration

- EVC/ATM-Ethernet Interworking.
- Feature: EVC for ATM-Ethernet interworking with pseudowire core connectivity for end-to-end circuit with multiple links. Bridge domain is disabled. One link terminates on an ATM interface on N-PE 1, and the other link terminates on an Ethernet interface on N-PE 2.
- Device configuration:
 - The N-PE 1 is a Cisco 7600 with IOS 12.2(33) SRB3.
Interface(s): ATM1/0/0.370.
 - The N-PE 2 is a Cisco ASR 9000 with IOS XR 3.9.0.
Interface(s): GigabitEthernet0/0/0/12.433.

Configlets

N-PE 1 (ATM)	N-PE 2 (Ethernet)
<pre>! 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 !</pre>	<pre>interface GigabitEthernet0/0/0/12.433 l2transport encapsulation dot1q 433 rewrite ingress tag push dot1q 43 second-dot1q 53 symmetric ! l2vpn xconnect group ISC p2p CISCO interface GigabitEthernet0/0/0/12.433 neighbor 192.169.105.20 pw-id 4531 ! ! ! !</pre>

Comments

- None.
-