CHAPTER 7

Setting Up the Prime Fulfillment Services

To create L2VPN, VPLS, and FlexUNI/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 chapter contains the basic steps to set up the Cisco Prime Fulfillment 6.1, services for an L2VPN services. It contains the following sections:

Note This chapter presents high-level information on Prime Fulfillment services that are relevant to L2VPN. For more detailed information on setting up these and other basic Prime Fulfillment services, see the chapters contained in *Part 3, Setting Up Services*.

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

Every network element that Prime Fulfillment manages must be defined as a device in the system. An element is any device from which Prime Fulfillment 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 Chapter 4, "Setting Up Physical Inventory."

Configuring Device Settings to Support Prime Fulfillment

Two device settings must be configured to support the use of Prime Fulfillment 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 Fulfillment 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 Fulfillment 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 > Resources > 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 **LDPTermination 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 Fulfillment 6.1, 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 Fulfillment as an IOS XR device, as follows:

a. Create the Cisco device by choosing **Inventory > Devices > Create Cisco Devcie**.

b. Choose **Cisco Device** in the drop-down list.

The Create Cisco Router window appears.

c. 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 Chapter 18, "Sample Configlets".

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 Chapter 5, "Setting Up Resources."

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 Chapter 5, "Setting Up Resources."

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 Chapter 3, "Setting Up Logical Inventory."

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 Fulfillment 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 Fulfillment. 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 Chapter 5, "Setting Up Resources."

Creating VLAN Pools

For L2VPN and VPLS, you create a VLAN pool so that Prime Fulfillment 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 Fulfillment 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 Fulfillment service, Prime Fulfillment warns you if the VLAN ID is outside the valid range of the defined VLAN pool. If so, Prime Fulfillment 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 Fulfillment automatically assign a VLAN to the links, perform the following steps.

Step 1 Choose **Service Design > Resources > 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 7-4.) 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 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 Fulfillment service, Prime Fulfillment warns you if the VC ID is outside the valid range of the defined VC ID pool. If so, Prime Fulfillment 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 > Resources > 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 7-8.
- Through the autodiscovery process. For details on how to do this, see Creating NPC Links Through the Autodiscovery Process, page 7-9.

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 > Logical 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 Chapter 3, "Setting Up Logical Inventory."

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 > Logical 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 Fulfillment 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 Fulfillment, see Appendix E, “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 Fulfillment database. NPCs are further abstracted from the discovered connectivity.

For detailed steps to create NPCs using autodiscovery, see Chapter 3, "Setting Up Logical Inventory."

Creating and Modifying Pseudowire Classes for IOS XR Devices

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 Fulfillment 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 Fulfillment 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 Chapter 12, "Creating an L2VPN Policy" and Chapter 13, "Managing an L2VPN Service Request."

Creating a Pseudowire Class

To create a pseudowire class, perform the following steps.

Step 1 Choose **Inventory > Logical 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 theIOS 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 7-12.

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 configures 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 Fulfillment 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 Fulfillment, 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 Fulfillment.

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 Object

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 > Logical 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.

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 Fulfillment, navigate to **Administration > Control Center > 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 Fulfillment 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 Fulfillment, navigate to **Administration > Control Center > 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**.