



Before Setting Up Prime Provisioning

This chapter explains how to set up the services. It contains the following sections:

- [Setting Up Devices and Device Groups, page 2-1](#)
- [Setting Up Resources, page 2-39](#)
- [Setting Up Logical Inventory, page 2-53](#)

Setting Up Devices and Device Groups

This section explains how to set up the physical services. It contains the following sections:

- [Devices, page 2-1](#)
- [Device Configuration Collection, page 2-13](#)
- [Providers, page 2-14](#)
- [Provider Regions, page 2-16](#)
- [Provider Devices, page 2-17](#)
- [Using the Inventory Manager Window, page 2-19](#)
- [Device Groups, page 2-27](#)
- [Ethernet Access Topology Information, page 2-29](#)
- [Managing Customer Premise Devices, page 2-34](#)

Devices

Every network element that Cisco Prime Provisioning (Prime Provisioning) manages must be defined as a device in the system. An element is any device from which Prime Provisioning can collect information. Devices can be Cisco IOS XR and IOS XE routers that function as Provider Edge Routers (PEs) or Customer Edge Routers (CEs) in the MPLS VPN or they can be a variety of non-Cisco devices.



Note

To provision services with Prime Provisioning, you must have IPv4 connectivity.

This section describes how to configure SSHv1 or SSHv2, set up SNMP, manually enable an RTR responder, and create, edit, delete, and configure various types of supported devices. This section includes the following topics:

- [Configuring SSHv1 or SSHv2, page 2-2](#)
- [Creating a Device, page 2-5](#)
- [Copying a Device, page 2-11](#)
- [Editing a Device, page 2-12](#)
- [Deleting Devices, page 2-12](#)
- [Editing a Device Configuration, page 2-12](#)
- [E-mailing a Device's Owner, page 2-13](#)

**Note**

To add non-Cisco devices in Prime Provisioning, please contact your Cisco representative and request information about activating and licensing this feature.

Configuring SSHv1 or SSHv2

Prime Provisioning needs a mechanism to securely access and deploy configuration files on devices, which include routers and switches. And, to securely download a configlet and upload a configuration file from a device, SSH version 1 (SSHv1) or SSH version 2 (SSHv2) must be enabled.

**Note**

SSHv1 is only supported for Cisco IOS devices.

The following sections describe:

- [Configuring SSHv1 on Cisco IOS Routers Using a Domain Name, page 2-2](#)
- [Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs, page 2-3](#)
- [Configuring SSHv1 or SSHv2 on Cisco IOS XR Routers, page 2-3](#)

Configuring SSHv1 on Cisco IOS Routers Using a Domain Name

The procedure for configuring SSHv1 on a Cisco IOS router is as follows:

	Command	Description
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# ip domain-name <i><domain_name></i>	Specifies the IP domain name.
Step 3	Router(config)# username <i><username></i> password <i><password></i>	Configures the user ID and password. Enter your Prime Provisioning username and password. For example: username admin password iscpwd
Step 4	Router(config)# crypto key generate rsa	Generates keys for the SSH session.
Step 5	You will see the following prompt: Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. How many bits in the modulus (nnn): Press Enter to accept the default number of bits.	Sets the number of bits.
Step 6	Router(config)# line vty 0 4	Enables SSH as part of the vty login transport.

	Command	Description
Step 7	Router(config-line)# login local	The login local command indicates that the router stores the authentication information locally.
Step 8	Router(config-line)# transport input telnet ssh	Enables SSH transport.
Step 9	Router(config-line)# Ctrl+Z	Returns to Privileged Exec mode.
Step 10	Router# copy running startup	Saves the configuration changes to nonvolatile random-access memory (NVRAM).

Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs

The procedure for configuring SSHv1 or SSHv2 on a Cisco IOS router is as follows.

	Command	Description
Step 1	Router# enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# ip ssh rsa keypair-name <keypair-name>	Specifies which RSA keypair to use for SSH usage. Note: A Cisco IOS router can have many RSA key pairs.
Step 4	Router(config)# crypto key generate rsa usage-keys label <key-label> modulus <modulus-size>	Enables the SSH server for local and remote authentication on the router. For SSH version 2, the modulus size must be at least 768 bits. Note: To delete the Rivest, Shamir, and Adelman (RSA) key-pair, use the crypto key zeroize rsa command. After you have deleted the RSA command, you automatically disable the SSH server.
Step 5	Router(config)# ip ssh [timeout <seconds> authentication-retries <integer>]	Configures SSH control variables on your router.
Step 6	Router(config)# ip ssh version [1 2]	Specifies the version of SSH to be run on a router.

Configuring SSHv1 or SSHv2 on Cisco IOS XR Routers

The procedure for configuring SSHv2 on a Cisco IOS XR router is as follows.

	Command	Description
Step 1	RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	RP/0/RP0/CPU0:router(config)# hostname <hostname>	Configures a hostname for your router.
Step 3	RP/0/RP0/CPU0:router(config)# domain name <domain-name>	Defines a default domain name that the software uses to complete unqualified host names.
Step 4	RP/0/RP0/CPU0:router(config)# exit	Exits global configuration mode, and returns the router to EXEC mode.

	Command	Description
Step 5	RP/0/RP0/CPU0:router(config)# crypto key generate rsa [usage keys general-keys] [<keypair-label>]	Generates an RSA key pair.
Step 6	RP/0/RP0/CPU0:router# crypto key generate dsa	Enables the SSH server for local and remote authentication on the router. The recommended minimum modulus size is 1024 bits. Generates a DSA key pair. To delete the DSA key pair, use the crypto key zeroize dsa command. This command is used only for SSHv2.
Step 7	RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 8	RP/0/RP0/CPU0:router# ssh timeout <seconds>	(Optional) Configures the timeout value for user authentication to authentication, authorization, and accounting (AAA). If the user fails to authenticate itself to AAA within the configured time, the connection is aborted. If no value is configured, the default value of 30 is used for 30 seconds. The range is from 5 to 120.
Step 9	RP/0/RP0/CPU0:router(config)# ssh server or RP/0/RP0/CPU0:router(config)# ssh server v2	Brings up an SSH server. To bring down an SSH server, use the no ssh server command. (Optional) Forces the SSH server to accept only SSHv2 clients if you configure the SSHv2 option by using the ssh server v2 command. If you choose the ssh server v2 command, only the SSH v2 client connections are accepted.
Step 10	RP/0/RP0/CPU0:router(config)# end or RP/0/RP0/CPU0:router(config)# commit	Saves configuration changes. When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel] Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

	Command	Description
Step 11	RP/0/RP0/CPU0:router# show ssh	(Optional) Displays all of the incoming and outgoing SSHv1 and SSHv2 connections to the router.
Step 12	RP/0/RP0/CPU0:router# show ssh session details	(Optional) Displays a detailed report of the SSHv2 connections to and from the router.

Creating a Device

From the Create window, you can define different types of devices.

To create a device, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
- The Device List window appears.
- Step 2** Click the **Create** button.
- The Create options window appears.
- The **Create** options include the following:
- **Catalyst Switch**—A Catalyst device running the Catalyst Operating System.
 - **Cisco Device**—Any device that runs the Cisco IOS. This includes Catalyst devices running Cisco IOS.
 - **Non Cisco Device**—Any device that does not run Cisco IOS.
 - **Terminal Server**—A device that represents the workstation that can be used to provision edge routers.
- Step 3** The following sections include examples with instructions for creating each type of device.
- [Creating a Catalyst Switch, page 2-5](#)
 - [Creating a Cisco or Non-Cisco Device, page 2-6](#)
 - [Creating a Terminal Server, page 2-7](#)
-

Creating a Catalyst Switch

To create a Catalyst switch, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
- The Device List window appears.
- Step 2** Click the **Create** button.
- The Create options window appears.
- Step 3** Select **Catalyst Switch**.
- The Create Catalyst Device window appears.
- See the following sections for descriptions of these attribute fields:
- [General Attributes, page 2-7](#)

- [Login and Password Attributes, page 2-9](#)
- [Device and Configuration Access Information Attributes, page 2-9](#)
- [SNMP v1/v2c Attributes, page 2-10](#)

Step 4 Enter the desired information for the Catalyst device you are creating.

Step 5 To access the Additional Properties section of the **Create Catalyst Device**, click **Show**.
The Additional Properties window appears.

See the following sections for descriptions of the Additional Properties attribute fields:

- [SNMP v3 Attributes, page 2-10](#)
- [Terminal Server Options Attributes, page 2-11](#)
- [Device Platform Information Attributes, page 2-11](#)

Step 6 Enter any desired Additional Properties information for the Catalyst device you are creating.

Step 7 Click **Save**.

The Devices window reappears with the new Catalyst device listed.

Creating a Cisco or Non-Cisco Device

To create a Cisco or Non-Cisco device, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices**.

The Device List window appears.

Step 2 Click the **Create** button.

The Create options window appears.

Step 3 Select a device.

The Create Device window appears.

See the following sections for descriptions of the fields:

- [General Attributes, page 2-7](#)
- [Login and Password Attributes, page 2-9](#)
- [Device and Configuration Access Information Attributes, page 2-9](#)
- [SNMP v1/v2c Attributes, page 2-10](#)

Step 4 Perform the following steps, if you are creating a Cisco IOS device:

- Enter the desired information for the Cisco IOS device you are creating.
- To access the Additional Properties section of the **Create Cisco Device**, click **Show**.

The Additional Properties window appears.

See the following sections for descriptions of the Additional Properties fields:

- [SNMP v3 Attributes, page 2-10](#)
- [Terminal Server Options Attributes, page 2-11](#)
- [Device Platform Information Attributes, page 2-11](#)

- Enter any desired Additional Properties information for the Cisco IOS device you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new device listed.

Creating a Terminal Server

To create a Terminal Server device, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices**.

The Device List window appears.

Step 2 Click the **Create** button.

The Create options window appears.

Step 3 Select **Terminal Server**.

The Create Terminal Server window appears.

See the following sections for descriptions of the fields:

- [General Attributes, page 2-7](#)
- [Login and Password Attributes, page 2-9](#)
- [Device and Configuration Access Information Attributes, page 2-9](#)
- [SNMP v1/v2c Attributes, page 2-10](#)

Step 4 Enter the desired information for the Terminal Server you are creating.**Step 5** To access the Additional Properties section of the **Create Terminal Server**, click **Show**.

The Additional Properties window appears.

See the following sections for descriptions of the Additional Properties fields:

- [SNMP v3 Attributes, page 2-10](#)
- [Terminal Server Options Attributes, page 2-11](#)
- [Device Platform Information Attributes, page 2-11](#)

Step 6 Enter any desired Additional Properties information for the Terminal Server device you are creating.**Step 7** Click **Save**.

The Devices window reappears with the new Terminal Server device listed.

General Attributes

The General Attributes sections contains the following fields:

- **Device Host Name** (required)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.

- **Description** (optional)—Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional)—Drop-down list of all collection zones within the Prime Provisioning. Choices include: None and all collection zones within the Prime Provisioning. Default: None.
- **Management IP Address** —Valid IP address of the device that Prime Provisioning uses to configure the target router device.
- **Element Management Key** —Valid IP address of the device that Prime Provisioning.
- **Interfaces** (optional)—Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See [Table 2-1](#) for a description of the Interfaces fields.

Table 2-1 Create Catalyst Device Interfaces Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
IPv4 Address	IPv4 address associated with this interface.	
IPv6 Address	IPv6 address associated with this interface.	
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
Port Type		NONE ACCESS TRUNK ROUTED

Table 2-1 Create Catalyst Device Interfaces Fields (continued)

Field	Description	Additional
Description	Description of the device interface.	Description of the device interface.
IP Address Type	IP address type.	IP address type.

- **Associated Groups** (optional)—Click the **Edit** button to view, add, and remove all Device Group associations.

Login and Password Attributes

The Login and Password Information section contains the following fields:

- **Login User** (optional)—Not required by Prime Provisioning. However, collection and upload/download will not function without the Login User and Login Password as Prime Provisioning will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional)—Not required by Prime Provisioning. However, collection and upload/download will not function without the Login User and Login Password, because Prime Provisioning will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional)—Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional)—Not required by Prime Provisioning. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional)—Not required by Prime Provisioning. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional)—Must match the Enable Password field. Limited to 80 characters.

Device and Configuration Access Information Attributes

The Device and Configuration Access Information section contains the following fields:

- **Terminal Session Protocol** (optional)—Configures the method of communication between Prime Provisioning and the device. Choices include: Telnet, SSH version 1 (SSHv1), RSH, and SSH version 2 (SSHv2). In previous versions of Prime Provisioning, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional)—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **SOCKS5 Proxy IP** (optional)—The device with SOCKS5 Proxy IP acts as an End-point Network Element (ENE) device and is used for both Telnet and SSH type of Terminal Session Protocol. This attribute configures the IP address of Gateway Network Element (GNE) as the proxy IP for the ENE device. ENE device cannot directly connect to any network or to any another ENE device. The connection is possible only using SOCKS5 proxy IP.



Note You can also configure this attribute for other Cisco devices which needs proxy connection.

- **PORT** (optional)—Connects to the Cisco devices via the specified port number while connecting using the Terminal Session Protocol either as Telnet or SSH.
- **OS** (optional)—The choices are: IOS, IOS_XR, and ME1200. Applicable for Creating a Cisco Device and for Creating a Terminal Server.
- **SNMP Version** (optional)—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

SNMP v1/v2c Attributes

The SNMP v1/v2c section contains the following fields:

- **Community String RO** (optional)—SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional)—SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMP v3 Attributes

The SNMP v3 section contains the following fields:

- **SNMP Security Level** (optional)—Choices include: Default (*<default_set_in_DCPL>*), Authentication/No Encryption, Authentication/Encryption, and No Authentication/No Encryption. Default: Default (*<default_set_in_DCPL>*). Note: When you change the DCPL property, the *<default_set_in_DCPL>* variable changes.
- **Authentication User Name** (optional)—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional)—Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional)—In previous versions of Prime Provisioning, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional)—Must match the Encryption Password field. Limited to 80 characters.

- **Encryption Algorithm** (optional)—In previous versions of Prime Provisioning, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None, DES 56 and AES 128. Default: None.

Terminal Server Options Attributes

The Terminal Server Options section contains the following fields:

- **Terminal Server** (optional)—Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional)—Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.

The following fields are also available when you are creating a Cisco Device:

- **Fully Managed** (optional)—If the Fully Managed check box is checked, the device becomes a fully managed device. Prime Provisioning performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside Prime Provisioning and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **IE2100** (optional)—Disabled unless the Device State field is INACTIVE. Choices include: None and the list of existing IE2100 names. Default: None.

Device Platform Information Attributes

The Device Platform Information section contains the following fields:

- **Platform** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional)—Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.



Note

Email feature has been deprecated and will be removed in a subsequent release.

Copying a Device

From the Copy window, you receive a copy of the chosen device and can name it and change values.

To access the Copy window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Device**.
The Device List window appears.
 - Step 2** Select a single device to copy by checking the check box to the left of the Device Name.
 - Step 3** Click the **Copy** button. This button is only enabled if a device is selected.

A window appropriate to the type of device selected to copy appears. You receive an exact copy of the selected device but the Name, Management IP Address, all Interfaces, and VPNSM blades for a Catalyst Switch running Cisco IOS are blanked out and you must fill in the required information and save this new device. See the [“Creating a Device” section on page 2-5](#) for specifics.

Editing a Device

From the Edit window, you can modify the fields that have been specified for a particular device.

To access the Edit window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
The Device List window appears.
 - Step 2** Select a single device to edit by checking the box to the left of the Device Name. You can also select a device to edit by clicking on the hyperlink of the device name.
 - Step 3** Click the **Edit** button. This button is only enabled if a device is selected.
The Edit window appropriate to the type of device selected appears. For example, if you selected a Cisco IOS device the Edit Cisco IOS Device window appears.
 - Step 4** Enter the changes you want to make to the selected device.
 - Step 5** Click **Save**.
The changes are saved and the Devices window reappears.
-

Deleting Devices

From the Delete window, you can remove selected devices from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
The Device List window appears.
 - Step 2** Select one or more devices to delete by checking the check box(es) to the left of the Device Name(s).
 - Step 3** Click the **Delete** button. This button is enabled only if one or more devices are selected.
The Confirm Delete window appears.
 - Step 4** Click the **Delete** button to confirm that you want to delete the device(s) listed.
The Devices window reappears with the specified device(s) deleted.
-

Editing a Device Configuration

From the Config window, you can edit the configuration for a specified device.

To access the Config window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
The Device List window appears.
- Step 2** Select a single device to modify by checking the check box to the left of the Device Name.
- Step 3** Click the **Config** button.
The Device Configurations window for the selected device appears.
- Step 4** Check the box to the left of the Date for the configuration that you want to modify and click the **Edit** button. This button is only enabled if a device is selected.
The Device Configuration window for the selected device appears.
- Step 5** Enter the changes you want to make to the selected device configuration.
- Step 6** Click **Save**.
The changes are saved and the Device Configurations window reappears.
- Step 7** Click **OK** to return to the Devices window.
-

E-mailing a Device's Owner

From the E-mail window, you can send a device report via e-mail to the owners of specified devices. To access the E-mail window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Devices**.
The Device List window appears.
- Step 2** Select the devices for which you want to send a device report by checking the check box(es) to the left of the Device Name(s).
- Step 3** Click the **E-mail** button. This button is only enabled if one or more devices are selected.
The Send Mail to Device Owners window appears.
- Step 4** Compose the e-mail that you want to send to the selected device owners.
- Step 5** Click **Send**.
The e-mail is sent and the Devices window reappears.
-

Device Configuration Collection

We recommend that a Task Manager Collect Configuration task is used to add interface configuration to Devices in the Prime Provisioning Repository. A Task Manager Collect Configuration task connects to the physical device in the network, collects the device information from the router (including interface configuration), and populates the Prime Provisioning Repository with this information.

For details of how to add Device interface configuration using a Task Manager Collect Configuration task, see [This chapter contains the following sections:](#), page 12-1.

Synchronizing the Prime Provisioning Repository with Device Configuration



Note

We recommend that the device configuration is resynchronized with the physical devices after any configuration changes and at periodic intervals. This ensures that the device configuration held in the Prime Provisioning inventory is consistent with the physical devices in the network.

We recommend that device configuration is kept up-to-date using a scheduled Task Manager task. Either Collect Configuration or Collect Configuration from File can be used. For details of how to create a scheduled Task Manager Collect Configuration task, see [This chapter contains the following sections; page 12-1](#). All PE and P routers in the MPLS network should have their configuration collected using a scheduled Task Manager Collect Configuration task. The Task Manager Collect Configuration task collects details of interface configuration and other device attributes. The interval at which Task Manager Collect Configuration tasks should be scheduled to run depends on the frequency of configuration changes to the network. We recommend running the Task Manager Collect Configuration task daily on each P and PE router.

Providers

This section describes how to create and manage providers. This section includes the following topics:

- [Creating a Provider, page 2-14](#)
- [Editing a Provider, page 2-15](#)
- [Deleting Providers, page 2-15](#)

Creating a Provider

From the Create Provider window, you can create different providers.

To create a provider, follow these steps:

Step 1 Choose **Service Design > Resources > Providers**.

The Providers window appears.

Step 2 Click the **Create** button.

The Create Provider window appears.

The Create Provider window contains the following fields:

- **Name** (required)—Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters.
- **BGP AS** (required)—Each BGP autonomous system is assigned a unique 16-bit number (1 to 65535) or a 32-bit number (1 to 4294967295) by the same central authority that assigns IP network numbers. This has an impact on the RD and RT values associated with the BGP AS number.

ASNumber:VPN ID/index (hex or decimal format)

When BGP AS is a 16 bit number, you need to enter a 32 bit value as the VPN ID/index and vice versa. If these values are not entered correctly, the service request moves to failed deploy state.

- **Contact Information** (optional)—Any pertinent information about the provider that could be helpful to service provider operators. Limited to 256 characters.

Step 3 Enter the name, BGP AS, and any contact information for the Provider that you are creating.

Step 4 Click **Save**.

The Providers window reappears with the new provider listed.

Editing a Provider

From the Edit Provider window, you can modify the fields that have been specified for a particular provider.

To access the Edit Provider window, follow these steps:

Step 1 Choose **Service Design > Resources > Providers**.

The Providers window appears.

Step 2 Select a single provider to modify by checking the check box to the left of the Provider Name.

Step 3 Click the **Edit** button. This button is only enabled if a customer is selected.

The Edit Provider window appears.

Step 4 Enter the changes you want to make to the selected provider.

Step 5 Click **Save**.

The changes are saved and the Providers window reappears.

Deleting Providers

From the Delete window, you can remove selected providers from the database.

To access the Delete window, follow these steps:

Step 1 Choose **Service Design > Resources > Providers**.

The Providers window appears.

Step 2 Select provider(s) to delete by checking the check box to the left of the Provider Name.

Step 3 Click the **Delete** button. This button is enabled only if one or more Providers are selected.

The Confirm Delete window appears.

Step 4 Click the **Delete** button to confirm that you want to delete the provider(s) listed.

The Providers window reappears with the specified provider(s) deleted.

Provider Regions

A Provider Region is considered to be a group of provider edge routers (PEs) within a single BGP autonomous system. The primary objective for defining Provider Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.

This sections covers the following topics:

- [Creating a Provider Region, page 2-16](#)
- [Editing a Provider Regions, page 2-16](#)
- [Deleting Provider Regions, page 2-17](#)

Creating a Provider Region

From the Create Provider Region window, you can create different PE regions.

To create a provider region, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Provider Regions**.
The Provider Regions window appears.
- Step 2** Click the **Create** button.
The Create Provider Regions window appears.
- Step 3** Enter the name and information for the Provider that you are creating. To enter the provider name follow these steps:
- a.** Click the **Select** button next to the Provider field.
A list of provider names appears.
 - b.** Click the radio button next to provider name and then **Select**.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customer Site window reappears.
-

Editing a Provider Regions

From the Edit Provider Regions window, you can modify the fields that have been specified for a particular provider region.

To access the Edit Provider Regions window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Provider Regions**.
The Provider Regions window appears.
- Step 2** Select a single site name to modify by checking the check box to the left of the PE Region Name.
- Step 3** Click the **Edit** button. This button is only enabled if a PE region name is selected.
The Edit Provider Region window appears.
- Step 4** Enter the changes you want to make to the selected provider region.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window.

Otherwise, click **Save**. The changes are then saved and the Provider Region window reappears.

Deleting Provider Regions

From the Delete window, you can remove selected provider regions from the database.

To access the Delete window, follow these steps:

- Step 1** Choose **Inventory > Resources > Provider Regions**.
The Provider Regions window appears.
- Step 2** Select one or more region to delete by checking the check box to the left of the PE Region Name.
- Step 3** Click the **Delete** button. This button is enabled only if one or more PE region name are selected.
The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window.
Otherwise, click **Delete** to confirm that you want to delete the region name(s) listed. The Provider Regions window reappears with the specified PE region name(s) deleted.
-

Provider Devices

The PE Devices feature provides a list of provider edge routers (PEs) that have been associated with the region, either through the PE editor or Inventory Manager.

This section covers the following topics:

- [Creating a Provider Devices, page 2-17](#)
- [Editing a Provider Devices, page 2-18](#)
- [Deleting Provider Devices, page 2-18](#)

Creating a Provider Devices

From the Create Provider Device window, you can create different PE regions.

To create a provider region, follow these steps:

- Step 1** Choose **Inventory > Resources > Provider Devices**.
The PE Devices window appears.
- Step 2** Click the **Create** button.
The Create New Provider Devices window appears.
- Step 3** To enter the Device Name follow these steps:
- a. Click the **Select** button next to the Device Name field.
A list of Device Name window appears.
 - b. Click the radio button next to device name and then **Select**.

- Step 4** To enter the PE Region Name follow these steps:
- a. Click the **Select** button next to the PE Region Name field.
A list of Region Name window appears.
 - b. Click the radio button next to device name and then **Select**.
- Step 5** Select the PE Role Type from drop-down list. The options are N-PE, U-PE, P, and PE-AGG.
- Step 6** Check the check box next to the 6VPE.
- Step 7** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Provider Device window reappears.
-

Editing a Provider Devices

From the Edit Provider Devices window, you can modify the fields that have been specified for a particular provider region.

To access the Edit Provider Devices window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Provider Devices**.
The PE Devices window appears.
- Step 2** Select a single site name to modify by checking the check box to the left of the Device Name.
- Step 3** Click the **Edit** button. This button is only enabled if a PE Device name is selected.
The Edit Provider Region window appears.
- Step 4** Enter the changes you want to make to the selected PE device name.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Provider Device window reappears.
-

Deleting Provider Devices

From the Delete window, you can remove selected provider device from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Provider Devices**.
The PE Devices window appears.
- Step 2** Select one or more region to delete by checking the check box to the left of the Device Name.
- Step 3** Click the **Delete** button. This button is enabled only if one or more PE Device name are selected.
The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the provider device(s) listed. The Provider Devices window reappears with the specified provider device(s) deleted.
-

Using the Inventory Manager Window

To access the Inventory Manager, choose **Inventory > Physical Inventory > Inventory Manager**.

From the Inventory Manager window you can import devices or open a list of devices, providers, or customers.

This section covers the following topics:

- [Importing Devices, page 2-19](#)
- [Opening and Editing Devices, page 2-19](#)
- [Opening and Editing PEs, page 2-20](#)
- [Opening and Editing CEs, page 2-21](#)
- [Assigning Devices, page 2-26](#)

Importing Devices

To import a device, it must be in an existing directory on the same server that is running Prime Provisioning. After a device is imported into the Prime Provisioning repository, you can assign it to a customer or provider, if desired.

To import devices with configuration files, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Inventory Manager**.
 - Step 2** Click the **Import Devices** button.
The Import Devices from Configuration Files window appears.
 - Step 3** Click the **Select** button.
The Select Device Configuration File window appears.
 - Step 4** At the **Select Device Configuration File** window, enter the directory on the Prime Provisioning server where the configuration files reside, and the **Import Devices from Configuration Files** window appears.
 - Step 5** Select as many of the configuration files as you want to import by checking the box to the left of the Configuration File name.
 - Step 6** If you want to import devices from more than one directory, you can repeat Steps 3 through 6.
 - Step 7** Click **Import**.
The **General Attributes** window appears with the added information.
 - Step 8** Click **Save**.
-

Opening and Editing Devices

To open device configuration files to bulk edit, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Inventory Manager**.
 - Step 2** Click the **Open** button.

The **Open** drop-down list appears. The **Open** options include the following:

- **Devices**—Every network element that Prime Provisioning manages.



Note To edit a PE, **Open Provider**, *not* **Open Devices**.

- **Provider**—PEs belonging to a specific provider.
- **Customer**—CEs belonging to a specific customer.

Step 3 Select **Devices**.

The Device Select Picker appears.

Step 4 Select a device to open by checking the check box to the left of the Device Name. You can select more than one device to open.

Step 5 Click the **Select** button.

The General Attributes window appears containing information on the selected devices.

Step 6 To view specific attributes click the **Attributes** button.

The Attributes options window appears.

Step 7 Select the type of attribute to display.

See the following sections for descriptions of these attribute fields.

- [General Attributes, page 2-22](#)
- [Password Attributes, page 2-23](#)
- [SNMP Attributes, page 2-23](#)
- [Platform Attributes, page 2-24](#)
- [Interfaces, page 2-24](#)

Step 8 To bulk edit an attribute, do the following:

- Check the one or more boxes to the left of the Device Name.
- Check the check box above the attribute name column.
- Click the **Edit** button.

Step 9 Enter the changes you want to make.

Step 10 Click **Save**.

The changes are saved.

Opening and Editing PEs

To open PE files to bulk edit, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Inventory Manager**.

Step 2 Click the **Open** button.

The **Open** drop-down list appears. The **Open** options include the following:

- **Devices**—Every network element that Prime Provisioning manages.

- **Provider**—PEs belonging to a specific provider.
 - **Customer**—CEs belonging to a specific customer.
- Step 3** Select **Provider**.
The Select Provider window appears.
- Step 4** Select a provider by clicking the radio button to the left of the Provider Name.
- Step 5** Click the **Select** button.
The General Attributes Provider window appears showing the PEs assigned to the selected provider.
- Step 6** To view specific attributes click the **Attributes** button.
The Attributes options window appears.
- Step 7** Select the type of attribute to display.
See the following sections for descriptions of these attribute fields.
- [General Attributes, page 2-22](#)
 - [Password Attributes, page 2-23](#)
 - [SNMP Attributes, page 2-23](#)
 - [Platform Attributes, page 2-24](#)
 - [Platform Attributes, page 2-24](#)
 - [PE Attributes, page 2-25](#)
 - [Interfaces, page 2-24](#)
- Step 8** To bulk edit an attribute, do the following:
- a. Check the one or more boxes to the left of the Host or Device Name.
 - b. Check the check box above the attribute name column.
 - c. Click the **Edit** button.
- Step 9** Enter the changes you want to make.
- Step 10** Click **Save**.
The changes are saved.
-

Opening and Editing CEs

To open CE files to bulk edit, follow these steps:

- Step 1** Choose **Inventory > Physical Inventory > Inventory Manager**.
- Step 2** Click the **Open** button.
The **Open** drop-down list appears. The **Open** options include the following:
- **Devices**—Every network element that Prime Provisioning manages.
 - **Provider**—PEs belonging to a specific provider.
 - **Customer**—CEs belonging to a specific customer.
- Step 3** Select **Customer**.

The Select Customer window appears.

Step 4 Select a customer by clicking the radio button to the left of the Customer Name.

Step 5 Click the **Select** button.

The General Attributes Customer window appears showing the CEs assigned to the selected customer.

Step 6 To view specific attributes click the **Attributes** button.

The Attributes Options window appears.

Step 7 Select the type of attribute to display.

See the following sections for descriptions of these attribute fields.

- [General Attributes, page 2-22](#)
- [Password Attributes, page 2-23](#)
- [SNMP Attributes, page 2-23](#)
- [Platform Attributes, page 2-24](#)
- [CPE Attributes, page 2-25](#)
- [Interfaces, page 2-24](#)

Step 8 To bulk edit an attribute, do the following:

- a. Check the one or more boxes to the left of the Host or Device Name.
- b. Check the check box above the attribute name column.
- c. Click the **Edit** button.

Step 9 Enter the changes you want to make.

Step 10 Click **Save**.

The changes are saved.

General Attributes

The General Attributes Devices window contains the following:

- **Host**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
 - Cisco Router
 - Catalyst OS device
 - Terminal server
 - IE2100 (Cisco Configuration Engine server)
- **Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management IP Address**—Valid IP address of the device that Prime Provisioning uses to configure the target router device. This IP address must be reachable from the Prime Provisioning host.

- **Device Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Terminal Session Protocol**—Configures the method of communication between Prime Provisioning and the device. Choices include: Telnet, SSH version 1 (SSHv1), SSH version 2 (SSHv2), and RSH. Default: Telnet.
- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: Terminal
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Password Attributes

The Password Attributes Devices window contains the following:

- **Device Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by Prime Provisioning. However, collection and upload/download will not function without the Login User and Login Password, as Prime Provisioning will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by Prime Provisioning. However, collection and upload/download will not function without the Login User and Login Password, as Prime Provisioning will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable User**—Not required by Prime Provisioning. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by Prime Provisioning. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Community String RO**—Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW**—Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMP Attributes

The SNMP Attributes Devices window contains the following:

- **Device Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **SNMP Version**—Choices include: SNMP v1/v2c, and SNMP v3. The default value is determined by the setting in the DCPL property `SnmpService/defaultSNMPVersion`. See [Appendix G, “Property Settings”](#) for more details. (DCPL properties can be set in the software UI, see [Cisco Prime Provisioning 6.8 Administration Guide](#).)

- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User Name**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None, DES 56 and AES 128. Default: None.

Platform Attributes

The Platform Attributes Devices window contains the following:

- **Device Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number**—Should match what is configured on the target router device. Limited to 80 characters.

Interfaces

The Interfaces Devices window contains the following:

- **Host**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Interface Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required. Limited to 256 characters.
- **Interface Type**—Specifies the type of interface. It is a display-only field.
- **Interface Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.
- **Interface IP Address**—IPv4 address associated with this interface.

- **Interface IPv6 Address**—IPv6 address associated with this interface.
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Possible values are:
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY
 - FRAME_RELAY_IETF
 - HDLC
 - PPP
 - ATM
 - AAL5SNAP
 - AAL0
 - AAL5
 - AAL5MUX
 - AAL5NLPID
 - AAL2
 - ENCAP_QinQ
 - GRE
- **Port Type**—Choices include: Access, Trunk, Routed, and None.

PE Attributes

The PE Attributes Provider window contains the following:

- **Device Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Provider**—Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- **Region**—Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Role**—Choices include: N-PE, U-PE, P, PE_AGG.
- **Loopback Interface**—Loopback address is the IP address of any loopback interface on the device. You can select one of the loopback interfaces for this field and use the IP address on that loopback interface.
- **Managed**—Provisioned by Prime Provisioning. Check the check box for yes. Default is no.

CPE Attributes

The CPE Attributes Customer window contains the following:

- **Device Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Customer**—Lists the names of customers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by customer name.
- **Site**—Lists the names of sites. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by site name.
- **Management Type**—Choices include: Managed, Unmanaged, Managed - Management LAN, Unmanaged - Management LAN, Directly Connected, Directly Connected Management Host, Multi-VRF, and Unmanaged Multi-VRF.

Assigning Devices

To assign a device to a provider or customer, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Inventory Manager**.
- Step 2** Click the **Open** button.
The **Open** drop-down list appears.
- Step 3** Select **Devices**.
The Device Select Picker appears.
- Step 4** Select a device to open by checking the box to the left of the Device Name. You can select more than one device to open.
- Step 5** Click the **Select** button.
The General Attributes Devices window appears containing information on the selected devices.
- Step 6** Click the **Assign CE/PE** button.
- Step 7** Select **Customer** or **Provider**.
The corresponding **Select Customer** or **Select Provider** window appears.
- Step 8** Select the customer or provider to which you want to assign the device by checking the box to the left of the Customer or Provider Name.
- Step 9** Click the **Select** button.
If you assigned the device to a provider, the PE Attributes window appears. If you assigned the device to a customer, the CPE Attributes window appears.
- Step 10** To save the assigned devices to the Prime Provisioning repository, you must specify the Site in the CPE Attributes window or the Region in the PE Attributes window. Do the following:
- a. Check the one or more boxes to the left of the Device Name.
 - b. Check the check box above the **Site** or **Region** column.
 - c. Click the **Edit** button. The **Edit Attributes** window appears.
 - d. Click **Select**. The **Select Site** or **Select Region** window appears.
 - e. Select a site or region by checking the box to the left of the Site Name or Region Name.
 - f. Click **Save**.

Step 11 You can choose to edit attributes as desired. Enter any changes you want to make.

Step 12 Click **Save**.

The PE or CPE is saved to the Prime Provisioning repository.

Device Groups

Every network element that Cisco Prime Provisioning manages must be defined as a device in the system. After you have defined your network elements as devices, you can organize the devices into groups for collection and management purposes.

This section describes how to create, edit, and delete device groups and e-mail device group owners. This section includes the following topics:

- [Creating a Device Group, page 2-27](#)
- [Editing a Device Group, page 2-27](#)
- [Deleting Device Groups, page 2-28](#)
- [E-mailing a Device Group, page 2-28](#)

Creating a Device Group

From the Create Device Group window, you can create different device groups.

To create a device group, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Device Groups**.

The Device Groups window appears.

Step 2 Click the **Create** button.

The Create Device Group window appears.

Step 3 Enter the name and the description of the Device Group that you are creating.

Step 4 Click **Edit**.

The Select Group Members window appears.

Step 5 Select the devices that you want to be group members by checking the check box to the left of the device name.

Step 6 Click **OK**.

The Create Device Group window appears listing the selected devices.

Step 7 Click **Save**.

The Device Groups window reappears with the new device group listed.

Editing a Device Group

From the Edit Device Group window, you can modify the fields that have been specified for a particular device group.

To access the Edit Device Group window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Device Groups**.
 - Step 2** Select a single device group to modify by checking the check box to the left of the Device Group Name.
 - Step 3** Click the **Edit** button. This button is only enabled if a device group is selected.
The Edit Device Group window appears.
 - Step 4** Enter the changes you want to make to the selected device group.
 - Step 5** Click **Save**.
The changes are saved and the Device Groups window reappears.
-

Deleting Device Groups

From the Delete window, you can remove selected device groups from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Device Groups**.
The Device Groups window appears.
 - Step 2** Select one or more device groups to delete by checking the check box(es) to the left of the Device Group Names.
 - Step 3** Click the **Delete** button. This button is enabled only if one or more device groups are selected.
The Confirm Delete window appears.
 - Step 4** Click the **Delete** button to confirm that you want to delete the device group(s) listed.
The Device Groups window reappears with the specified device group(s) deleted.
-

E-mailing a Device Group

From the E-mail window, you can send a device report via e-mail to the owners of specified device groups.

To access the E-mail window, follow these steps:

-
- Step 1** Choose **Inventory > Physical Inventory > Device Groups**.
The Device Groups window appears.
 - Step 2** Select the device groups for which you want to send a device report by checking the check box to the left of the Device Group Name.
 - Step 3** Click the **E-mail** button. This button is only enabled if one or more device groups are selected.
The Send Mail to Device owners of selected groups window appears.
 - Step 4** Compose the e-mail that you want to send to the selected device group owners.
 - Step 5** Click **Send**.

The e-mail is sent and the Device Groups window reappears.

Ethernet Access Topology Information

This section covers the following topics:

- [Physical Rings, page 2-29](#)
- [Named Physical Circuits, page 2-31](#)

Physical Rings

The Physical Rings displays the capability to create a two-node ring. You can create an NPC Ring with a minimum of two devices.

This section describes how you can create, edit, and delete Physical Rings. This section includes the following topics:

- [Creating Physical Rings, page 2-29](#)
- [Editing Physical Rings, page 2-31](#)
- [Deleting Physical Rings, page 2-31](#)

Creating Physical Rings

Rings with two devices has the option to add more devices to the same ring through add or edit option.

To create physical rings, follow these steps:

Step 1 Choose **Inventory > Logical Inventory > Physical Rings**.

The Physical Circuits window appears.

Step 2 Click the **Create** button.

The Create Ring window appears. A ring has a minimum of two physical links that form a ring.



Note At any time, if you click **Cancel**, everything you have chosen disappears.

Step 3 Start with the first line, which represents the first physical link.

Step 4 In the **Source Device** column, click **Select source device** and a Select Source Device - CPE/PE window appears.



Note The CPE you choose *must* be a Multi-VRF CE.

Step 5 Click a radio button next to the device to be the source device for this physical link and then click **Select**. The Create Ring window reappears with the chosen **Source Device**.

**Note**

When choosing the **Source Device** for a physical link, this same choice is made for the **Destination Device** for the previous physical link (or the last physical link if you are choosing for the first physical link). For a selected device, do not select the same interface for the source and destination interface.

- Step 6** In the **Source Interface** column in this new version of the new Create Ring window, click **Select source interface** and a Select Source Interface window appears with a list of interfaces.
- Step 7** Click a radio button next to the interface to be the source interface for this physical link and then click **Select**. The Create Ring window reappears with the chosen **Source Interface**.
- Step 8** In the **Destination Device** column in this new version of the Create Ring window, click **Select destination device** and a Select Source Device — CPE/PE window appears.
- Step 9** Click a radio button next to the device to be the destination device for this physical link and then click **Select**.
- The Create Ring window reappears with the chosen **Destination Device**.

**Note**

When choosing the **Destination Device** for the a physical link, this same choice is made for the next **Source Device**. Do not choose the same Interface for these devices. The minimum number of devices that can participate in a ring is two.

- Step 10** In the **Destination Interface** column in this new version of the Create Ring window, click **Select destination interface** and the Select Source Interface window appears with a list of interfaces.
- Step 11** Click a radio button next to the interface to be the destination interface for this NPC and then click **Select**. The Create Ring window reappears with the chosen **Destination Interface**.
- Step 12** Repeat [Step 4](#) for the middle physical links and [Step 4](#) to [Step 7](#) for the last physical link.
- Step 13** If you want to insert an extra physical link in the ring, check the check box for the line that represents the physical link you want the new physical link to follow and click **Insert**. Implement [Step 4](#) to fill in the remaining entries in this new physical link.
- Step 14** If you want to delete a physical link in the ring but a minimum of three physical links will remain, check the check box for the line that represents the physical link you want to delete and click **Delete**.
- Step 15** If you want to establish additional cross links between non-adjacent devices in this ring, you can click **Edit Cross Links** in the Create Ring window, and you then view a new Create Ring window with no entry. Click the **Add** button and you can choose from the devices already in your ring. The result is a new entry in the Create Ring window with this device as the **Source Device**. Establish the Destination Device and Source and Destination Interfaces as you did when creating the ring. The choices of devices and interfaces is limited to those already established in your ring.

**Note**

To **Edit Cross Links**, a minimum of four devices is needed to form this ring.

- Step 16** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, when you have completed setting up your ring click **Save**. The new ring is added in Physical Rings window, and a green check for Succeeded appears. The new ring is identified by the source device-source interface.

- Step 17** To create a ring with more than three physical links, check the check box for the link in the Create Ring window to which you want to insert and the **Insert** button is then enabled. Proceed in adding links as explained in this section.
-

Editing Physical Rings

To edit physical rings, follow these steps:



Note If the specified Physical Ring is participating in any of the Named Physical Circuits, then you can not edit the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

- Step 1** Choose **Inventory > Logical Inventory > Physical Rings** and a window appears.
- Step 2** Check the check box next to the line that represents an NPC ring and then click **Edit**.
The Create Ring window appears with all the data for this ring. Proceed as in the [“Creating Physical Rings” section on page 2-29](#) to make any changes you want.
- Step 3** When you have the ring as you want it, click **Save**. The Physical Rings window appears with the appropriate name (source device-source interface) and a green check for Succeeded appears.
-

Deleting Physical Rings

Rings with more than two nodes has the option to transition to a two device ring by removal of the device from the ring topology through edit or delete option.

To delete physical rings, follow these steps:



Note If the specified NPC Ring is participating in any of the Named Physical Circuits, then you can not delete the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

- Step 1** Choose **Inventory > Logical Inventory > Physical Rings** and a window appears.
- Step 2** Check the check box(es) next to the line(s) that represent(s) NPC ring(s) that you want to delete and then click **Delete**.
- Step 3** Click **Cancel** if you change your mind about deleting the chosen ring(s) or click **Delete** to actually delete the ring.
The Physical Rings window appears with the remaining ring names and a green check for Succeeded appears.
-

Named Physical Circuits

Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or U-PE and an N-PE. The intermediate nodes of the NPCs can either be CPE or PE. They can be connected in a circular fashion forming a ring of devices, which is represented by an entity known as

NPC Rings. NPC Rings represent the circular topology between devices (CPE or PE) to the Named Physical Circuits. To create an NPC, you must specify how the source CPE/U-PE and the destination N-PE are connected and specify the intermediate nodes.

The connectivity of the NPCs is defined by specifying a set of devices serving as physical links; each device has two interfaces that are part of the NPC connections. The Incoming Interface defines the interface from the CE direction. The Outgoing Interface defines the interface toward the PE direction.

You can also add (meaning after the chosen device) or insert (meaning before the chosen device) an NPC Ring in the link.

Keep in mind the following when you are creating an NPC:

- In the Prime Provisioning software, the device you select can be any node in the link. The Prime Provisioning software only shows the appropriate devices. The first device *must* be a CPE or U-PE and the last device *must* be an N-PE.
- NPCs should be created before the MPLS multi-device, VPLS, or L2VPN service request is created with `cpe1` and `pe1`. So when you create the SR, you would select the policy, `cpe1`, `pe1`, and the NPC that defines the link between `cpe1` and `pe1`.

This section describes how you can create and delete NPCs and create, edit, and delete NPC Rings. This section includes the following topics:

- [Creating a Named Physical Circuit, page 2-32](#)
- [Deleting Named Physical Circuits, page 2-33](#)

Creating a Named Physical Circuit

To add an NPC physical link, follow these steps:

Step 1 Choose **Inventory > Logical Inventory > Named Physical Circuit**.

The Named Physical Circuit window appears.

Step 2 Click the **Create** button.

The Create a Named Physical Circuits window appears.

Each line represents a physical link and each physical link contains the following attributes:

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



Note Before adding a ring in an NPC, create a ring and save it in the repository, as explained in the [“Creating Physical Rings” section on page 2-29](#).



Note An NPC must have at least one link defined. The link must have two devices, an Incoming Interface, and an Outgoing Interface.

Step 3 Click **Add Device** or **Insert Device**.

The Device Select Picker appears.

- Step 4** Be sure that the drop-down list in **Show** is **CPE or PE**.
- Step 5** Click a radio button next to a device and then click **Select**. The Create a Named Physical Circuits window reappears with the chosen **Device**.
- Step 6** If you want to add a device to your NPC as the last item or after the item checked in the check box, click the **Add Device** button in the Create a Named Physical Circuit window and then add device and interface information as explained in the previous steps. If you want to insert a device to your NPC as the first item or before the item checked in the check box, click the **Insert Device** button in the Create a Named Physical Circuit window and then add device and interface information as explained in the previous steps.
- Step 7** In the **Outgoing Interface** column in this new version of the Create a Named Physical Circuit window, click **Select outgoing interface** and a window appears with a list of interfaces.
- Step 8** Click a radio button next to the interface to be the source interface for this NPC and then click **Select**. The Create a Named Physical Circuit window reappears with the chosen **Interface**.
- Step 9** In the **Incoming Interface** column in this new version of the Create a Named Physical Circuit window, click **Select incoming interface** and a window appears with a list of interfaces.
- Step 10** Click a radio button next to the interface to be the incoming interface for this NPC and then click **Select**. The Create a Named Physical Circuit window reappears with the chosen **Incoming Interface**.
- Step 11** If you created an NPC ring that you want to insert or add into this NPC, as explained in the [“Creating Physical Rings” section on page 2-29](#), you can click **Insert Ring** or **Add Ring** and the ring appears at the beginning or before the item checked in the check box for **Insert Ring** or the ring appears at the end or after the item checked in the check box for **Add Ring**.



Note When inserting a ring, select the source device of the ring that connects to a source device or an NPC and the destination device of the ring that connects to the destination device of the NPC.

If you have not created an NPC ring that you want to insert into this NPC, proceed to [Step 14](#).

- Step 12** Click a radio button next to the ring you choose and then click **Select**. The Create a Named Physical Circuit window reappears with the chosen **Ring**.
- Step 13** Select the missing devices and interfaces as explained in the [“Creating Physical Rings” section on page 2-29](#).
- Step 14** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The Create a Named Physical Circuit window reappears with the new NPC listed.
-

Deleting Named Physical Circuits

To delete NPC(s), follow these steps:

-
- Step 1** Choose **Inventory > Logical Inventory > Named Physical Circuits**.
The Named Physical Circuits window appears.
- Step 2** Select one or more NPCs to delete by checking the check box(es) on the left.
- Step 3** Click the **Delete** button.
The Delete NPC window appears.

**Note**

If the specified NPC is being used by any of the Service Requests, you will not be allowed to delete it. An error message appears explaining this.

- Step 4** Click the **Delete** button to confirm that you want to delete the NPCs listed.
The Named Physical Circuits window reappears with the specified NPCs deleted.
-

Managing Customer Premise Devices

This section includes the following topics:

- [Customers, page 2-34](#)
- [Customer Sites, page 2-35](#)
- [Customer Devices, page 2-37](#)

Customers

A customer site is a set of IP systems with mutual IP connectivity between them without the use of a VPN. Each customer site belongs to exactly one customer. A customer site can contain one or more (for load balancing) edge device routers. This section describes how to create, edit, and delete customers.

This section covers the following topics:

- [Creating a Customer, page 2-34](#)
- [Editing a Customer, page 2-35](#)
- [Deleting Customers, page 2-35](#)

Creating a Customer

From the Create Customer window, you can create different customers.

To create a customer, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Customers**.
The Customers window appears.
- Step 2** Click the **Create** button.
The Create Customer window appears.
- Step 3** Enter the name and information for the Customer that you are creating. Check the **Site of Origin Enabled** check box if you want this enabled.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customers window reappears.
-

Editing a Customer

From the Edit Customer window, you can modify the fields that have been specified for a particular customer.

To access the Edit Customer window, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Customers**.
The Customers window appears.
- Step 2** Select a single customer to modify by checking the check box to the left of the Customer Name.
- Step 3** Click the **Edit** button. This button is only enabled if a customer is selected.
The Edit Customer window appears.
- Step 4** Enter the changes you want to make to the selected customer.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customers window reappears.
-

Deleting Customers

From the Delete window, you can remove selected customers from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Customers**.
The Customers window appears.
- Step 2** Select one or more customers to delete by checking the check box to the left of the Customer Name.
- Step 3** Click the **Delete** button. This button is enabled only if one or more customers are selected.
The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the customer(s) listed. The Customers window reappears with the specified customer(s) deleted.
-

Customer Sites

The Customer Sites window feature is used to create, edit, and delete customer sites.

This section covers the following topics:

- [Creating a Customer Site, page 2-35](#)
- [Editing a Customer Site, page 2-36](#)
- [Deleting Customer Sites, page 2-36](#)

Creating a Customer Site

From the Create Customer Sites window, you can create different customer sites.

To create customer sites, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Customer Sites**.
The Customer Sites window appears.
- Step 2** Click the **Create** button.
The Create New Customer Sites window appears.
- Step 3** Enter the name and information for the Customer that you are creating. To enter the customer name follow these steps:
- a.** Click the **Select** button next to the Customer field.
A list of customer names appears.
 - b.** Click the radio button next to customer name and then **Select**.
- Step 4** Enter the Site Information.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customer Site window reappears.
-

Editing a Customer Site

From the Edit Customer Sites window, you can modify the fields that have been specified for a particular customer sites.

To access the Edit Customer Sites window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Customer Sites**.
The Customer Sites window appears.
- Step 2** Select a single site name to modify by checking the check box to the left of the Site Name.
- Step 3** Click the **Edit** button. This button is only enabled if a customer is selected.
The Edit Customer window appears.
- Step 4** Enter the changes you want to make to the selected customer site.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customer Site window reappears.
-

Deleting Customer Sites

From the Delete window, you can remove selected customer sites from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Customer Sites**.
The Customer Sites window appears.
- Step 2** Select one or more customer sites to delete by checking the check box to the left of the Site Name.
- Step 3** Click the **Delete** button. This button is enabled only if one or more customer sites are selected.

The Confirm Delete window appears.

- Step 4** Click **Cancel** if you do not want to delete this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the customer site(s) listed. The Customer Sites window reappears with the specified customer site(s) deleted.
-

Customer Devices

The CPE feature provides a list of CPEs that have been associated with a site through the CPE editor or Inventory Manager.

This section covers the following topics:

- [Create CPE Device, page 2-38](#)
- [Edit CPE Device, page 2-38](#)
- [Delete CPE Device, page 2-39](#)

Choose **Inventory > Resources > Customer Devices**, the CPE Devices window appears.

The CPE Devices window contains the following:

- **Device Name**—Lists the names of devices. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by device name.
- **Customer Name**—Lists the names of customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.
- **Site Name**—Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Management Type**—When associating a CE with a customer site, you can select Managed or Unmanaged. Other choices are available (see below), but they should not be confused with this primary choice.
 - **Managed**—A managed CE can be provisioned directly by the provider using Prime Provisioning. The CE must be reachable from an Prime Provisioning server.
 - **Unmanaged**—An unmanaged CE cannot be provisioned directly by the provider. If Unmanaged is selected, the provider can use Prime Provisioning to generate a configuration, and then send the configuration to the customer for placement on the CE.
 - **Managed - Management LAN**—A managed Management LAN or Management CE (MCE) is configured like a managed CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
 - **Unmanaged - Management LAN**—An unmanaged Management LAN or MCE is configured like an unmanaged CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
 - **Directly Connected**—In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.
 - **Directly Connected Management Host**—In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device, on which Prime Provisioning resides.

- Multi-VRF —A multi-VRF CE (MVRFCE) is owned by the customer, but resides in the provider space. It is used to offload traffic from the PE.
- Unmanaged Multi-VRF—An unmanaged multi-VRF CE is provisioned like an unmanaged CE (configurations are not uploaded or downloaded to the device by the provider). It is owned by the customer and resides in the provider space.



Note Unmanaged devices are subject to read-only based operations, but will not be interacted with for ready-write based operations.

Create CPE Device

From the Create Customer Devices window, you can create different CPE devices.

To create a CPE device, follow these steps:

Step 1 Choose **Inventory > Resources > Customer Devices**.

The Customer Devices window appears.

Step 2 Click **Create** to create new CPE devices. Enabled only if no customer site is selected.

The Create New CPE Device window appears.

Step 3 Click **Select** for the required **Device Name** and **Site Name**.

For each, you receive a list of the devices and sites, respectively, from which you can choose one in each window and then click **Select**. Click **Cancel** if you do not want to save this information, and you will proceed to the previous window.



Note The Customer Name is displayed only if the customer site is created.

Step 4 The drop-down window for **Management Type** allows you choose the management type of the CPE device you are creating.

Step 5 Click **Cancel** if you do not want to save this information, and you will proceed to the previous window.

Otherwise, click **Save**. The changes are saved and the CPE Device window reappears.

Edit CPE Device

From the Edit Customer Device window, you can modify the fields that have specified for a particular CPE device.

To edit a CPE device, follow these steps:

Step 1 Choose **Inventory > Resources > Customer Devices**.

The Customer Devices window appears.

Step 2 Select a single device name to modify by checking the check box to the left of the Device Name.

Step 3 Click the **Edit** button. This button is only enabled if a device name is selected.

The Edit Customer window appears.

Step 4 Enter the changes you want to make to the selected CPE device.

- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customer Device window reappears.
-

Delete CPE Device

From the Delete window, you can remove selected customer device from the database.

To access the Delete window, follow these steps:

- Step 1** Choose **Inventory > Resources > Customer Devices**.
The Customer Devices window appears.
- Step 2** Select one or more device name to delete by checking the check box to the left of the Device Name.
- Step 3** Click the **Delete** button. This button is enabled only if one or more device names are selected.
The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the device name(s) listed. The Customer Devices window reappears with the specified device name(s) deleted.
-

Setting Up Resources

This section explains how to set up the resources. It contains the following sections:

- [Access Domains, page 2-39](#)
- [Interface Access Domains, page 2-41](#)
- [Resource Pools, page 2-43](#)
- [Route Targets, page 2-51](#)

Access Domains

To access the Access Domains window: Choose **Inventory > Resources > Access Domains**.

From the Access Domains window, you can create, edit, or delete access domains.

This sections covers the following topics:

- [Creating Access Domains, page 2-39](#)
- [Editing Access Domains, page 2-40](#)
- [Deleting Access Domains, page 2-40](#)

Creating Access Domains

From the Create Access Domains window, you can create different access domain.

To create a access domain, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Access Domains**.
The Access Domains window appears.
- Step 2** Click the **Create** button.
The Create New Access Domains window appears.
- Step 3** Enter the access domain name. This is a required field.
- Step 4** To enter the Provider follow these steps (this is a required field):
- a. Click the **Select** button next to the Provider field.
A list of Provider Name window appears.
 - b. Click the radio button next to provider name and then **Select**.
- Step 5** Enter the PEs information (required field). This information about the PE will be helpful to the access domain operators. Limited to 256 characters.
- Step 6** Enter the Reserved VLAN information (this is optional).
- Step 7** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Access Domains window reappears.
-

Editing Access Domains

From the Edit Access Domains window, you can modify the fields that have been specified for a particular provider region.

To access the Edit Access Domains window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Access Domains**.
The Access Domains window appears
- Step 2** Select a single access domain to modify by checking the check box to the left of the Access Domains Name.
- Step 3** Click the **Edit** button. This button is only enabled if a access domain name is selected.
The Edit Access Domains window appears.
- Step 4** Enter the changes you want to make to the selected access domain.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Access Domains window reappears.
-

Deleting Access Domains

From the Delete window, you can remove selected access domain from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Access Domains**.
The Access Domains window appears

- Step 2** Select one or more access domain to delete by checking the check box to the left of the Access domain Names.
- Step 3** Click the **Delete** button. This button is enabled only if one or more access domains are selected. The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the access domain(s) listed. The Access Domains window reappears with the specified access domain(s) deleted.
-

Interface Access Domains

To access the Interface Access Domains window: Choose **Inventory > Resources > Interface Access Domains**.

From the Access Domains window, you can create, edit, or delete access domains.

This sections covers the following topics:

- [Creating Interface Access Domains, page 2-41](#)
- [Editing Interface Access Domains, page 2-42](#)
- [Deleting Interface Access Domains, page 2-42](#)



Note

Outer VLAN ID resource pools can be created once the Interface Access Domains is created.

Creating Interface Access Domains

From the Create Interface Access Domains window, you can create different interface access domains.

To create an interface access domain, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Interface Access Domains**.
The Interface Access Domains window appears.
- Step 2** Click the **Create** button.
The Create New Interface Access Domains window appears.
- Step 3** Enter the interface access domain name. This is a required field.
- Step 4** To enter the Provider follow these steps (this is a required field):
- a. Click the **Select** button next to the Provider field.
A list of Provider Name window appears.
 - b. Click the radio button next to provider name and then **Select**.
- Step 5** Select the PE device (required field) from the list of Provider devices available for the selected Provider.
- Step 6** Select the Interfaces (required field) from the interface pop-up window. Interface pop-up window displays all available EVC supported physical ports from the selected NPE device.



Note Single interface or group multiple interfaces can be selected based on the requirements.

- Step 7** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Interface Access Domains window reappears.
-

Editing Interface Access Domains

From the Edit Interface Access Domains window, you can modify the fields that have been specified for a particular provider region.

To access the Edit Interface Access Domains window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Interface Access Domains**.
The Interface Access Domains window appears
- Step 2** Select a single interface access domain to modify by checking the check box to the left of the Interface Access Domains Name.
- Step 3** Click the **Edit** button. This button is only enabled if an interface access domain name is selected.
The Edit Access Domains window appears.
- Step 4** Enter the changes you want to make to the selected interface access domain.
- Step 5** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Interface Access Domains window reappears.
-

Deleting Interface Access Domains

From the Delete window, you can remove selected access domain from the database.

To access the Delete window, follow these steps:

-
- Step 1** Choose **Inventory > Resources > Interface Access Domains**.
The Interface Access Domains window appears.
- Step 2** Select one or more access domain to delete by checking the check box to the left of the Interface Access Domain Names.
- Step 3** Click the **Delete** button. This button is enabled only if one or more access domains are selected.
The Confirm Delete window appears.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** to confirm that you want to delete the access domain(s) listed. The Interface Access Domains window reappears with the specified access domain(s) deleted.
-

Resource Pools

Prime Provisioning enables multiple pools to be defined and used during operations. The following resource pools are available:

- **IP address pool:** The IP address pool can be defined and assigned to regions or VPNs. This feature gives the service operator the flexibility to manage the allocation of all IP addresses in the network.
- **Multicast pool:** The Multicast pool is used for Multicast MPLS VPNs.
- **Route Target (RT) pool:** A route target is the MPLS mechanism that informs PEs as to which routes should be inserted into the appropriate VRFs. Every VPN route is tagged with one or more route targets when it is exported from a VRF and offered to other VRFs. The route target can be considered a VPN identifier in MPLS VPN architecture. RTs are a 64-bit number.
- **Route Distinguisher (RD) pool:** The IP subnets advertised by the CE routers to the PE routers are augmented with a 64-bit prefix called a route distinguisher (RD) to make them unique. The resulting 96-bit addresses are then exchanged between the PEs, using a special address family of Multiprotocol BGP (referred to as MP-BGP). The RD pool is a pool of 64-bit RD values that Prime Provisioning uses to make sure the IP addresses in the network are unique.
- **Site of origin pool:** The pool of values for the site-of-origin (SOO) attribute. The site-of-origin attribute prevents routing loops when a site is multihomed to the MPLS VPN backbone. This is achieved by identifying the site from which the route was learned, based on its SOO value, so that it is not readvertised back to that site from a PE in the MPLS VPN network.
- **VC ID pool:** VC ID pools are defined with a starting value and a size of the VC ID pool. (VC ID is a 32-bit unique identifier that identifies a circuit/port.) A given VC ID pool is not attached to any Inventory object. During the deployment of an Ethernet Service (EWS, ERS for example), VC ID is auto-allocated from the VC ID pool.
- **VLAN ID pool:** VLAN ID pools are defined with a starting value and a size of the VLAN pool. A given VLAN ID pool can be attached to an Access Domain. During the deployment an Ethernet Service (EWS, ERS for example), VLAN ID can be auto-allocated from the Access Domain's VLAN pools. This gives the Service Provider a tighter control of VLAN ID allocation.

All these resources, that are made available to the service provider, enable the automation of service deployment.

This section describes how you can create and manage pools for various types of resources. This section includes the following topics:

- [Creating an IP Address Pool, page 2-44](#)
- [Creating an IPv6 Address Pool, page 2-44](#)
- [Creating a Multicast Pool, page 2-45](#)
- [Creating a Route Distinguisher and Route Target Pool, page 2-46](#)
- [Creating a Site of Origin Pool, page 2-47](#)
- [Creating a VC ID Pool, page 2-48](#)
- [Creating a VLAN Pool, page 2-49](#)
- [Creating an EVC Outer VLAN Pool, page 2-49](#)
- [Creating an EVC Inner VLAN Pool, page 2-50](#)
- [Deleting Resource Pools, page 2-51](#)

Creating an IP Address Pool

Prime Provisioning uses IP address pools to automatically assign IP addresses to PEs and CEs. Each Region has an IP address pool to use for IP numbered addresses (/30 and /31 pools) and a separate IP address pool for IP unnumbered addresses (/32 loopback address pools).

Within a VPN or extranet, all IP addresses must be unique. Customer IP addresses must not overlap with the provider's IP addresses. Overlapping IP addresses are only possible when two devices cannot see each other—that is, when they are in isolated VPNs.

From the Create IP Address Pool window, you can create IP address pools.

To create an IP address pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **IPv4 Address** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New IP Address Resource Pool window appears.

The Create New IP Address Resource Pool window contains the following fields:

- **IP Address Pool** (required)—Text field in the format a.b.c.d/mask, for example 172.0.0.0/8.
- **Pool Mask (bits)** (required)—Choices include: **30**, **31** and **32**

where:

30 and **31** are used for IP numbered address pools (/30 and /31)

32 is used for IP unnumbered loopback address pools (/32).

- **Pool Association** (required)—Choices include: **Region**, **VPN**, and **Customer** from the drop-down list. Then you can click the **Select** button to receive all selections for the choice you made in the drop-down list. From this new window, make your selection and click **Select**.



Note If you choose **VPN**, an additional optional field appears, **Pool Name Suffix**. This field allows the creation of multiple address pools within the same VPN. If you are creating this address pool for DMVPN usage, the recommendation is to use this field to specify a suffix.

- **Pool Name Suffix** (optional)—Suffixes are used to make a pool name unique. You can append this IP Address Pool to an existing pool by selecting a previously defined suffix, or click **New** to create a new pool.

Step 4 Enter the required information for the IP address pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new IP address pool listed.

Creating an IPv6 Address Pool

Prime Provisioning uses IPv6 address pool to automatically assign IPv6 addresses to PEs and CEs. Each Region has an IPv6 address pool to use for IPv6 numbered addresses (/64, /126 and /127 pools).

From the Create New IPv6 Address Resource Pool window, you can create IPv6 address pool.

To create an IPv6 address pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **IPv6 Address** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New IPv6 Address Resource Pool window appears.

The Create New IPv6 Address Resource Pool window contains the following fields:

- **IPv6 Address Pool** (required)—IPv6 Address/Mask, text field in the format a:b:c:d:e:f:g:h/i, for example 2003:adbc:99ff:5623:9023::/120.
- **Pool Mask (bits)** (required)—Choices include: 64, 126, and 127.
- **Pool Association** (required)—Choice: only **Region** from the drop-down list.

Provides option to select a Region and associate IPv6 Pool to a particular Region. Select **Region** from the drop-down list, then click the **Select** button. From this new window, select the particular Region, and then click **Select**.

Step 4 Enter the required information for the IPv6 address pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new IPv6 address pool listed.

Creating a Multicast Pool

From the Create Multicast Pool window, you can create multicast pools. These pools are global and are not associated with any provider or customer.

To create a multicast pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **Multicast** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New Multicast Resource Pool window appears.

The Create New Multicast Resource Pool window contains the following fields:

- **Multicast Address** (required)—Text field in the format **a.b.c.d/mask**, for example 239.0.0.0/8. Range: 224.0.1.0/8 to 239.255.255.255/32.
- **Use for default MDT** (optional)—This is a check box. Default: selected.
- **Use for Data MDT** (optional)—This is a check box. The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT. Default: selected.

Step 4 Enter the required information for the multicast pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new multicast pool listed.

Creating a Route Distinguisher and Route Target Pool

MPLS-based VPNs employ Border Gateway Protocol (BGP) to communicate between PEs to facilitate customer routes. This is made possible through extensions to BGP that carry addresses other than IPv4 addresses. A notable extension is called the route distinguisher (RD).

The purpose of the route distinguisher (RD) is to make the prefix value unique across the network backbone. Prefixes should use the same RD if they are associated with the same set of route targets (RTs) and anything else that is used to select routing policy. The community of interest association is based on the route target (RT) extended community attributes distributed with the Network Layer Reachability Information (NLRI). The RD value must be a globally unique value to avoid conflict with other prefixes.

The MPLS label is part of a BGP routing update. The routing update also carries the addressing and reachability information. When the RD is unique across the MPLS VPN network, proper connectivity is established even if different customers use non-unique IP addresses.

For the RD, every CE that has the same overall role should use a VRF with the same name, same RD, and same RT values. The RDs and RTs are only for route exchange between the PEs running BGP. That is, for the PEs to do MPLS VPN work, they have to exchange routing information with more fields than usual for IPv4 routes; that extra information includes (but is not limited to) the RDs and RTs.

From the Create Route Distinguisher Pool window, you can create route distinguisher pools.

Create a Route Distinguisher Pool

To create a route distinguisher pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **Route Distinguisher** from the **Pool Type** in the upper left of the Resource Pools window.**Step 3** Click the **Create** button.

The Create New Route Distinguisher Resource Pool window appears.

The Create New Route Distinguisher Resource Pool window contains the following fields:

- **RD Pool Start** (required)—Range: 0 to 2147483646.
- **RD Pool Size** (required)—Range: 1 to 2147483647.
- **Provider** (required)

**Note**

When a new VRF object is created using Autopick RD option or when a service request is created using VPN, Prime Provisioning picks the RD start value of the provider and reduces RD pool size value by one. The current limitation is that this value never returns back to the pool even if the corresponding VRF or service request gets deleted.

Step 4 Enter the **RD Pool Start** and **Size** information for the route distinguisher pool you are creating.

- Step 5** Click the **Select** button.
The Provider for new Resource Pool window appears.
- Step 6** Select one of the providers listed and click **Select**.
- Step 7** Click **Save**.
The Resource Pools window reappears with the new route distinguisher pool listed.
-

Create a Route Target Pool

To create a Route Target Pool, follow these steps:

- Step 1** Choose **Service Design > Resources > Resource Pools**.
The Resource Pools window appears.
- Step 2** Select **Route Target** from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Click the **Create** button.
The Create New Route Target Resource Pool window appears.
The Create New Route Target Resource Pool window contains the following fields:
- **RT Pool Start** (required)—Range: 0 to 2147483646.
 - **RT Pool Size** (required)—Range: 1 to 2147483647.
 - **Provider** (required)
- Step 4** Enter the **RT Pool Start** and **Size** information for the route target pool you are creating.
- Step 5** Click the **Select** button.
The Provider for new Resource Pool window appears.
- Step 6** Select one of the providers listed and click **Select**.
- Step 7** Click **Save**.
The Resource Pools window reappears with the new route target pool listed.
-

Creating a Site of Origin Pool

In MPLS VPN, CE sites use private/public AS numbers and when one AS number is used for each VPN, all sites belonging to the same VPN share the same private/public AS number. The default BGP behavior is to drop any prefix if its own AS number is already in the AS path. As a result, a customer site does not learn prefixes of a remote site in this situation. AS-OVERRIDE must be configured (if there are hub sites involved, ALLOWAS-IN must be configured) to allow those prefixes to be sent by PE routers but a routing loop can occur.

For example, CE1 and CE2 belong to the same customer VPN and have the same AS number 65001. The AS path between two customer sites is 65001 - 1234 - 65001 and prefixes cannot be exchanged between customer sites because AS 65001 is already in the path. To solve this problem, AS-OVERRIDE options are configured on PE routers; but it introduces a routing loop into the network without using extended community site of origin attributes.

Site of origin is a concept in MPLS VPN architecture that prevents routing loops in sites that are multi-homed to the MPLS VPN backbone and in sites using AS-OVERRIDE in conjunction. Site of origin is a type of BGP extended community attribute used to identify a prefix that originated from a site so that the re-advertisement of that prefix back to the site can be prevented. This attribute uniquely identifies the site from which the PE router learned the route. Site of origin is tagged at PE in peering with BGP neighbors using an inbound route-map and works in conjunction with BGP CE-PE routing protocol.

Site of origin must be unique per customer site per VPN/customer (when these sites are multi-homed). Therefore, the same value of site of origin must be used on PE routers connected to the same CE router or to the same customer site.

**Note**

Each time a customer site is created, Prime Provisioning generates a unique site of origin value from the selected site of origin provider pool if Site of Origin is enabled. This site of origin value must be unique per customer site per customer/VPN.

From the Create Site of Origin Pool window, you can create site of origin pools.

To create a site of origin pool, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Resource Pools**.
The Resource Pools window appears.
- Step 2** Select **Site of Origin** from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Click the **Create** button.
The Create New Site of Origin Resource Pool window appears.
The Create New Site of Origin Resource Pool window contains the following fields:
- **SOO Pool Start** (required)—Range: 0 to 2147483646.
 - **SOO Pool Size** (required)—Range: 1 to 2147483647.
 - **Provider** (required)
- Step 4** Enter the **SOO Pool Start** and **Size** information for the site of origin pool you are creating.
- Step 5** Click the **Select** button.
The Provider for new Resource Pool window appears.
- Step 6** Select one of the providers listed and click **Select**.
- Step 7** Click **Save**.
The Site of Origin pools window reappears with the new route target pool listed.
-

Creating a VC ID Pool

From the Create VC ID Pool window, you can create VC ID pools. These pools are global and are not associated with any provider or customer

To create a VC ID pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **VC ID** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New VC ID Resource Pool window appears.

The Create New VC ID Resource Pool window contains the following fields:

- **VC Pool Start** (required)—Range: 1 to 2147483646.
- **VC Pool Size** (required)—Range: 1 to 2147483647.

Step 4 Enter the required information for the site of origin pool you are creating.

Step 5 Click **Save**.

The VC ID Pools window reappears with the new VC ID pool listed.

Creating a VLAN Pool

From the Create VLAN Pool window, you can create VLAN pools.

To create a VLAN pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **VLAN** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New VLAN Resource Pool window appears.

The Create New VLAN Resource Pool window contains the following fields:

- **VLAN Pool Start** (required)— Range: 1 to 4094.
- **VLAN Pool Size** (required)—Range: 1 to 4094.
- **Access Domain** (required)

Step 4 Enter the **VLAN Pool Start** and **Size** information for the VLAN pool you are creating.

Step 5 Click the **Select** button.

The Access Domain for new VLAN Pool window appears.

Step 6 Select one of the access domains listed and click **Select**.

Step 7 Click **Save**.

The VLAN Pools window reappears with the new VLAN pool listed.

Creating an EVC Outer VLAN Pool

From the Create EVC OUTER VLAN Pool window, you can create EVC OUTER VLAN pools.

To create an OUTER VLAN pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **EVC OUTER VLAN** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New OUTER VLAN Resource Pool window appears.

The Create New OUTER VLAN Resource Pool window contains the following fields:

- **OUTER VLAN Pool Start** (required)— Range: 1 to 4094.
- **OUTER VLAN Pool Size** (required)—Range: 1 to 4094.
- **Interface Access Domain** (required)

Step 4 Enter the **OUTER VLAN Pool Start** and **Size** information for the OUTER VLAN pool you are creating.

Step 5 Click the **Select** button.

The Select Interface Access Domain for new OUTER VLAN Pool window appears.

Step 6 Select one of the interface access domains listed and click **Select**.

Step 7 Click **Save**.

The OUTER VLAN Pools window reappears with the new OUTER VLAN pool listed.

Creating an EVC Inner VLAN Pool

From the Create EVC Inner VLAN Pool window, you can create EVC INNER VLAN pools.

To create an INNER VLAN pool, follow these steps:

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

The Resource Pools window appears.

Step 2 Select **EVC INNER VLAN** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create New INNER VLAN Resource Pool window appears.

The Create New INNER VLAN Resource Pool window contains the following fields:

- **INNER VLAN Pool Start** (required)— Range: 1 to 4094.
- **INNER VLAN Pool Size** (required)—Range: 1 to 4094.
- **Interface Access Domain** (required)

Step 4 Enter the **INNER VLAN Pool Start** and **Size** information for the **INNER VLAN** pool you are creating.

Step 5 Click the **Select** button.

The Select Interface Access Domain for new **INNER VLAN** Pool window appears.

Step 6 Select one of the interface access domains listed and click **Select**.

Step 7 Click **Save**.

The **INNER VLAN** Pools window reappears with the new **INNER VLAN** pool listed.

Deleting Resource Pools

From the Resource Pool window, you can delete specific resource pools.

To delete resource pools, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Resource Pools**.
- The Resource Pools window appears.
- Step 2** Select a pool type from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Select one or more resource pools to delete by checking the check box(es) to the left of the resource pool(s).
- Step 4** Click the **Delete** button.
- A Confirm Delete window appears.
- Step 5** Click the new **Delete** button to confirm that you want to delete the resource pool(s) listed.
- The Resource Pools window reappears with the specified pool(s) deleted.
-

Route Targets

A VPN can be organized into subsets called *Route Targets*. A Route Target describes how the CEs in a VPN communicate with each other. Thus, Route Targets describe the logical topology of the VPN. Prime Provisioning can be employed to form a variety of VPN topologies between CEs by building hub and spoke or full mesh CE routing communities. Route Targets are building blocks that allow you to form complex VPN topologies and CE connectivity.

The most common types of VPNs are *hub-and-spoke* and *full mesh*.

- A hub-and-spoke Route Target is one in which one or a few CEs act as hubs, and all spoke CEs talk only to or through the hubs, never directly to each other.
- A full mesh Route Target is one in which every CE connects to every other CE.

These two basic types of VPNs—full mesh and hub and spoke—can be represented with a single Route Target. Whenever you create a VPN, the Prime Provisioning software creates one default Route Target for you. This means that until you need advanced customer layout methods, you will not need to define new Route Targets. Up to that point, you can think of a Route Target as standing for the VPN itself—they are one and the same. If, for any reason, you must override the software's choice of route target values, you can do so only at the time you create a Route Target in the Prime Provisioning software.

To build very complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed, or has a hub and spoke pattern. (Note that a CE can be in more than one group at a time, if each group has one of the two basic patterns.) Each subgroup in the VPN wants its own Route Target. Any CE that is only in one group just joins the corresponding Route Target (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, the provisioning software does the rest, assigning route target values and VRF tables to arrange exactly the connectivity the customer requires. You can use the Topology tool to double-check the Route Target memberships and resultant VPN connectedness.

Prime Provisioning supports multiple CEs per site and multiple sites connected to the same PE. Each Route Target has unique route targets (RT), route distinguisher (RD), and VPN Routing and Forwarding instance (VRF) naming. After provisioning a Route Target, it is a good idea to run the audit reports to verify the Route Target deployment and view the topologies created by the service requests. The product supports linking two or more CE routing communities in the same VPN.

This section describes how you can create and manage CE routing communities. This section includes the following topics:

- [Creating Route Targets, page 2-52](#)
- [Deleting Route Targets, page 2-53](#)

Creating Route Targets

When you create a VPN, the Prime Provisioning software creates one default Route Target for you. But if your network topology and configuration require customized Route Target definitions, you can define Route Targets customized for your network.



Tip

Customized Route Targets should be defined only in consultation with the VPN network administrator. To build complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed or has a hub-and-spoke pattern. A CE can be in more than one group at a time, as long as each group has one of the two basic configuration patterns.

Each subgroup in the VPN wants its own Route Target. Any CE that is only in one group just joins the corresponding Route Target (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, Prime Provisioning does the rest, assigning route target values and VRF tables to arrange the precise connectivity the customer requires.

To create a CE routing community, follow these steps:

-
- Step 1** Choose **Service Design > Resources > Route Targets**.
- The Route Targets window appears.
- Step 2** Click **Create**.
- The Create CE Routing Community window appears.
- Step 3** Complete the Route Target fields as required for the CE Routing Community:
- Provider Name** (required)—To specify the service provider associated with this Route Target, click **Select**.
The Select Provider window appears.
 - From this new window, choose the name of the service provider, then click **Select**.
 - Name** (required)—Enter the name of the Route Target.
 - Route Target Type**—Specify the Route Target type: Hub and Spoke or Fully Meshed.
 - Auto-Pick Route Target Values**—Choose to either let Prime Provisioning automatically set the route target (RT) values or set the RT values manually.
By default, the **Auto-pick route target values** check box is checked. If you uncheck the check box, you can enter the Route Target values manually.

**Caution**

If you choose to bypass the **Auto-pick route target values** option and set the route target (RT) values manually, note that the RT values cannot be edited after they have been defined in the Prime Provisioning software.

Step 4 When you have finished entering the information in the Create CE Routing Community window, click **Save**.

After creating the Route Target, you can add it to the VPN.

Deleting Route Targets

From the CE Routing Community window, you can delete specific Route Targets.

To delete Route Target(s), follow these steps:

Step 1 Choose **Service Design > Resources > Route Targets**.

The Route Targets window appears.

Step 2 Select Route Target(s) to delete by checking the check box(es) to the left of the Route Target name.

Step 3 Click the **Delete** button.

The Confirm Delete window appears.

Step 4 Click **OK** to confirm that you want to delete the Route Target(s) listed.

The Route Targets window reappears with the specified Route Target(s) deleted.

Setting Up Logical Inventory

VPNs

At its simplest, a virtual private network (VPN) is a collection of sites that share the same routing table. A VPN is also a framework that provides private IP networking over a public infrastructure such as the Internet. In Prime Provisioning MPLS VPN Management, a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is defined by a set of administrative policies.

A VPN is a network in which two sites can communicate over the provider's network in a private manner; that is, no site outside the VPN can intercept their packets or inject new packets. The provider network is configured such that only one VPN's packets can be transmitted through that VPN—that is, no data can come in or out of the VPN unless it is specifically configured to allow it. There is a physical connection from the provider edge network to the customer edge network, so authentication in the conventional sense is not required.

This section describes how you can create and manage pools for various types of resources. This section includes the following topics:

- [Creating a VPN, page 2-54](#)
- [Deleting VPNs, page 2-56](#)

Creating a VPN

To create a VPN, follow these steps:

Step 1 Choose **Inventory > Logical Inventory > VPN**.

The VPNs window appears.

Step 2 Click **Create**.

The Create VPN window appears.

Step 3 Complete the fields as required for the VPN:

- a. **Name** (required)—Enter the name of the VPN, any name of your choice.
- b. **Customer** (required)—To select the customer associated with this VPN, choose **Select**.
- c. From the list of customers, select the appropriate customer, then click **Select**.
- d. If you want MPLS attributes, complete the fields in the MPLS Attributes section of the window. For VPLS, skip to step **aa**.
- e. **Create Default Route Targets** (optional)—To create a default Route Targets, check the **Create Default Route Targets** check box and select a provider.
- f. **Enable Unique Route Distinguisher**—The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature is enabled only under the IPv4 VRF address family configuration mode. When enabled, this feature can perform load balancing on eBGP and/or iBGP paths that are imported into the VRF.
- g. **Enable IPv4 Multicast** —To enable multicast IPv4 VPN routing, check the **Enable IPv4 Multicast** check box.

An IP address that starts with the binary prefix *1110* is identified as a *multicast group address*. There can be more than one sender and receiver at any time for a given multicast group address. The senders send their data by setting the group address as the destination IP address. It is the responsibility of the network to deliver this data to all the receivers in the network who are listening to that group address.



Note Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools.

- h. **Enable IPv6 Multicast** —To enable multicast IPv6 VPN routing, check the **Enable IPv6 Multicast** check box.

An IP address that starts with the binary prefix *1110* is identified as a *multicast group address*. There can be more than one sender and receiver at any time for a given multicast group address. The senders send their data by setting the group address as the destination IP address. It is the responsibility of the network to deliver this data to all the receivers in the network who are listening to that group address.



Note Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools.

- i. **Enable Auto Pick MDT Addresses** (optional)—Check this check box to use **Default MDT Address** and **Default MDT Subnet** values from a multicast resource pool.

- j. **Default MDT Address**—If **Enable Auto Pick MDT Addresses** is set on, **Default MDT Address** is required.
- k. **Data MDT Subnet** (optional)—If **Enable Auto Pick MDT Addresses** is not checked (set on), you can provide the **Default MDT Subnet**.
- l. **Data MDT Size** (optional)—If **Enable Multicast** is set on, **Data MDT Size** is required. From the drop-down list, select the data MDT size.
MDT refers to a *multicast distribution tree* (MDT). The MDT defined here carries multicast traffic from customer sites associated with the multicast domain.
- m. **Data MDT Threshold** (optional)—If **Enable Multicast** is set on, **Data MDT Threshold** is required. Enter the bandwidth threshold for the data multicast distribution tree.
The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT.
- n. **Default PIM Mode** (optional)—For Default Protocol Independent Multicast (PIM) mode, click the drop-down list and choose **SPARSE_MODE** or **SPARSE_DENSE_MODE**. For IOS XR devices, no configlet is generated for either mode.
- o. **Enable PIM SSM** (optional)—Check this check box for PIM Source Specific Multicast (SSM).
- p. **SSM List Name** (optional)—Choose **DEFAULT** from the drop-down list and you create the following CLI: **ip pim vpn <vpnName> ssm default**. No configlet is generated for IOS XR devices, because they are using the standard SSM range 232.0.0.0/8. Choose **RANGE** from the drop-down list to associate an access-list number or a named access-list with the SSM configuration. This creates the following CLI: **ip pim vpn <vpnName> ssm range {ACL#!named-ACL-name}**.
- q. **Multicast Route Limit** (optional)—Enter a valid value of 1 to 2147483647. For IOS XR devices, no configlet is generated.
- r. **Enable Auto RP Listener** (optional)—Check this check box to enable the Rendezvous Point (RP) listener function. By default, this feature is running on IOS XR devices and no configlet is generated for this attribute.
- s. **Configure Static-RP** (optional)—To configure Static RPs, check the associated check box. The Edit option for **PIM Static-RPs** then goes active.
- t. **PIM Static-RPs**—To edit or add PIM Static-RPs, click **Edit**. The Edit PIM Static RPs window appears. Then click **OK**.
- u. **Route Targets** (optional)—If **Enable Multicast** is set on, **Route Targets** is required. If you do not choose to enable the default Route Target, you can select a customized Route Target that you have already created in Prime Provisioning. From the Route Targets pane, click **Select**.
The Select Route Targets window appears.
- v. Check the check box for the Route Target you want used for this service policy, then click **Select**.
You return to the Create VPN window, where the new Route Target selection is displayed, along with its hub route target (HRT) and spoke route target (SRT) values.
- w. **Import RT List**— Enter one or more Route Targets (RTs) to be imported in the VPN.
- x. For multiple RTs, use a comma (,) separated list. An example RT list is 100:120,100:130,100:140.
- y. **Export RT List**— Enter one or more Route Targets (RTs) to be exported from the VPN.
- z. For multiple RTs, use a comma (,) separated list.

- aa. If you want VPLS attributes, the optional fields for that are in [ab.](#) to [ae.](#)
- ab. **Enable VPLS** (optional)—Check this check box to enable VPLS.
- ac. **VPLS VPN ID** (optional)—Enter an integer in the range of 1 to 2147483646.
- ad. **Service Type** (optional)—Click the drop-down list and choose from **ERS** (Ethernet Relay Service) or **EWS** (Ethernet Wire Service).
- ae. **Topology** (optional)—Choose the VPLS topology from the drop-down list: **Full Mesh** (each CE has direct connections to every other CE) or **Hub and Spoke** (only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other).

Step 4 When you are satisfied with the settings for this VPN, click **Save**.

You have successfully created a VPN, as shown in the **Status** display in the lower left corner of the VPNs window.

Deleting VPNs

From the VPNs window, you can delete specific VPNs.



Note

Only VPNs not associated with MPLS service requests can be deleted.

To delete VPN(s), follow these steps:

Step 1 Choose **Inventory > Logical Inventory > VPN**.

The VPNs window appears.

Step 2 Select VPN(s) to delete by checking the check box(es) to the left of the VPN name.

Step 3 Click the **Delete** button.

The Confirm Delete window appears.

Step 4 Click **OK** to confirm that you want to delete the VPN(s) listed.

The VPNs window reappears with the specified VPN(s) deleted.
