A P P E N D I X E

Inventory - Discovery

This appendix describes how to use the Discovery feature to discover devices, connections, and services for the Prime Provisioning provisioning process. It contains the following sections:

Overview of Prime Provisioning Discovery

Prime Provisioning discovery is designed to be an aid in installing Prime Provisioning in a brown-field network, that is a network that has pre-existing services before Prime Provisioning is introduced. Prime Provisioning discovery is not a mechanism to repeatedly discover services and synchronize with the database. After the initial discovery has been completed, all provisioning must then be done using Prime Provisioning. If services are provisioned directly on the network without using Prime Provisioning, these services are not known by Prime Provisioning and Prime Provisioning might overwrite or conflict with these services. Therefore, any services provisioned outside of Prime Provisioning must be brought into Prime Provisioning, by means of provisioning them in Prime Provisioning through the Graphical User Interface (GUI) or the Application Program Interface (API). This can be done in echo mode, so that a subsequent configuration audit confirms that the network and Prime Provisioning database are synchronized.

Cisco Confidential — Draft Label

In general, Prime Provisioning can only discover a subset of what it can provision, so Prime Provisioning cannot discover a service of a type that it cannot provision.

Prime Provisioning can expedite the process for building a network device inventory by discovering the devices, connections, and services that your MPLS VPN or L2VPN Metro Ethernet network comprises.

Note Service discovery is a complex operation that can be impacted by many variables within the network. The original network configuration must have been performed in accordance with the same rules that Prime Provisioning follows when provisioning services. Otherwise, errors might occur during the discovery. As a result of the many possible configurations in a given network, it is strongly recommended that you contact your Cisco account team or Cisco advanced services to provide support, before committing to the service discovery process.

Users who run service discovery should have a thorough understanding of their overall network topology, should be familiar with network terminology, such as: PE, N-PE, U-PE, PE-AGG, and CE, and should understand the definition of NPC and Metro Ethernet/MPLS services in Prime Provisioning.

Prime Provisioning supports the discovery process for admin users only.

The Prime Provisioning Discovery feature can be used to populate repository for three of the applications in the Prime Provisioning application suite:

- Prime Provisioning MPLS VPN Management
- Prime Provisioning L2VPN Management
- Prime Provisioning Prime Diagnostics

Note Service discovery does not support Secure Shell version 2 (SSHv2) as a terminal session protocol. MPLS and L2VPN service discovery do not support devices running IOS XR.

When a device in Prime Provisioning only has a hostname, the Prime Provisioning device has no IP management address or domain name configured. If in Discovery, a device with the same hostname is discovered with an IP management address or is created manually in the Device Editor, the device might fail to commit to the Prime Provisioning repository. The failure occurs because a match is determined with the existing Prime Provisioning device, because both devices do not have a configured domain name.

The workaround is to do either 1. or 2., as follows:

1. Edit the device that exists in Prime Provisioning and add the management IP address before Discovery. Discovery then treats that device as a duplicate and marks it read-only in the Device Editor.

   or

2. During Discovery, in the Device Editor, enter a domain name for the discovered device. Discovery then treats this as a new device.

The Prime Provisioning Traffic Engineering Management has its own Discovery interface and process. This is documented under TE Network Discovery, page 8-10.

Multiple service discovery processes are supported and you can restart from any of the previous steps. Support for multiple discovery processes allows you to do incremental discovery of the network. The ability to restart from previous steps helps you roll back the discovery process to a selected previous step.

You can then resume discovery from that step instead of needing to restart the entire discovery process from the beginning. Restarting from discovery data collection prompts the user to select devices for which data needs to be collected.

Incremental discovery occurs for existing VPN links. The existing VPNs are not editable in the discovery GUI and the existing VPN links are by-passed during commit.

There is no synchronization in MPLS and L2VPN service discovery. Any modification must be done manually through the Prime Provisioning user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

The commit to Prime Provisioning happens only at the end of the discovery phase, not after each step. The Discovery process does not change the state of Prime Provisioning during discovery workflow. It is only at the end of the workflow that a user can commit the discovered devices and services to Prime Provisioning.

The Discovery process provides you with several choices on how to discover your network topology.

3. If you are running Discovery to provision Prime Provisioning MPLS VPN Management or Prime Provisioning L2VPN Management, you can choose between three Discovery methods:

   a. CDP Discovery

      You can use the Cisco Discovery Protocol (CDP) to discover devices connected to an initial device that has an IP address you provide in a **policy.xml** file.

   b. Device/Topology Based Discovery

      You can use a Device/Topology-based method. This method uses XML files that specify device and NPC topology information.

   c. Import Configuration File Based

      You can use an Import Configuration Files-based method. This method uses a directory on the server that contains configuration files for the devices to be discovered and an XML file that contains device connectivity information that is used to automatically create NPCs.

4. You can choose the network topology to discover an MPLS VPN topology, an L2VPN (Metro Ethernet) topology, or both.

   If you choose L2VPN (Metro Ethernet) Discovery, you can discover either a Metro Ethernet with an MPLS core, a Metro Ethernet with an Ethernet core, or a combination of the two, a mixed core. In a mixed core, the L2VPN services can span across the MPLS core or they can be confined to a local Ethernet domain alone (local switched services). Local switched services that do not traverse N-PE devices across an ethernet domain can also be discovered. Figure E-1, shows a mixed core.

Cisco Confidential — Draft Label

Figure E-1   ***Mixed Core***
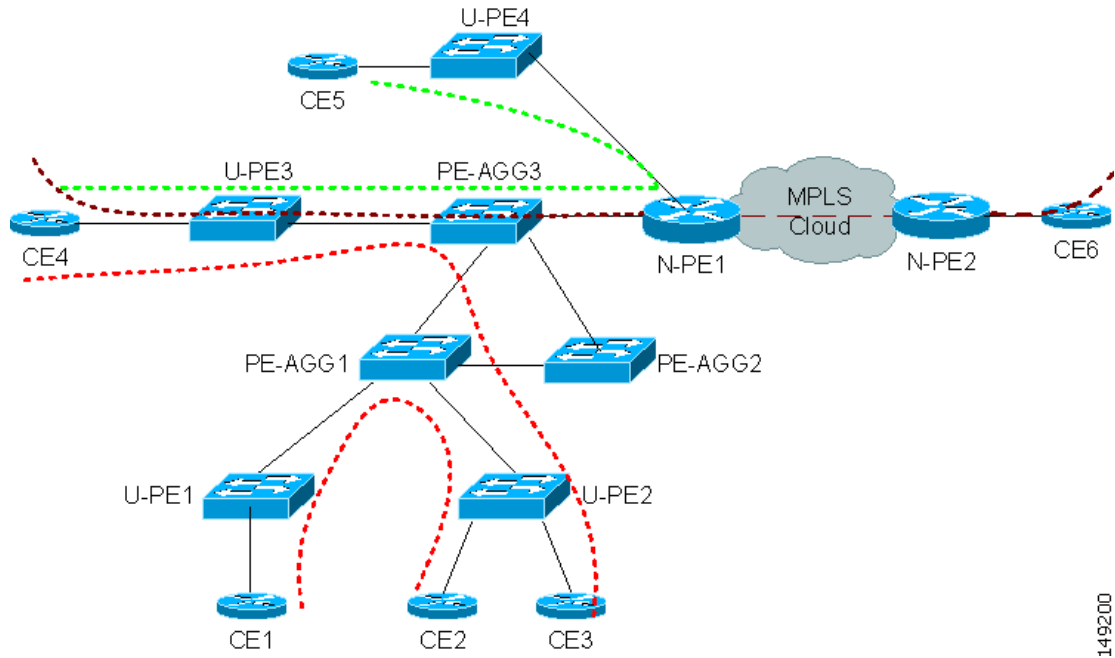
Figure E-2 illustrates the phases in the Discovery process.

Figure E-2   ***Prime Provisioning Discovery Steps***
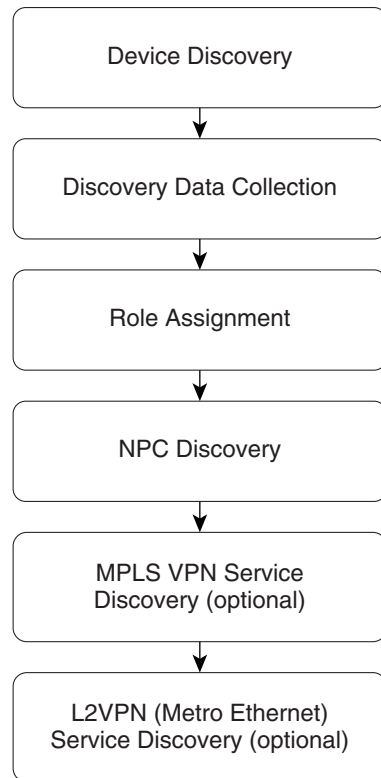
Cisco Confidential — Draft Label

Table E-1 describes the phases in the Discovery process.

Table E-1   Steps in the Discovery Process

Step	Description
Device Discovery	Discovers devices in the MPLS VPN and/or Metro Ethernet topology.
Discovery Data Collection	Collects the IOS configuration for the devices discovered.
Role Assignment	Does the role assignment for the discovered devices based on rules.xml, and prompts you to edit the device roles as N-PE, U-PE, or CE. **Note** A sample is found at: $PRIMEP_HOME/resources/discovery/data/ rules.xml, where the rules.xml file must be kept.
NPC Discovery	Displays discovered NPCs and allows addition or removal of NPCs.
MPLS VPN Discovery	Discovers the topology for your MPLS VPN network and allows you to change it as required. **Note** The MPLS VPN Discovery step is not required if you are using Prime Provisioning Discovery with Prime Diagnostics.
(L2VPN) Metro Ethernet Discovery	Discovers the topology for your Metro Ethernet network and allows you to change it as required. **Note** The (L2VPN) Metro Ethernet Discovery step is not required if you are using Prime Provisioning Discovery with Prime Diagnostics.

The following discovery operations are not supported by Prime Provisioning:

- Initial discovery of MPLS VPN services on devices running IOS XR
- Initial discovery of Ethernet access (U-PE, PE-AGG) into MPLS VPN services
- Initial discovery of VRF-lite/MVRF
- Initial discovery of VRF with multicast configuration
- Initial discovery of MPLS VPN services with unique route distinguishers
- Initial discovery of VRF that is not associated with an interface
- Initial discovery of VRF associated with one interface and no other VRF is in service among discovered devices
- Discovered extranet, unless the user manually splits VPNs
- Discovery of MPLS VPN/MLS VRF which is attached to a Loopback interface
- Initial discovery of services using the new ethernet service instance (EVC) syntax that was introduced in 12.2(33) SRB on the Cisco 7600 Series Routers

- Initial discovery of L2VPN services on devices running IOS XR

- Discovery of ERS and ERMS services with access port (only discovery with VLAN access is supported)

- Discovery of ATM or Frame Relay services (only discovery of Ethernet services is supported)

- Incremental NPC synchronization

- Re-synchronization, including discrepancy management

Technical Notes for Prime Provisioning Discovery

This section presents technical tips, general information, and limitations about the Prime Provisioning Discovery process.

The Prime Provisioning Discovery feature can be used to populate repository for three of the applications in the Prime Provisioning application suite:

- Prime Provisioning MPLS VPN Management

- Prime Provisioning L2VPN Management

- Prime Provisioning Prime Diagnostics

Although the general steps are similar, there are some differences in the workflow for the various types of Discovery. These are described in the section covering each Prime Provisioning application:

- Using Prime Provisioning Discovery with Prime Provisioning MPLS VPN Management, page E-7

- Using Prime Provisioning Discovery With Prime Provisioning L2VPN Management, page E-7

- Using Prime Provisioning Discovery with Prime Provisioning Prime Diagnostics, page E-8

- Using Prime Provisioning Discovery With Prime Provisioning Traffic Engineering Management, page E-9

> **Note** Prime Provisioning Traffic Engineering Management has its own Discovery interface and process.
>
> This is documented under TE Network Discovery, page 8-10.

For technical notes on using Prime Provisioning Discovery in installations that include both Prime Provisioning Traffic Engineering Management and Prime Provisioning MPLS VPN Management, see Using Prime Provisioning Discovery With Prime Provisioning Traffic Engineering Management, page E-9.

General Notes

Note the following points before running Prime Provisioning Discovery:

- You can use the Prime Provisioning GUI to create providers, customers, and resource pools before doing Discovery.

- Only one user can control the Discovery workflow interface at a given time.

- The procedures in the chapter show a "generic" procedure. If you do not have licenses for a particular application, you will not see the selections for that application on the start screen for Prime Provisioning Discovery.

- Perform "manual" device collection after discovery is over.

- After you have started the Discovery process, a **Restart** button appears on the Discovery Workflow window. You can click the **Restart** button, a drop-down list of completed steps pops up and you can select a step and restart from that step.

- Restarting from initialization aborts the current discovery process.

- Discovery using Role Based Access Control (RBAC) is not supported.

Using the Discovery Log Files

A log file is written for each phase of the Discovery process. You can view a log file by clicking the **View** selection in the Log column next to each discovery phase summary on the Discovery Workflow window.

The log file provides useful information in the event a discovery step fails.

Using Prime Provisioning Discovery with Prime Provisioning MPLS VPN Management

If you are running the Discovery process to discover an MPLS VPN network for use with Prime Provisioning MPLS VPN Management, note the following points:

- You must perform all of the main steps in the Discovery process.

- You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.

- Prime Provisioning does not support partial mesh VPN topologies. If the Discovery process discovers a Partial Mesh VPN, you must split the partial mesh VPN into smaller units (usually a combination of full mesh VPNs and Hub and Spoke VPNs).

- After completion of the automated Discovery process, you must schedule and run a **Operate > Tasks > Task Manager > Collect Config** task for all discovered devices.

Note   There is no synchronization in MPLS service discovery. Any modification must be done manually through the Prime Provisioning user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

Using Prime Provisioning Discovery With Prime Provisioning L2VPN Management

If you are running the Discovery process to discover an L2VPN network that will be provisioned and managed using Prime Provisioning L2VPN Management, note the following points:

- You must perform all of the main steps in the Discovery process.

- You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.

- A new L2VPN service is discovered when any of the following are found compared to the services existing in Prime Provisioning:

- – A new Virtual LAN Identifier (VLAN ID) in an Ethernet core (Ethernet access domain)

- – A new Virtual Circuit Identifier (VC ID) for virtual private wire service (VPWS) services on an MPLS core.

- – A new VPLS Forwarding Instance Identifier (VFI ID) for virtual private LAN service (VPLS) services on an MPLS core.

- • The Discovery process for Prime Provisioning L2VPN Management can discover Metro Ethernets with an MPLS core, an Ethernet core, or both.

- • Prior to performing the NPC Discovery step for Prime Provisioning L2VPN Management, you must specify the Access Domain for N-PE devices.

- • Any new links that are configured on NPCs marked as Existing Modified or Conflicting are not discovered.

- • After completion of the automated Discovery process, you must schedule and run a **Task Manager > Collect Config** task for all discovered devices.

> **Note** There is no synchronization in L2VPN service discovery. Any modification must be done manually through the Prime Provisioning user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

Using Prime Provisioning Discovery with Prime Provisioning Prime Diagnostics

If you are running the Discovery process to discover an MPLS VPN network for use with Prime Diagnostics, note the following points.

- • You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.

- • For Prime Provisioning Prime Diagnostics, you only need to perform the Device Discovery, Discovery Data Collection, and Role Assignment Steps. You do not need to perform the NPC Discovery step or the Service Discovery step. However, you can let the NPC Discovery process run.

  See for a flowchart of the required steps for Prime Provisioning Discovery with Prime Provisioning Prime Diagnostics.

- • If you are using Prime Provisioning Prime Diagnostics, then you normally only need to discover P and PE devices. Therefore, when you perform the Role Assignment step for discovered devices, you only need to assign roles to the P and PE devices.

> **Note** If you do discover any CE devices, you must assign them CE roles.

- • After completion of the automated Discovery process, you must schedule and run a **Task Manager > Collect Config** task for all discovered devices.

Cisco Confidential — Draft Label

Using Prime Provisioning Discovery With Prime Provisioning Traffic Engineering Management

Normally you do not have to run the Prime Provisioning Discovery process if you are using Prime Provisioning Traffic Engineering Management. Prime Provisioning Traffic Engineering Management has its own discovery process,. This process is documented under TE Network Discovery, page 8-10.

However, if you are running *both* Prime Provisioning Traffic Engineering Management (TEM) and Prime Provisioning MPLS VPN Management, you must run the Discovery process for MPLS VPN Management.

Note the following points:

* One region (default region) is used for TEM.

* If you are also running Prime Provisioning Discovery for MPLS VPN Management, make sure you run the Discovery workflow described in this chapter *first*, and then run the Traffic Engineering Management process later.

Summary of Tasks for Discovery (Prime Provisioning MPLS VPN Management and L2VPN Management)

Figure E-3 provides a general workflow diagram for the Discovery process used with the MPLS VPN Management or L2VPN Management application.

Note   Figure E-5 provides a general workflow diagram for the Discovery process as used with the Prime Diagnostics application.

Cisco Confidential — Draft Label

Figure E-3   ***Basic Workflow for Discovery with Prime Provisioning MPLS VPN Management or Prime Provisioning L2VPN Management***

Step 1:
Perform Preliminary Steps

Step 2:
Perform Device Discovery

Step 3:
Perform Discovery Data Collection

Step 4:
Perform Role Assignment

Step 5:
Perform NPC Discovery

Step 6:
Perform MPLS VPN Service
Discovery (optional)

Step 7:
Perform L2VPN (Metro Ethernet)
Service Discovery (optional)

Step 8:
Commit Discovered Devices
and Services to ISC

Step 9:
Create and Run a Collect Config
Task for Discovered Devices

Step 10:
View and Edit Services
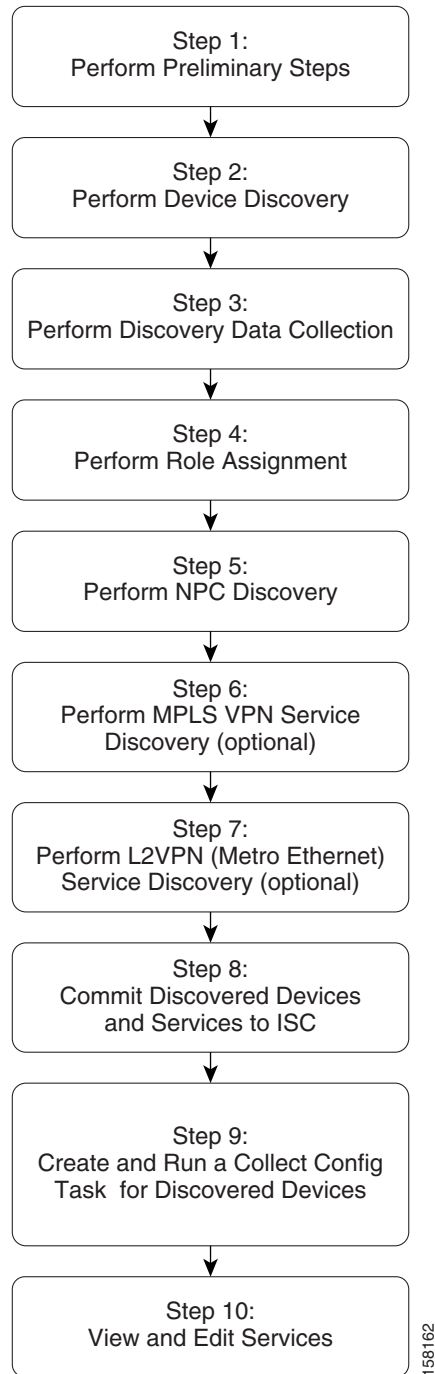
158162

Table E-2 describes each task in the Discovery workflow for Prime Provisioning MPLS VPN Management and Prime Provisioning L2VPN Management.

Table E-2   Description of Discovery Steps for MPLS VPN and L2VPN Management

Step	Description
Step 1: Perform Preliminary Steps	Perform preliminary steps that are required for Prime Provisioning Discovery. See Step 1: Perform Preliminary Steps, page E-16. • Review System Requirements See Review System Requirements, page E-17. • Install Licenses See Install Licenses, page E-18. • (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined See (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined, page E-18 • (CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered See (CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered, page E-19. • Code XML Files Required for Discovery See Code XML Files Required for Discovery, page E-20.
Step 2: Perform Device Discovery	• Start Device Discovery See Starting Device Discovery, page E-27. • After Device Discovery is complete, enter device passwords For information on entering device passwords, see Setting Password Attributes (Required Step), page E-31. • Enter additional device information as required See Setting General Device Attributes, page E-32 and Setting Cisco CNS Attributes, page E-32.
Step 3: Perform Discovery Data Collection	Start configuration collection. No input is required for this step. See Step 3: Perform Discovery Data Collection, page E-33.
Step 4: Perform Role Assignment	Assign device roles to each device. See Step 4: Perform Role Assignment, page E-33.
Step 5: Perform NPC Discovery	If you are discovering a Metro Ethernet Network with an Ethernet Core, perform the required preliminary steps. See Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks, page E-41 • Start NPC Discovery See Step 5: Perform NPC Discovery, page E-41. • Modify and/or add NPCs as required. See Adding a Device for an NPC, page E-44, Adding a Ring, page E-45, Inserting a Device, page E-45, Inserting a Ring, page E-45, or Deleting a Device or a Ring, page E-46.

Cisco Confidential — Draft Label

Table E-2   Description of Discovery Steps for MPLS VPN and L2VPN Management (continued)

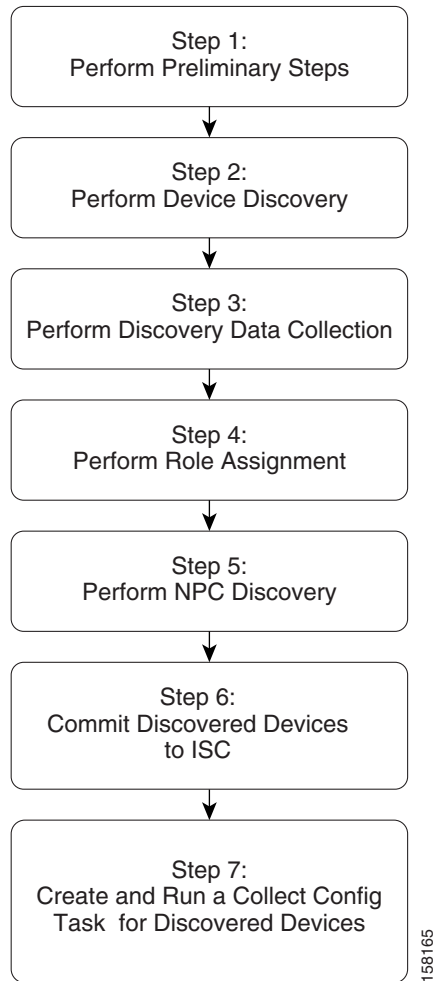| Step	Description
Step 6: Perform MPLS VPN Service Discovery (optional)	Start MPLS VPN Service Discovery. See Step 6: Perform MPLS VPN Service Discovery (Optional), page E-46. This step is required for the Prime Provisioning MPLS VPN Management application, **Note** This step is not required for the Prime Provisioning L2VPN Management application or the Prime Provisioning Prime Diagnostics application.
Step 7: Perform L2VPN Service Discovery (optional)	Start L2VPN Service Discovery. See Step 7: Perform L2VPN (Metro Ethernet) Service Discovery (Optional), page E-51. This step is required for the Prime Provisioning L2VPN Management application. **Note** This step is not required for the Prime Provisioning MPLS VPN Management application or the Prime Provisioning Prime Diagnostics application.
Step 8: Commit Discovered Devices and Services to Prime Provisioning Repository	Commit the discovered devices and services to the Prime Provisioning repository. Prior to this step, discovery workflow stores the discovered devices and services in a temporary repository, which gets committed to Prime Provisioning only at the last step of discovery workflow.
Step 9: Create and Run a Collect Config Task for Discovered Devices	From the Prime Provisioning Start Page, choose **Operate > Tasks > Task Manager**. Select the **Collect Config** task and select all of the devices discovered in the Device Discovery step; then submit the task. See Step 9: Create and Run a Collect Config Task for the Discovered Devices, page E-58.
Step 10: View and Edit Services	The discovered services will be in Pending state and you need to do a config audit to move them to Deployed state. See Step 10: View and Edit Services, page E-59.

Within each step, additional tasks must be performed and choices must be made. Figure E-4 shows a detailed flowchart that illustrates all of the steps in the Discovery workflow.

Cisco Confidential — Draft Label

Figure E-4   Detailed Diagram of Discovery Steps (Prime Provisioning MPLS VPN Management and Prime Provisioning L2VPN Management)
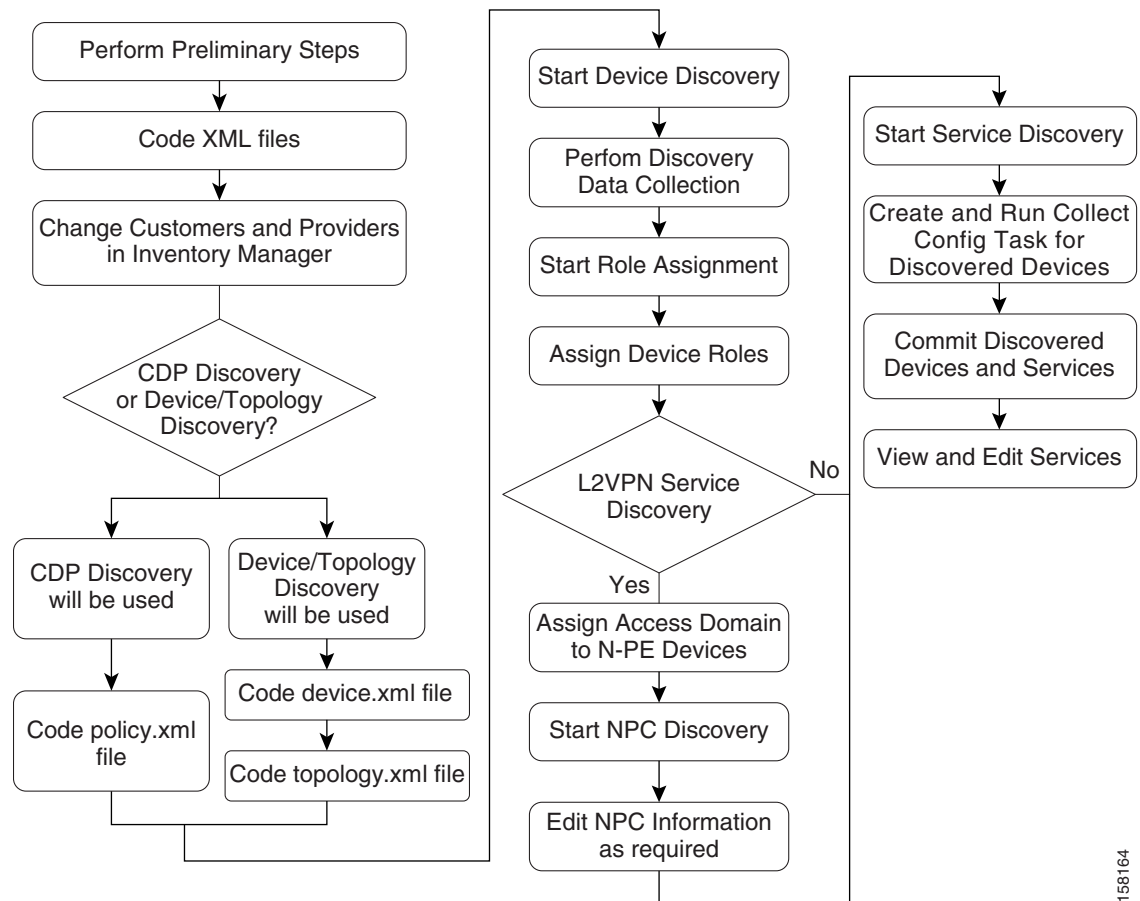
Summary of Prime Provisioning Discovery Steps for Prime Diagnostics

Figure E-5 shows the basic Discovery steps for Prime Provisioning with the Prime Diagnostics application. For Prime Diagnostics, several of the steps required for Prime Provisioning MPLS VPN Management and Prime Provisioning L2VPN Management are not required.

Cisco Confidential — Draft Label

Figure E-5   *Discovery Workflow for the Prime Diagnostics Application*

Cisco Confidential — Draft Label

Table E-3   *Description of Discovery Steps for Prime Diagnostics*

Step	Description
Step 1: Perform Preliminary Steps	Perform preliminary steps that are required for Prime Provisioning Discovery. • Review System Requirements See Review System Requirements, page E-17. • Install Licenses See Install Licenses, page E-18 • Code XML Files Required for Discovery For specific instructions, see the following section: – Code XML Files Required for Discovery, page E-20.
Step 2: Perform Device Discovery	• Start Device Discovery See Starting Device Discovery, page E-27. • After Device Discovery is complete, enter device passwords For information on entering device passwords, see Setting Password Attributes (Required Step), page E-31. • Enter additional device information as required See Setting General Device Attributes, page E-32 and Setting Cisco CNS Attributes, page E-32.
Step 3: Perform Discovery Data Collection	Start configuration collection. No input is required for this step. See Step 3: Perform Discovery Data Collection, page E-33.

Table E-3   Description of Discovery Steps for Prime Diagnostics (continued)

Step	Description
Step 4: Perform Role Assignment	Assign device roles to each device. See Step 4: Perform Role Assignment, page E-33.
	For Prime Diagnostics, you normally discover only P and PEs and assign P and PE roles to them However, if you discover CEs, assign CE roles to the CE devices.
	Note Although you do not have to edit NPCs for Prime Diagnostics, after you perform role assignment this step should complete.
Step 5: Create and Run a Collect Config Task for Discovered Devices	From the Prime Provisioning Start Page, choose **Operate > Tasks > Task Manager**. Select the **Collect Config** task and select all of the devices discovered in the Device Discovery step; then submit the task.
	See Step 8: Commit Discovered Devices and Services to Prime Provisioning Repository, page E-58.

Step 1: Perform Preliminary Steps

Before you initiate the Prime Provisioning Discovery process, complete the following preliminary steps:

- Review System Requirements
- Install Licenses
- Discovery in Large Networks
- (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined
- (CDP Discovery Only) Verify That CDP is Running on Devices To Be Discovered
- Code XML Files Required for Discovery

Figure E-6 summarizes the preliminary steps for Prime Provisioning Discovery.

Figure E-6   Summary of Preliminary Steps for Discovery
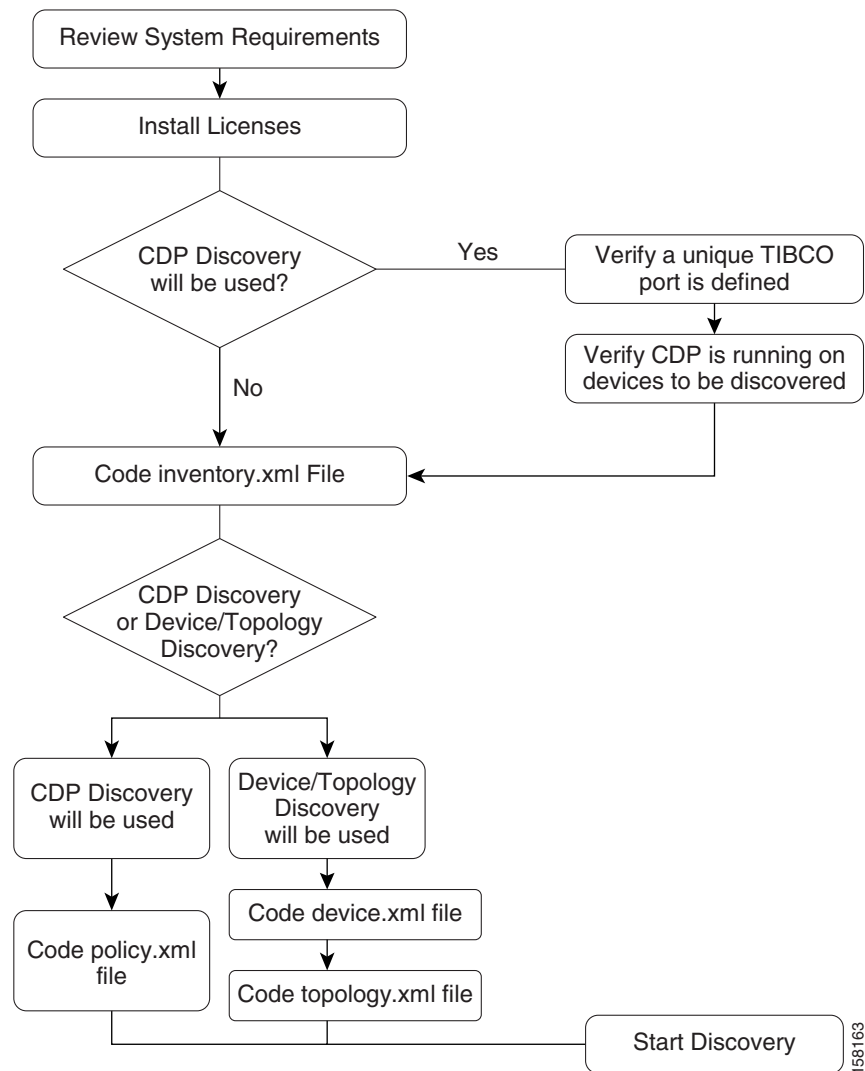
Review System Requirements

We recommend that you thoroughly review the system requirements for Prime Provisioning before planning your installation, to be sure that you have all the hardware and software that you must successfully install.

The system recommendations and requirements for Prime Provisioning are listed in Chapter 1, "System Recommendations" of the *Cisco Prime Provisioning 6.4 Installation Guide* and in the *Cisco Prime Provisioning 6.4 Release Notes.*

Cisco Confidential — Draft Label

Install Licenses

Before starting Discovery, the appropriate licenses (both Activation and VPN licenses) must be installed. Also, each license must be large enough to handle all possible discovered objects. For information on installing licenses, see the "Installing License Keys" section of Chapter 2 of the *Cisco Prime Provisioning 6.4 Installation Guide*, "Installing and Logging In to Prime Provisioning."

Discovery in Large Networks

To discover large networks with a complex topology, we recommend you reset two DCPL properties, as follows:

Step 1 See the *Cisco Prime Provisioning 6.4 Administration Guide* for an explanation of how to navigate to the Dynamic Component Properties Library (DCPL) properties.

Step 2 Navigate to the property **watchdog\server\discovery\heartbeat\timeout** and set this property to **180000 milliseconds** (3 minutes).

Step 3 Navigate to the property **watchdog\server\discovery\java\flags** and set this property to **-Xmx3072m -XX:PermSize=256m -XX:MaxPermSize=512m**

Step 4 Restart the Prime Provisioning server.

Heap is a block of memory segment for the L2VPN and Metro Ethernet, Layer 3 MPLS VPN, and TEM components. It is allocated for use by the Java virtual machine (JVM) process during runtime. It might need to be increased for large deployments. If the **httpd** process restarts, increase the heap size, as follows:

Step 1 **cd $PRIMEP_HOME/bin**

Step 2 **vi tomcat.sh**

Step 3 Search for a line with **-Xmx** and specify a higher value.

Step 4 Set the heap size to 1GB or 2GB by replacing **-Xmx512m** with **-Xmx1024m** or **-Xmx2048m**, respectively.

Step 5 Save the **tomcat.sh** file.

Step 6 Enter **stopall** to stop the Prime Provisioning server.

Step 7 Enter **startwd** to start the Prime Provisioning server.

(CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined

If you are using CDP Discovery to discover the network topology, make sure the TIBCO Port is unique. Otherwise, CDP discovery will fail.

Cisco Confidential — Draft Label

During installation, the TIBCO port can be specified if the "custom" Installation Type is selected at the start of the installation process. Otherwise, the default port installed is 7530. You specify the TIBCO port on the Choose TIBCO Port dialog.

The port number that is specified must be unique throughout the network, and no other Prime Provisioning installations are allowed with the same port.

Figure E-7 shows the Choose TIBCO Port dialog.

Figure E-7   Choose TIBCO Port
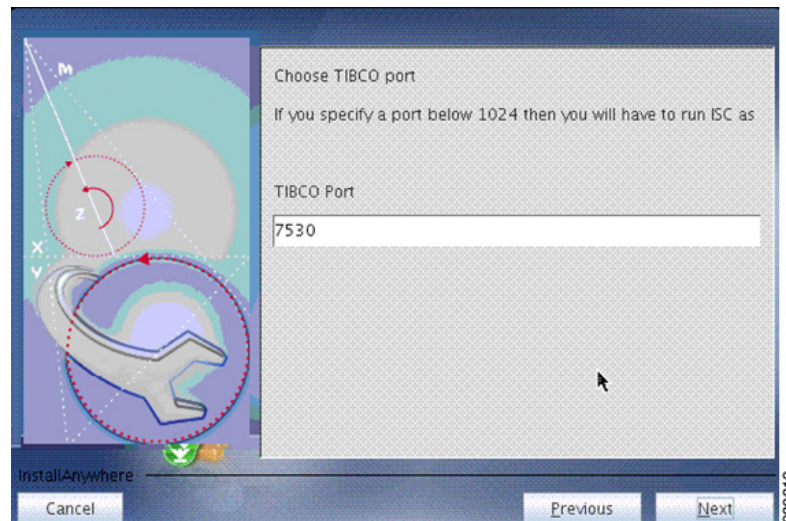
The Tibco port can be changed after installation by modifying the Dynamic Component Properties Library (DCPL) entry /SYSTEM/tibco/port. To locate these system properties, see the *Cisco Prime Provisioning 6.4 Administration Guide*.

(CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered

If CDP Discovery is going to be used, use the **show cdp** command to ensure that CDP is running on all of the devices intended to be discovered.

For each device, enter the **show cdp** command, as shown in Example E-1.

Example E-1   The show cdp Command:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
Router#
```

Cisco   Confidential   —   Draft   Label

> **Note** When performing CDP Discovery for devices with more than one IP address configured, it is possible that CDP discovery will find an IP address other than the management IP address. If the IP address found is not accessible from the Prime Provisioning server, then it will not be possible to discover that device using CDP discovery.

Code XML Files Required for Discovery

Before you can run Prime Provisioning Discovery, you must code XML files that are required for the Discovery process. A different set of files is required, depending on whether you use CDP Discovery or Device/Topology-based Discovery.

Table E-4 describes the XML files and indicates which files are required for each type of discovery method.

Table E-4   XML Files Used with Prime Provisioning Discovery

XML File	Description	Required for CDP Discovery	Required for Device/Topology Based Discovery
policy.xml	Specifies one or more seed IP addresses that can be reached from the specified seed device and a maximum hop count for the device discovery process.	Yes	No
device.xml	Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).	No	Yes
topology.xml	Specifies information used to build NPCs used by MPLS VPN and/or Metro Ethernet topology.	No	Yes

> **Note** Make sure that the coding in your XML files is accurate. If there are errors in the files, you might need to re-run the Discovery process.

Sample XML Files

The initial installation of Prime Provisioning provides sample XML files that you can use as a starting point in coding your own XML files. The sample XML files are located in the following directory:

<*install_directory*>/resources/discovery/sample

where <*install_directory*> is the installation directory that you specified when prompted by the Prime Provisioning installation program.

Coding the policy.xml File

The **policy.xml** file:

- Is required for CDP Discovery.

Cisco Confidential — Draft Label

- Is required for Prime Provisioning MPLS VPN Management, Prime Provisioning Carrier Ethernet and L2VPN Management, and Prime Diagnostics.
- Is not required for Device/Topology-based Discovery.
- Is not required for Prime Provisioning Traffic Engineering Management.
- Provides a seed IP address that the CDP protocol uses to discover devices near the seed device.

Example E-2 shows the sample **policy.xml** file that is provided with the Prime Provisioning installation.

Example E-2   Sample policy.xml File

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.232" hop="1"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

If there are additional routers that are on the other side of PE routers on the edge of the core segment of the network, you can specify more than one seed IP address in order to discover these devices.

Example E-3 shows a **policy.xml** file that contains two seed IP addresses.

Example E-3   Policy.xml File with Two IP Addresses

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.241" hop="8"/>
  </DISCOVERY_METHOD>
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.244" hop="8"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

Table E-5 describes the XML tags used in the **policy.xml** file.

Table E-5   XML Tags and Attributes Used in the policy.xml File

Tag	Description
<DISCOVERY_METHOD>	Starts a **<DISCOVERY_METHOD>** tag. The **<DISCOVERY_METHOD>** tag must contain a **<CDP>** tag.
<CDP>	Starts a <CDP> tag. The **<CDP>** tag specifies a seed IP address and a hop count. The **<CDP>** tag must contain the following attributes: • **ipaddress** • **hop**
ipaddress	Specifies the IP address of a seed device. Required attribute for the **<CDP>** tag.
hop	Specifies the number of hops from the device identified by the ipaddress attribute to go in discovering devices. Required attribute for the **<CDP>** tag.

Follow these steps to edit the sample **policy.xml** file:

Step 1   Edit the sample file and replace the IP address specified with the **ipaddress** XML attribute with an appropriate IP address from your network.

This IP address is a device that can be reached from the Prime Provisioning host. For each seed device, an accessible interface on the starting point is configured, because the management interface must be provided. The management interface is the address on the device that the Prime Provisioning host uses to reach the device.

Note   You can provide more than one IP address. This is useful in situations where one network domain is on the other side of a PE router on the edge of the core segment of the network.

Step 2   Edit the hop count specified with the **hop** attribute and specify a hop count that will be used when the Discovery process is initialized.

When you choose the seed devices and hop count, pick a seed device that can reach a large section of the network. Pick one or more of them until you think these devices will enable you to reach your entire managed network.

Point-of-presence (POP) routers are usually good choices. If you choose all the POPs in your network as the collection of seed devices and put in the appropriate number of hubs, you discover the entire managed network.

To pick the hop count number, go to the CE that is the furthest from its associated POP, and count the number of devices between them. If this number is N, the hub number is N+1, assuming you are picking the POP as the seed.

Step 3   If you need to add additional IP addresses for seed devices, code additional **<DISCOVERY_METHOD>** tags.

Within the additional **<DISCOVERY_METHOD>** tags, include **<CDP>** tags.

For each **<CDP>** tag, specify an IP address with the **ipaddress** attribute and a hop count with the **hops** attributes.

Cisco Confidential — Draft Label

Step 4   Save the **policy.xml** file to an appropriate directory on the Prime Provisioning host.

When you run the Discovery process, the process queries the starting point device for its CDP table. From this table, all of those devices are queried for their CDP information. This process continues until the maximum hop count from the starting point is reached. When you use the CDP-based method, note that only devices running CDP are discovered.

Coding the device.xml File

The **device.xml** file:

- Is required for Device/Topology-based Discovery.

- Is not required for CDP-based Discovery.

- Is required for Prime Provisioning MPLS VPN Management, Prime Provisioning Carrier Ethernet and L2VPN Management, and Prime Diagnostics.

- Is not required for Prime Provisioning Traffic Engineering Management.

- Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).

Example E-4 shows a sample **device.xml** file. Use the sample file as an example and save your edited file in an appropriate directory.

Example E-4   Sample device.xml file

```
<network>
<device>
<device-name>mlpe8</device-name>
<ip-address>209.168.133.244</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.509</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw11</device-name>
<ip-address>209.168.133.170</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw16</device-name>
<ip-address>209.168.133.175</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw17</device-name>
<ip-address>209.168.133.176</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
```

```
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

</network>
```

Table E-6 describes the XML tags used in the **device.xml** file.

Table E-6   XML Tags Used in the device.xml File

Tag	Description
<device>	Starts a **<device>** tag. The **<device>** tag must contain the following tags: • **<device-name>** • **<ip-address>** The following tags are optional within the **<device>** tag: • **<system-object-id>** • **<snmp-info>**
<device-name>	Specifies the name of the device. Required within the **<device>** tag.
<ip-address>	Specifies the IP address of the device. Required within the **<device>** tag.
<system-object-id>	(optional) Can be included to specify the SNMP Object ID (OID) for the device. If this is provided, it is specified within the **<device>** tag.
<snmp-info>	Specifies SNMP information for the device. The **<snmp-info>** tag must contain a **<ro-community>** tag. Optional within the **<device>** tag.
<ro-community>	Specifies the level of SNMP access for the device. Normally, this should be "public." Required within the **<snmp-info>** tag.
Note: SNMPv3 is not supported.	

Follow these steps to code the **device.xml** file:

Step 1   Edit the sample **device.xml** file provided with the installation.

Step 2   For each device that is to be discovered by Prime Provisioning, code a **<device>** entry.

Each **<device>** entry should contain the following tags:

• A **<device-name>** tag specifying the device name.

• An **<ip-address>** tag specifying the IP address for the device.

• A **<system-object-id>** tag specifying the OID for the device (optional).

• An **<snmp-info>** tag specifying **<ro-community>** information

Cisco Confidential — Draft Label

Step 3   Save the **device.xml** file to an appropriate directory on the Prime Provisioning host.

Coding the topology.xml File

The **topology.xml** file:

- Is required for Device/Topology-based Discovery.

- Is not required for CDP-based Discovery.

- Is required to perform Prime Provisioning Discovery for Prime Provisioning MPLS VPN Management, Prime Provisioning Carrier Ethernet and L2VPN Management, and Prime Diagnostics.

- Is not required for Prime Provisioning Traffic Engineering Management.

- Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).

The **topology.xml** file specifies the discovery protocol that is used in the discovery process, and, for each connection, specifies the starting IP address, the starting interface, the end device, and the end interface

Example E-5 shows a sample **topology.xml** file. Use the sample file as an example and save your edited file in an appropriate directory.

Example E-5   Sample topology.xml File

```
<topology>
<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="GigabitEthernet1/1/2"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="GigabitEthernet1/1/1" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/23"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="FastEthernet1/0/24" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet
1/0/24"   toDevice="mlsw18"  toIP="209.168.133.177"  toIF="FastEthernet1/0/23" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/22"   toDevice="mlsw22"  toIP="209.168.133.221"
toIF="FastEthernet1/0/24" >
</connection>

</topology>
```

Table E-7 describes the XML tags used in the **topology.xml** file.

Cisco Confidential — Draft Label

Table E-7   XML tags and Attributes Used in the topology.xml File

Tag	Description
<connection>	Starts a **<connection>** tag. The **<connection>** tag must specify the following attributes: • **discovery-protocol** • **fromDevice** • **FromIP** • **FromInterface** • **toDevice** • **toIP** • **toIF**
discovery-protocol	Specifies the Discovery protocol used to discover the network topology. Normally, this is "CDP."
fromDevice	Specifies the name of the device from which the Named Physical Circuit starts. Required attribute for the **<connection>** tag.
FromIP	Specifies the management IP address of the device from which the Named Physical Circuit starts. Required attribute for the **<connection>** tag.
FromInterface	Specifies the name of the device interface from which the Named Physical Circuit starts. Required attribute for the **<connection>** tag.
toDevice	Specifies the name of the device to which the Named Physical Circuit connects. Required attribute for the **<connection>** tag.
toIP	Specifies the management IP address of the device from which the Named Physical Circuit connects. Required attribute for the **<connection>** tag.
toIF	Specifies the device interface on the device to which the Named Physical Circuit connects. Required attribute for the **<connection>** tag.

Follow these steps to code the **topology.xml** file:

Step 1   Edit the sample **topology.xml** file provided with the installation.

Step 2   For each NPC connection that is to be discovered by Prime Provisioning, code a **<connection >** entry.

Each **<connection>** entry must contain the following tags:

• A **discovery-protocol** attribute specifying the CDP protocol.

• A **fromDevice** attribute specifying the device from which the NPC starts.

• A **FromIP** attribute specifying the management IP address from which the NPC starts.

Cisco Confidential — Draft Label

- A **FromInterface** attribute specifying the device interface from which the NPC starts.
- A **toDevice** attribute specifying the name of the device to which the NPC connects.
- A **toIP** attribute specifying the management IP address of the device to which the NPC connects
- A **toIF** attribute specifying the name of the interface on the device to which the NPC connects

Step 3   Save the **topology.xml** file to an appropriate directory on the Prime Provisioning host.

Step 2: Perform Device Discovery

This section describes how to start the device discovery process and edit device configuration.

Starting Device Discovery

To start discovery, follow these steps:

Step 1   Log into Prime Provisioning.

Step 2   Click the **Inventory > Physical Inventory > Discovery**.

The Device Discovery — CDP Fields window appears.

Initially, the CDP Discovery method is selected and the window displays the required input for this method.

The editable **Output Device File** field is optional and defaults to an XML file of the discovered devices. This file can then be an input **Devices File** for rerunning discovery using the **Device/Topology** option, by choosing that radio button.

The editable **Output Connection File** is optional and defaults to an XML file that contains device connectivity information that is written during CDP Device Discovery. This file can then be an input **NPC Topology File** for rerunning discovery using the Device/Topology option, by choosing that radio button.

Step 3   Choose a Discovery method:

- To use the Cisco Discovery Protocol (CDP) method, click the **CDP** radio button.
- To use the Device/Topology method, click the **Device/Topology** button.
- To use the Import Configuration Files method, click the **Import Configuration Files** button.

The required **Directory** field is the directory on the server that contains configuration files for the devices to be discovered. The format of these files *must* be *<filename>*.**cfg**.

The **NPC Topology File** field contains an XML file that contains device connectivity information that is used to automatically create NPCs.

Note   During service discovery, Providers, Regions, Customers, and Sites are not automatically created, and therefore you must manually create them before running service discovery. If Resource Pools are used for provisioning in Prime Provisioning, Access Domains and Resource Pools must be manually created before running service discovery.

Cisco Confidential — Draft Label

Step 4   In the Discovery window, specify the settings indicated in Table E-8.

Table E-8   Discovery Settings

Setting	Description
Name	In this field, enter a unique name of your choice for the Workflow name. If you do not enter a name in this field, the system automatically generates a unique name for you.
CDP	Click this radio button to select Cisco Discovery Protocol (CDP) as the Discovery method.
Policy File	If you click the **CDP** button, specify the path to your **policy.xml** file here. This file is an XML file that indicates the IP address of one or more devices used as a starting point for the discovery process. For more information on the **policy.xml** file, see Coding the policy.xml File, page E-20.
Output Device File	This editable optional field defaults to an XML file of the discovered devices. This file can then be an input **Devices File** for rerunning discovery using the **Device/Topology** option.
Output Connection File	This editable optional field defaults to an XML file that contains device connectivity information that is written during CDP device discovery. This file can then be an input **NPC Topology File** for rerunning discovery using the **Device/Topology** option.
Device/Topology	Click this radio button to select Device/Topology as the Discovery method.
Devices File	If you click the **Device/Topology** button, specify the path to your **device.xml** file here. This file contains information used to locate the devices in your network, such as IP addresses and OIDs. For more information on the **device.xml** file, see Coding the device.xml File, page E-23.
NPC Topology File	If you click this optional **Device/Topology** button, specify the path to your **topology.xml** file here. This file contains information used to determine the NPC topology of your network. For more information on the **topology.xml** file, see Coding the topology.xml File, page E-25.
Import Configuration Files	Click this radio button to select Import Configuration Files as the Discovery method.
Directory	This required field is the directory on the server that contains configuration files for the devices to be discovered. The format of these files *must* be *<filename>*.**cfg**.

Table E-8   Discovery Settings (continued)

Setting	Description
NPC Topology File	This field contains an XML file that contains device connectivity information that is used to automatically create NPCs.
MPLS VPN	To discover devices used in an MPLS VPN service, click the **MPLS VPN** radio button.
L2VPN (Metro Ethernet) Discovery	To discover layer 2 devices used in a Metro Ethernet service, click the **L2VPN (Metro Ethernet) Discovery** radio button.

Step 5   Click the **Start** button.

The discovery process starts and the Discovery Workflow window appears.

The **Workflow** category in the data pane gives the name information about the current discovery request/workflow.

Click the **Restart** button and you receive a drop-down list of completed steps. Select a step and you will restart from that step.

In the left column, **Current Request** gives the discovery request/workflow that is currently running. If there is no currently running discovery request/workflow, an initialization window appears to create a new discovery request/workflow.

In the left column, **Previous Requests** lists all the discovered requests/workflows. You can look at the status and logs for any of these discovery requests/workflows.

Discovery Workflow window indicates the progress of each phase of device discovery:

- When the window first appears, the status indicator is yellow and indicates that the device discovery process is **Initializing**.
- The status indicator then indicates that the process is **In Progress**.
- After the discovery processes has completed, the display indicates how many devices were discovered, and the status indicator changes to orange and indicates that there is **Pending Input.**

The Progress area at the bottom of the window indicates how many devices were discovered.

At the lower right of the window there is a **Restart** button. You can click this button to restart the entire discovery process. However, if you restart the Discovery process, any work that has been done previous to restarting Discovery is lost.

✎

Note   After each phase of the Discovery process, make sure that you check the log file to ensure that there were no errors in the process. For specific instructions, see Using the Discovery Log Files, page E-7.

Cisco Confidential — Draft Label

Editing Device Configurations

After the initial discovery of devices in your network, you must edit the information that Prime Provisioning maintains about the devices. This allows the Discovery process to collect configuration information about the devices that are required to determine the network topology and generate service requests.

Editing device configuration includes these steps:

- Setting Password Attributes (a required step)
- Setting General Device Attributes
- Setting Cisco CNS Attributes

Follow these steps to edit device configurations:

Step 1   When the Discovery Workflow window indicates that the Device Discovery is **Pending Input,** click the **Continue** button.

The General Attributes - Devices window appears.

The General Attributes - Devices window allows you to do the following:

1. Delete devices.

If devices appear in the device list that you do not want to configure, you can delete them, as explained in Step 4.

2. Set the following groups of attributes for each device:

– **General Attributes**—The general attributes include the hostname of the device, the device type, the management IP address, and other settings.

You can accept the default attributes shown in the General Attributes - Devices window or change them as required.

For a list of the general attributes, see Setting General Device Attributes, page E-32.

– **Password Attributes**—The password attributes include the username and password for the device and the enable username and password for the device. You *must* set these attributes.

– **CNS Attributes**—If the device is a CNS device, set the CNS attributes.

Step 2   If you want to filter the devices that appear in the window, enter part of the device name for the devices that you want to view, preceded or followed by the asterisk (*) and then click the **Find** button.

If the Find field displays an asterisk, all devices are displayed.

The setting in the Find field applies to all of the attributes windows.

Step 3   To change the display to show one of the attributes areas, click the **Attributes** button at the bottom of the window and use the pull-down list to select the attributes area to display.

- If you need to change the general attributes for the device, such as the protocol used to configure the device (Config Access Protocol), you can do this in the initial window that appears.

  If the General Attributes - Devices window is not the current window, click the **Attributes** button and select **General Attributes** from the pull-down list.

  See Setting Password Attributes (Required Step), page E-31 for instructions on setting the General Attributes.

- To set the password attributes, click the **Attributes** button and then select Password Attributes from the pull-down list.

For instructions on setting the password attributes, see Setting Password Attributes (Required Step), page E-31.

✎

Note   This is a required step. To enable configuration collection, you *must* set the password attributes.

- If you need to change the CNS attributes, see Setting Cisco CNS Attributes, page E-32.

Step 4   If you want to delete one or more devices, follow these steps:

    a.   Check the check box next to each device that you want to delete.

        If you need to delete more than one device, you can check the check box next to the heading for the list of the devices. This selects all of the devices in the list. You can then uncheck the boxes next to any devices that you do not want to delete.

    b.   To delete the devices, click the **Delete** button.

Setting Password Attributes (Required Step)

In order for the Configuration Collection phase to succeed, you *must* set the password attributes for each device. Follow these steps to set password attributes:

Step 1   If the Password Attributes window is not the current window, click the **Attributes** button and select **Password Attributes** from the pull-down list.

The Password Attributes window appears.

Step 2   Follow these steps to select the devices and password attributes to configure:

    a.   Check the check box next to a device that has password attributes you want to configure.

        If several devices have the same password attributes, you can check multiple check boxes. If all of the devices have the same password attributes, you can check the box to the left of the heading row to select all of the devices in the list. If this check box is checked, you can uncheck it to deselect all of the devices.

    b.   To select the password attributes to configure, check one or more of the check boxes next to the attribute names in the heading row.

Step 3   Click the **Edit** button.

Step 4   Enter the following information for the device:

- **Login Password**—Enter the login password for the device
- **Login User**—Enter the username for the device
- **Enable Use**r—Enter the name of a user with enable privileges
- **Enable Password**— Enter the enable password for the enable user

Step 5   Click **Save**.

The information that you entered appears in the Password Attributes window.

Cisco Confidential — Draft Label

Setting General Device Attributes

After you complete the device discovery process, the General Attributes - Devices window displays the current general attributes settings for each device.

Follow these steps to change the general attributes for a device:

Step 1   Click on the attribute that you want to change.

An Edit Attributes dialog box appears for the selected attribute.

Step 2   In the dialog box, indicate the new setting for the attribute.

The General Device attributes include the following:

- **Host 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.

- **Device Type**—The device type is the Cisco Router.

- **Device Description (not editable from this window)**—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 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.

- **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.

- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Terminal, TFTP, and RCP.

Setting Cisco CNS Attributes

If one of the devices is a Cisco CNS device, follow these steps to set CNS attributes:

Step 1   If the CNS Attributes window is not the current window, click the **Attributes** button and select **CNS Attributes** from the pull-down list.

The CNS Attributes window appears.

The **Terminal Server** column specifies the devices that represent the workstations that can be used to provision edge routers, and the **Port Number** column specifies the port numbers used by the terminal server.

Step 2   Click an existing Event Identification item.

The Edit Attributes dialog box for Event Identification appears.

Step 3   From the drop-down list for Event Identification attribute, you can select **Event-Identification**, which indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.

.

Cisco Confidential — Draft Label

Saving the Device Configuration

After you are finished making device configuration changes, click the **Continue** button.

The Device Discovery indicator turns green and indicates that Device Discovery is **Complete**.

The Discovery Data Collection phase begins automatically.

Step 3: Perform Discovery Data Collection

After you save your device configuration settings, the Discovery Data Collection phase of Device Discovery starts automatically.

While Cisco Prime Provisioning is collecting the device configurations, the Discovery Data Collection indicator is yellow and indicates that the process is **In Progress**.

When the Discovery Data Collection phase is complete, the indicator changes to green and indicates that the process is **Complete**. You are now ready to assign device roles.

Step 4: Perform Role Assignment

After the Discovery Data Collection phase of Device Discovery is complete, the Discovery Workflow window indicates that the Role Assignment phase is **Pending Input**.

Restarting from Discovery Data Collection prompts you to select the devices for which discovery data collection needs to occur.

Follow these steps to assign device roles:

- Initiate Device Role Assignment
- Change the Device Assignment Display
- Change Device Assignments
- Determine Device Roles
- Assign CE Device Roles
- Assign PE Device Roles

The following sections describe each of these steps.

Initiating Device Role Assignment

Follow these steps to initiate device role assignment:

Step 1   In the Discovery Workflow window, click **Continue**.

The Role Assignment - Un-assigned Devices window appears.

On the Role Assignment - Un-assigned Devices window, if you select a single device, you are prompted directly for the device role assignment. However, if you select more than one device, either the Role Assignment - CEs window or the Role Assignment - PEs window appears. On these windows you can specify the desired device roles.

Cisco Confidential — Draft Label

Step 2   If you want to change the way that the devices are displayed, see the following section, Changing the Device Assignment Display, page E-34.

Changing the Device Assignment Display

You can change the way devices are displayed in the Role Assignment window in the following ways:

- You can change the display to show unassigned devices, PE devices, or CE devices using the pull-down list at the bottom of the Role Assignment window.

- You can change the range of devices that are displayed using the **Show devices with** selection at the top of the window in combination with the **matching** field.

Follow these steps to change the category of devices that is displayed:

Step 1   To change the category of devices that is displayed, select a value from the pull-down list at the bottom of the Role Assignment window:

- To view PE devices, select **PEs**.

- To view CE devices, select **CEs**.

- To view unassigned devices, select **Un-assigned Devices**.

Step 2   To change the range of devices that are displayed, use the **Show devices with** selection at the top of the window in combination with the **matching** field.

- To list devices by hostname, select **Device Host Name** and enter a search value in the matching field, then click **Find**.

- To list devices by domain name, select **Device Domain Name** name and enter a search value in the matching field, then click **Find**.

- To list devices by management IP address, select Management IP Address and enter a search value in the matching field, then click **Find**.

The value in the **matching** field specifies a search mask that controls which devices are displayed. An asterisk (*) specifies display of all devices by the selected search criteria. A string followed by an asterisk specifies display of all devices starting with part of a hostname, domain name, or management IP address. And a string preceded by an asterisk specifies display of all devices ending with part of a hostname, domain name, or management IP address.

You can specify more than one wildcard (asterisk) value in a search string. For example, to display all devices that have "ce" in the hostname, enter *ce* in the matching field.

The display changes depending on the selection that you made. For example, if two devices have been assigned the CE role, the Role Assignment - CEs window appears.

Changing Device Assignments

In some instances, the device discovery process assigns the wrong device role to groups of devices. For example, devices that should be PEs can be assigned as CEs.

Cisco Confidential — Draft Label

If this occurs, perform these steps:

- If all the devices you expected would appear as PEs are not listed on the Role Assignment - PEs window, check the Role Assignment - Unassigned Devices window and the Role Assignment - CEs window and assign the devices as PE devices.

  – Go to the Role Assignment - CEs window and select any devices that should be PE devices

  – Click the **Assign as PEs** button

  The Role Assignment - PEs window appears and now lists the devices that you assigned as PEs.

- If other devices are not assigned as desired, change their basic device assignment as required.

Assigning Devices Individually or in Bulk

Using the windows provided for Role Assignment, you can assign device roles one device at a time or using bulk assignment (by selecting several devices and assigning them all the same role).

If you assign device roles for a single device, you can also assign the other device attributes, such as Site, Region, etc. However, if you assign device roles in bulk, then you cannot assign the other attributes at this time. You will have to go to the PEs or CEs window later to assign the other attributes.

Determine Device Roles

The purpose of device assignment is to categorize the devices discovered in the provider's network into two general groups:

- Provider-related devices—Provider Edge (PE) devices.

  See Assigning the PE Role, page E-35 for instructions on assigning the PE roles (U-PE, N-PE, P, or PE-AGG).

- Customer-related devices—Customer Edge (CE) devices

  See Assigning the CE Role, page E-38 for instructions on assigning the CE role.

For PE devices, use the following guidelines to determine device roles:

- Assign a device that is at the center of a core domain as a P device.

- Assign any devices that interface with users of the VPN services as U-PE devices. These are devices that are on the customer facing edge of a domain.

- Assign any devices that are on the edge of the MPLS core domain or L2VPN core domain as N-PE devices.

- Assign any devices that are in device rings or which connect to multiple U-PE devices as PE-AGG devices.

  For CE devices, see the descriptions of the CE roles in the section on assigning CE roles (Assigning the CE Role, page E-38) for specific information.

Assigning the PE Role

Follow these steps to assign a device as a PE device:

Step 1   In the Role Assignment - Un-assigned Devices window, select a device that you want to assign as a PE.

Cisco Confidential — Draft Label

- To select a device, check the check box next to the device name.
- To deselect a device, uncheck the check box next to the device name.

Step 2   Click the **Assign as PE(s)** button.

Step 3   In the Assign as PE window, assign the required information for the PE.

a. To assign a PE Region Name, click the **Select** button.

The PE Region Name window appears.

b. In the PE Region Name window, click the radio button next to the region name that you want to assign and then click **Select**.

The Assign as PE window appears with the region name in the PE Region field.

c. To assign a PE role, select a value from the pull-down list for the PE Role field.

The PE role specifies the architectural role that a PE router performs. Assign the PE role based on the network layer to which the device belongs.

You can select the following PE roles:

- **N-PE**—Assign devices that are at the edge of domains (within the Edge layer) as Network Facing Provider Edge (N-PE) devices.
- **U-PE**—Assign devices within the User Facing Provider Edge as U-PE devices.
- **P**—Assign a device that is at the center of a core domain as a Provider Core (P) device.
- **PE-AGG**—Assign devices within the Aggregation Layer as Provider Edge Aggregation (PE-AGG) devices.

d. Click **OK**.

The Role Assignment - PEs window appears with the specified values shown.

Editing the PE Role

After you have assigned one or more devices as PE devices and they appear in the Role Assignment - PEs window, you can edit the PE role. You can edit the PE role even if no values have been assigned in the Assign as PE window.

> **Note**   PE role assignment is not mandatory. However, it is recommended to avoid unexpected behavior.

Follow these steps to edit the Role Assignment values for a PE device:

Step 1   While the Role Assignment phase of Device Discovery is active, choose the Role Assignment - PEs window.

If the Role Assignment - Un-assigned Devices or the Role Assignment - CEs window is active, select **Role-Assignment - PEs** from the pull-down list at the bottom of the window.

The Role Assignment - PEs window appears, as shown in Figure E-8.

Cisco Confidential — Draft Label

Figure E-8   Role Assignment - PEs Window

Note that on this window, sorting is disabled for the following columns:

- PE Device Host Name
- PE Provider Name
- PE Region Name.

In the sample window shown in Figure E-8, one of the PEs has role information assigned. The other two PEs have been assigned as PEs but do not have role information assigned. You can edit any of the information for the PEs, whether information has been entered or not.

Step 2   Select one or more PEs to edit.

- To select a specific PE, check the check box next to the device name.
- To select all the PEs shown in the window, check the check box in the heading row.

Step 3   To edit the PE role, follow these steps:

   a. Click the **Edit** button at the bottom of the window and choose **PE Role** from the pull-down list.

   You are prompted to select a PE role.

   b. Select a value from the pull-down list for the PE Role field.

   You can select the following PE roles:

   – **N-PE**—Assign devices within the Edge layer as Network Facing Provider Edge (N-PE) devices.

   – **U-PE**—Assign devices within the User Facing Provider Edge as U-PE devices.

   – **P**—Assign devices within the Core layer as Provider Core (P) devices.

   – **PE-AGG**—Assign devices within the Aggregation Layer as Provider Edge Aggregation (PE-AGG) devices.

The specified PE role appears in the Role Assignment - PEs window.

Step 4   To edit the PE provider name or PE region name, follow these steps:

   a. Click the **Edit** button at the bottom of the window and choose **Region/Provider** from the pull-down list.

   You are prompted for a Region name.

   b. Click the radio button next to one of the region names listed in the pop-up window and then click the **Select** button.

Cisco Confidential — Draft Label

The specified Region Name and its associated Provider Name appear in the Role Assignment - PEs window.

Assigning the CE Role

Follow these steps to assign a device as a CE device:

Step 1 In the Role Assignment - Un-assigned Devices window, select a device that you want to assign as a CE.

- To select a device, check the check box next to the device name.
- To deselect a device, uncheck the check box next to the device name.

Step 2 Click the **Assign as CE(s)** button. The Assign as CE window appears.

Step 3 In the Assign as CE window, assign the required information for the CE.

a. To assign a Customer Name (required field), click the **Select** button.

The Customer Name window appears.

b. To assign a customer name, click the radio button next to the customer name that you want to assign and then click the **Select** button.

The Assign as CE window appears with the specified customer name displayed.

c. To assign a CE management type, select a value from the pull-down list for the CE Management Type.

The CE Management type specifies the architectural role that a CE router performs. Assign the CE management type based on the network layer to which the device belongs.

You can select the following CE management types:

- **MANAGED-REGULAR**—This is the default CE role assignment. Assign this role to CEs that you want the Provider to manage. The CE must be reachable from an Prime Provisioning server. When you assign this role, then when you create a router in the Inventory Manager interface, the router configuration is automatically downloaded.

- **UNMANAGED**—Assign this role to a device that you want to manage manually. If this role is assigned, then the device configuration is not assigned automatically when a new device is created and the device must be configured manually. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration. The configuration is downloaded automatically when a new device is created. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration, but the configuration is not downloaded automatically when a new device is created. 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.

- **DIRECT-CONNECTED-REGULAR**—In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.

- **DIRECT-CONNECTED-MGMT-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**—Specifies that there is a device between the PE and the CE that is a VPN routing/forwarding instance (VRF). A multi-VRF CE (MVRFCE) is owned by the customer, but resides in the provider space. It is used to off-load 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.

d. Click **OK**.

The Role Assignment - CEs window appears with the specified values shown.

Note   The CE Site value is unassigned at this point. To assign this value, you must edit the settings. See Editing the CE Role, page E-39 for instructions on this task.

Editing the CE Role

After you have assigned one or more devices as CE devices and they appear in the Role Assignment - CEs window, you can edit the CE role. You can edit the CE role even if no values have been assigned in the Assign as CE window.

Follow these steps to edit the Role Assignment values for a CE device:

Step 1   While the Role Assignment phase of Device Discovery is active, choose the Role Assignment - CEs window.

If the Role Assignment - Un-assigned Devices or the Role Assignment - PE window is active, select **Role-Assignment - CEs** from the pull-down list at the bottom of the window.

The Role Assignment - CEs window appears.

Figure E-9   Role Assignment - CEs Window

In the sample Role Assignment - CEs window shown in Figure E-9, two of the CEs have role assignment information assigned, and two have no information assigned. You can edit any of the information for the CEs, whether information has been entered or not.

Note that on this window, sorting is disabled on the following columns:

- CE Device Host Name

- CE Site Name

- CE Customer Name

Step 2   Select one or more CEs to edit.

- To select a specific CE, check the check box next to the device name.

- To select all the CEs shown in the window, check the check box in the heading row.

Step 3   To edit the Customer name, follow these steps:

a.   Click the **Edit** button at the bottom of the window and choose **Customer** from the pull-down list.

You are prompted to select a customer name.

b.   To select a customer name, click the radio button next to one of the customer names that is displayed, and then click the **Select** button.

The Role Assignment - CEs window appears with the specified customer name displayed.

Step 4   To edit the CE management type, follow these steps:

a.   Select one or more CEs to edit.

b.   Click the **Edit** button at the bottom of the window and choose C**E Management Type** from the pull-down window.

The CE Management type specifies the architectural role that a CE router performs. Assign the CE management type based on the network layer to which the device belongs.

You can select the following CE management types:

- **MANAGED-REGULAR—**This is the default CE role assignment. Assign this role to CEs that you want the Provider to manage. The CE must be reachable from an Prime Provisioning server. When you assign this role, then when you create a router in the Inventory Manager interface, the router configuration is automatically downloaded.

- **UNMANAGED—**Assign this role to a device that you want to manage manually. If this role is assigned, then the device configuration is not assigned automatically when a new device is created and the device must be configured manually. 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-MGMT-LAN—**Specifies that the device management is linked to the PE configuration. The configuration is downloaded automatically when a new device is created. 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-MGMT-LAN—**Specifies that the device management is linked to the PE configuration, but the configuration is not downloaded automatically when a new device is created. 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.

- **DIRECT-CONNECTED-REGULAR—**In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.

- **DIRECT-CONNECTED-MGMT-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**—Specifies that there is a device between the PE and the CE that is a VPN routing/forwarding instance (VRF). A multi-VRF CE (MVRFCE) is owned by the customer, but resides in the provider space. It is used to off-load 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.

  c. Click **Select**.

The Role Assignment - CEs window appears with the specified CE management type displayed.

Step 5 To specify a site name or edit an existing site name, follow these steps:

  a. Select one or more CEs to edit.

  b. Click the **Edit** button at the bottom of the window and choose **Site** from the pull-down window.

The Site Name window appears.

  c. In the Site Name window, click the radio button next to the site name that you want to assign and then click the **Select** button.

The Role Assignment - CEs window appears with the specified site names displayed.

Saving the Role Assignment Information

After you finish assigning roles to the devices, click the **Continue** button.

The Role Assignment Discovery indicator turns green and indicates that Role Assignment is **Complete**.

You are now ready to start the NPC Discovery phase of Device Discovery.

Step 5: Perform NPC Discovery

After the Role Assignment phase of Device Discovery is complete, the Discovery Workflow window indicates that the NPC Discovery phase is **Pending Input**.

Follow these general steps to view a list of the NPCs that have been discovered and add or remove NPCs as required:

- If you are discovering *a Metro Ethernet topology with an Ethernet core*, perform the steps described in Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks, page E-41.

- Complete the steps for starting NPC assignment as described in Starting NPC Assignment, page E-43

- If necessary, complete steps for adding or modifying NPCs as described in Adding a Device for an NPC, page E-44 and the sections that follow.

Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks

Follow these steps if you are discovering a Metro Ethernet topology with an Ethernet core.

- Create one or more Access Domains and assign the devices that were discovered in the Device Discovery phase to the Access Domain(s).
- Create at least one Resource Pool.
- Edit the "inter N-PE interface" for each device.

These steps are performed using the Inventory and Connection Manager in the Service Inventory interface (**Service Inventory > Inventory and Connection Manager**).

Creating Access Domains

Follow these steps to create access domains and add discovered devices to the domains:

Step 1   In the Prime Provisioning start page, select **Service Inventory**.

Step 2   In the Service Inventory window, select **Inventory and Connection Manager**.

The Inventory and Service manager window appears.

Step 3   In the left area of the window, select **Access Domains**.

The Access Domains window appears.

Step 4   Create one or more Access Domains and assign the devices in the L2VPN Metro Ethernet topology to these Access Domains.

For detailed instructions on creating Access Domains, see the Creating Access Domains, page 2-41 section of Chapter 2, "Before Setting Up Prime Provisioning".

Creating Resource Pools

Follow these steps to create a resource pool:

Step 1   In the Prime Provisioning start page, select **Service Inventory**.

Step 2   In the Service Inventory window, select **Inventory and Connection Manager**.

The Inventory and Service manager window appears.

Step 3   In the left area of the window, select **Resource Pools**.

The Resource Pools window appears.

Step 4   Create a Resource Pools.

Step 5   For the **Pool Type**, make sure that you select **VLAN**.

Step 6   For the **Start** value, enter 2.

Step 7   For the **Pool Size** value, enter a value large enough to accommodate the number of devices in the resource pool, for example, 500.

For detailed instructions on creating Resource Pools, see the Resource Pools, page 2-44 section of Chapter 2, "Before Setting Up Prime Provisioning".

Cisco Confidential — Draft Label

Editing Inter-N-PE Interfaces

Follow these steps to edit the "Inter N-PE" interfaces for the devices in your Metro Ethernet topology:

Note   These steps are only required if the PE devices already exist in the repository.

Step 1   In the Prime Provisioning start page, select **Service Inventory**.

Step 2   In the Service Inventory window, select **Inventory and Connection Manager**.

The Inventory and Service manager window appears.

Step 3   In the left area of the window, select **PE Devices**.

The PE Devices window appears.

Step 4   Select each PE device in your topology and do the following:

    a.   Click the **Edit** button

        The Edit PE window appears.

    b.   Locate the interface that connects to each device that the device is connected to.

    c.   For each interface, in the Metro Ethernet column, change **Any** to **None**.

    d.   Save your changes

Go the following section, Starting NPC Assignment, page E-43 and follow the steps for starting NPC assignment.

Starting NPC Assignment

Follow these steps to initiate NPC assignment:

Step 1   In the Discovery Workflow window, click **Continue**.

The Named Physical Circuits window appears.

The Named Physical Circuits window initially displays any discovered circuits.

At this point, you can create, add, or remove NPCs as required.

The State column has the following categories:

- **New**—No corresponding NPC exists in Prime Provisioning. Only the New NPCs are committed to Prime Provisioning.

- **Existing**—The discovered NPC is the same as the NPC in Prime Provisioning.

- **Existing Modified** —The NPC in Prime Provisioning has the same source and endpoint but one or more of the intermediate links might not be the same.

- **Conflicting**—The discovered NPC conflicts with the NPC in Prime Provisioning.

Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or U-PE and a N-PE. The intermediate nodes of the NPCs can either be U-PE or PE-AGG. 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 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.

Step 2   If you need to define an NPC, follow these steps:

    a.   In the Named Physical Circuits window, click **Create**.

        The Create a Physical Circuit window appears.

    Initially, the list of NPCs is empty.

    b.   Click the **Add Device** button

    The Select a Device window appears.

Step 3   In this window, click the radio button for a device and then click the **Select** button.

    The Create a Named Physical Circuit window appears with an initial device added.

        The buttons on the window are now active.

    c.   Click a device that appears in the screen and then select one of the following actions:

        –   To insert a device, click the **Insert Device** button.

        –   To insert a ring, click the **Insert Ring** button.

        –   To add a device, click the **Add Device** button.

        –   To add a ring, click the **Add Ring** button.

        –   To delete an existing device or ring, select a device and then click the **Delete** button.

Step 4   Refer to the following sections for additional information.

Adding a Device for an NPC

Step 1   To select an incoming interface on the Create a Named Physical Circuit window click on **Select Incoming Interface**.

    The Select Device Interface window appears. This window shows the interfaces on the selected device.

Step 2   Click the radio button next to an interface in the list and then click the **Select** button.

    The selected interface now appears in the Create a Named Physical Circuit window.

Step 3   To select an outgoing interface, click on **Select Outgoing Interface**.

    A list of interfaces configured on the device appears

Step 4   Click the radio button next to an interface in the list and then click the **Select** button.

    The outgoing interface now appears in the Create a Named Physical Circuit window.

Step 5   Select additional devices as required and specify incoming and/or outgoing interfaces.

Step 6   After you are finished, click the **Save** button in the Create a Named Physical Circuit window.

Adding a Ring

Follow these steps to add a ring before the currently selected device:

> **Note**   Incremental service discovery of rings is not supported.

Step 1   In the Create a Named Physical Circuit window, click **Add Ring**.

The Select NPC Rings window appears. This window shows any rings that exist in the network topology.

Step 2   Click the radio button next to a ring listed in the window and then click the **Select** button.

The selected ring now appears in the Create a Named Physical Circuit window.

Inserting a Device

To insert a device after the last device in the topology, follow these steps:

Step 1   In the Create a Named Physical Circuit window, click the **Insert Device** button.

The Select a Device window appears.

Step 2   Check the check box next to a device that you want to insert and then click the **Select** button.

The device now appears on the Create a Named Physical Circuit window.

Step 3   Click **select incoming interface**.

A list of interfaces on the selected device appears.

Step 4   Check the check box next to the interface that you want to choose and then click **Select**.

The selected interface now appears on the list of interfaces.

Inserting a Ring

To insert a ring after the last device in the topology, follow these steps:

Step 1   In the Create a Named Physical Circuit window, click the **Insert Ring** button.

A list of the currently existing rings appears.

Step 2   In the list of rings, check the check box next to the ring that you want to insert and then click **Select**.

The selected ring now appears on the Create a Named Physical Circuit window.

Deleting a Device or a Ring

To delete a device or a ring, in the Create a Named Physical Circuit window, select a device or ring and then click the **Delete** button.

The create NPC window appears with the device deleted.

Saving the NPC Configuration

After you have selected two devices and have configured the connection between them, follow these steps to save the NPC configuration:

Step 1   In the Create a Named Physical Circuit window, click **Save**.

The NPC process validates the NPC configuration.

Step 2   Click **Continue** to continue.

The workflow window appears with NPC discovery marked as completed.

Step 6: Perform MPLS VPN Service Discovery (Optional)

After you have completed the NPC Discovery phase of Device discovery, if you selected **MPLS VPN Discovery** when you initiated the Discovery process, the NPC Discovery phase is marked as complete, and the MPLS VPN Discovery step is marked as **Pending Input**.
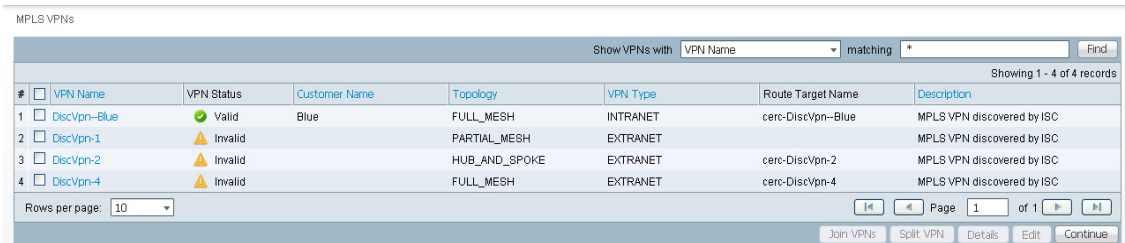
You are now ready to initiate configuration of the discovered MPLS VPN using the MPLS VPN Discovery user interface. Follow these steps to configure MPLS VPN services:

> **Note**   MPLS service discovery does not support devices running IOS XR.

Step 1   In the Discovery Workflow window, click **Continue**.

The MPLS VPNs window appears and lists the MPLS VPNs that were discovered. The status of the discovered MPLS VPNs is indicated as follows:

- If the MPLS VPN topology for a discovered MPLS is valid and ready to save in the Prime Provisioning Repository, then the VPN Status indicates a **Valid** VPN and the status indicator is green.

- If the MPLS VPN topology for a discovered MPLS is invalid (the topology is Partial Mesh), is missing a Customer assignment, or includes an invalid Route Target, then the VPN Status indicates an **Invalid** VPN and the status indicator is yellow. Partial Mesh topology VPNs are not supported by Prime Provisioning, and must be broken into Full Mesh and/or Hub and Spoke components.

The MPLS VPN window shown in Figure E-10 shows an invalid MPLS VPN (the topology is Partial Mesh and the Customer Name is blank).

Cisco Confidential — Draft Label

Figure E-10   MPLS VPNs Window with Invalid MPLS VPN

> **Note**   If the MPLS VPN Discovery process discovers an MPLS VPN with a Partial Mesh topology, you must split the VPN into two or more separate VPNs that have a supported topology (Hub and Spoke or Full Mesh).

Step 2   Do one of the following:

- If you want to change the view in the MPLS VPNs window, select another view option.

  For a description of the MPLS VPN view options, see Filtering the MPLS VPN View, page E-47.

- If the MPLS VPNs are valid and you do not need to make any changes to the MPLS VPN topology at this time, click **Continue** to create MPLS VPN services based on the discovered topology.

- If one or more of the discovered MPLS VPNs are invalid, you must complete the following steps:

  - **Split the VPN**—Select an invalid VPN and then click the **Split VPN** button.

    See Splitting a VPN, page E-48 for instructions.

  - **Create New VPNs and add Route Targets**—You must create new VPNs containing the devices in the VPN that you have split, and add Route Targets to each new VPN.

    See Creating a VPN, page E-49 for instructions.

Filtering the MPLS VPN View

Follow these steps to change the view in the MPLS VPNs window:

Step 1   Pull down the menu next to the **Show VPNs with** field.

You can filter the list of VPNs by VPN Name, Customer Name, Topology, VPN Type, or Description.

Step 2   To limit which VPNs are displayed within the selected category, enter a value in the **Matching** field.

The value in the **matching** field specifies a search mask that controls which sites are displayed. An asterisk (*) specifies display of all sites by the selected search criteria. A string followed by an asterisk specifies display of all sites starting with part of the element specified in the **Show VPNs with** field.

You can specify more than one wildcard (asterisk) value in a search string. For example, to display all VPNs that have "cisco" as part of the Customer Name, enter *cisco* in the matching field.

The display changes to display the VPNs with the selected criteria.

Cisco Confidential — Draft Label

Splitting a VPN

In some situations, you might need to split an existing MPLS VPN before you complete the MPLS VPN Discovery process and actually create the MPLS VPN services.

For example:

- If the MPLS Service Discovery process discovers an invalid MPLS VPN (an MPLS VPN with a Partial Mesh topology), you must split the VPN into two or more Route Targets that have a supported topology (Hub and Spoke or Full Mesh).

- You might also choose to split MPLS VPNs to change your topology, depending on your processing needs. Only one VPN can be split at a time.

Follow these steps to split a VPN:

Step 1   In the MPLS VPNs window, check the check box next to a VPN that you want to split.

Step 2   Click the **Split VPN** button.

The Split VPN window appears, as shown in Figure E-11.

Figure E-11   **Split VPN Window**

Step 3   In the Split VPN window, select several of the links.

Select the links that would comprise either a Hub and Spoke or Full Mesh topology.

For example, in the Split VPN window shown in Figure E-11, the first three links all have Route Targets of **1:102** and together form a Full Mesh topology.

The remaining two links have Route Targets of **1:106** and **1:105**. These links together form a Hub and Spoke topology.

To split this VPN, the first three links need to be associated with one Route Target, and the two remaining links need to be associated with another Route Targets. Then we can split this VPN into two separate VPNs following the Prime Provisioning best practice convention of one Route Targets per VPN.

Step 4   Click the **Create/Modify CERC** button.

You are prompted for a Route Targets name.

Step 5   Enter the new Route Targets name and then click the **Save** button.

Step 6   Repeat these steps for the rest of the devices that are included in invalid VPNs.

C i s c o   C o n f i d e n t i a l   —   D r a f t   L a b e l

For example, in the topology shown Figure E-11, select the devices that have the route target **1:106 to 1:105**.

Step 7   Click the **Create/Modify CERC** button.

Step 8   When you are prompted for a Route Target name, enter the new Route Target name and then click the **Save** button.

The Split VPNs window appears again, and the window shows the new Route Targets that have been created.

Notice that in the example, the two new Route Targets that have been created (**valid_cerc_one** and **valid_cerc_two**), have valid topologies. The first Route Target, v**alid_cerc_one,** has a Full Mesh topology and the second Route Target, **valid_cerc_two**, has a Hub and Spoke topology.

Step 9   Click the **Save** button.

You are now ready to continue to the next step, creating VPNs and adding Route Targets to the VPNs.

Creating a VPN

After you have created a Route Target, you must create a VPN and then add the Route Target to it.

Follow these steps to create a VPN:

Step 1   In the Split VPN window, select **Create/Modify VPN.**

The Create VPN window appears.

Step 2   Select the Route Targets that you want to assign to the VPN.

Step 3   In the VPN Name field, enter a name for the VPN.

For this example, enter **vpn_one**.

Step 4   Click the **Assign VPN Name** button.

Step 5   Click **Save**.

The VPN is created and appears in the Split VPN window in the VPN Name field.

Step 6   Create any additional VPNs as needed.

Continuing with the Route Targets shown in the sample windows in Splitting a VPN, page E-48, a VPN must be created and have a Route Target assigned to it. To do this:

   a.   In the Split VPN window, click **Create/Modify VPN**.

   b.   In the Create VPN window, create a second VPN and assign a Route Target to it.

In the example screen, you could select the second Route Target (**valid_cerc_two**) to the newly created VPN to it.

Step 7   After you are finished creating VPNs, click the **Save** button in the Split VPN window.

The MPLS VPNs window appears.

Cisco Confidential — Draft Label

Note   In the example shown, one of the VPNs is marked as **Valid** and has a green status indicator. However, the other VPN shown in the window is marked as **Invalid** and has a yellow indicator.

This occurs because in some instances, the MPLS Discovery process cannot completely validate the data. In this situation, you can still continue with the Service Discovery process and create MPLS VPN services. However, the process will skip the invalid VPN, and you must configure the VPN service manually using the Prime Provisioning provisioning commands.

Step 8   Follow these steps to assign a Customer to each VPN:

a.   Select a VPN entry in the MPLS VPNs window and then click the **Edit** button.

The Edit VPN window appears.

b.   Click the **Select** button next to the Customer Name field.

A list of customer names appears.

c.   Click the radio button next to customer name and then **Select**.

d.   If you want to rename the Route Target, click **Rename** and then rename it.

e.   Click **Save**.

The Customer name now appears in the MPLS VPNs window.

Note   In some cases, an apparently valid VPN will be marked as invalid. This VPN will be skipped in the processing. You will then have to configure it manually using the Prime Provisioning provisioning commands.

Step 9   After you are finished editing VPNs, click the **Continue** button to initiate the MPLS VPN service creation process.

Viewing VPN Link Details

Follow these steps to view details of VPNs that were discovered:

Step 1   In the MPLS VPNs window, select a VPN that has details you want to view and then click the **Details** button.

The MPLS VPN Link window appears.

Step 2   To filter the MPLS VPN links that are displayed, select a value from the pull-down list in the **Show Sites with** field.

You can filter the list of VPNs by From Site, From CE, From CE Domain, Route Target, To Site, To CE, or to CE Domain.

The value in the **matching** field specifies a search mask that controls which sites are displayed. An asterisk (*) specifies display of all sites by the selected search criteria. A string followed by an asterisk specifies display of all sites starting with part of the element specified in the **Show Sites with** field.

Cisco Confidential — Draft Label

You can specify more than one wildcard (asterisk) value in a search string. For example, to display all sites that have "realtime" in the From CE Name, select **From CE Name** in the **Show Sites with** field and then name, enter *realtime* in the matching field.

The display changes to show only the specified links.

Saving the MPLS VPNs and Initiating MPLS VPN Service Creation

After you are finished editing the data for the discovered MPLS VPNs in the MPLS VPNs window, click the **Continue** button.

The Discovery process creates VPN services. After the process is complete, the Discovery Workflow window indicates that the MPLS VPN Discovery process is **COMPLETE** and the status indicator is green.

If you also selected **L2VPN (Metro Ethernet) Discovery** in the Discovery window before starting the Discovery process, you can now proceed to Carrier Ethernet service discovery.

Step 7: Perform L2VPN (Metro Ethernet) Service Discovery (Optional)

If you selected **L2VPN (Carrier Ethernet) Discovery** in the Discovery window before starting the Discovery process, then after the previous steps are complete, the Discovery Workflow window shows the L2VPN (Metro Ethernet) Discovery as **Pending Input**.

Follow these steps to initiate Metro Ethernet Service Discovery:

Note L2VPN service discovery does not support devices running IOS XR and does not discover services defined using the EVC CLI framework.

Step 1 Before you initiate Metro Ethernet Service Discovery, follow these steps:

  a. Choose **Service Inventory > Inventory and Connection Manager.**

  b. In the task pane at the left of the Inventory and Connection Manager window, select **Access Domains**.

  c. Create access domains for any N-PE devices in the Metro Ethernet topology.

  For detailed instructions, see the Creating Access Domains, page 2-41 section of Chapter 2, "Before Setting Up Prime Provisioning".

  d. Choose **Service Inventory > Inventory and Connection Manager.**

  e. In the task pane at the left of the Inventory and Connection Manager window, select **Resource Pools**.

  f. Create resource pools for each of the access domains that you created.

  For detailed instructions, see the Resource Pools, page 2-44 section of Chapter 2, "Before Setting Up Prime Provisioning".

  g. Choose **Service Inventory > Discovery.**

Cisco Confidential — Draft Label

The Discovery Workflow window shows the L2VPN (Metro Ethernet) Discovery process as **Pending Input.**

Step 2   Click **Continue**.

The L2VPN Discovery (Ethernet Services) window appears.

Step 3   Select one of the following actions:

- **View/Edit Discovered Layer 2 Services grouped by VPN**—Allows you to view the discovered L2VPN services and edit them as required.

- **View/Edit Discovered Layer 2 End to End Wires**—Allows you to view the discovered Layer 2 End to End wires and edit them as required.

- **View/Edit Discovered Layer 2 VPLS Links**—Allows you to view the discovered Layer 2 Virtual Private LAN Service (VPLS) links and edit them as required.

The following sections of this chapter describe each of these actions.

Viewing Discovered Layer 2 Services Grouped by VPN

Follow these steps to view discovered Layer 2 services grouped by VPN:

Step 1   In the L2VPN Discovery (Ethernet Services) window, click the **VPNs** button.

The L2VPNs window appears.

The L2VPNs window allows you to perform the following tasks:

- View detailed information about a Layer 2 VPN.

    This task is explained in the following steps of this procedure.

- Display a window that allows you to edit the configuration information for an existing Layer 2 VPN.

    See Editing Discovered Layer 2 Services Grouped by VPN, page E-52 for detailed instructions.

- Delete an existing Layer 2 VPN.

    See Deleting Discovered Layer 2 Services Grouped by VPN, page E-53 for instructions on this task.

Step 2   To view detailed information about a Layer 2 service, check the check box next to a VPN that has details you want to view, and then click the **Details** button.

The L2VPN Details window appears.

The L2VPN Details window shows the details about the discovered VPN, such as the User-Network Interface (UNI), in a table format.

Step 3   When you are finished viewing the link details, click the **Close** button.

Editing Discovered Layer 2 Services Grouped by VPN

You can edit a discovered Layer 2 VPN service to change the policy that is applied to the service. Follow these steps to edit a Layer 2 VPN service:

Step 1   In the L2VPNs window, check the check box next to a VPN that you want to edit, and then click the **Edit** button.

The Edit VPN window appears.

Step 2   To edit the VPN name, enter a new VPN name in the VPN Name field.

Step 3   To edit the Customer Name, follow these steps:

a.   Click the **Select** button next to the Customer Name.

A list of customers appears.

b.   Click the radio button next to the new Customer Name that you want to configure.

c.   Click the **Save** button.

The new VPN name and/or Customer Name appears in the Metro Ethernet End to End Wires window.

Deleting Discovered Layer 2 Services Grouped by VPN

Follow these steps to delete a Layer 2 service:

Step 1   In the L2VPNs window, check the check box next to a VPN that you want to delete, and then click the **Delete** button.

The following message appears:

```
Links/End to End wires associated with all selected VPNs will be deleted as a result of
this operation. Do you really want to Delete?
```

Step 2   If you are sure that you want to delete the VPN, click **OK**; otherwise, click **Cancel**.

If you click **OK**, the VPN and associated links and end-to-end wires are deleted.

Editing the Policy using Discovered Layer 2 VPN Services

You can edit a discovered Layer 2 VPN service to change the policy that is applied to the service. Follow these steps to edit a Layer 2 VPN service:

Step 1   In the L2VPNs Details window, check the check box next to a UNI associated to the VPN and then click the **Edit** button.

The Edit Link Policy window appears.

Step 2   To change the link policy for the service, follow these steps:

a.   Click the **Policy** button next to the Policy Name field.

A list of policies appears.

You can change the list of policies by choosing a filter from the pull-down list in the **Show VPN policies with** field and/or entering a search mask in the **Matching** field.

You can filter the policy list by Policy Name, Customer Name, Provider Name, or Global policy name. And you can limit the lists of policies displayed in the selected category by entering a value in the Matching field.

Step 3 Click the radio button next to a policy that you want to apply to the service and then click **Select**.

Step 4 Do one of the following:

- Click **Save** to save your changes.
- Click **Cancel** to cancel the changes.

Viewing Discovered Layer 2 End to End Wires

Follow these steps to view discovered Layer 2 end-to-end wires:

Step 1 In the L2VPN Discovery (Ethernet Services) window, click the **End-End Wires** button.

The Metro Ethernet End to End Wires window appears.

The Metro Ethernet End to End Wires window allows you to perform the following tasks:

- View detailed information about a Metro Ethernet end-to-end wire.

    This task is explained in the following steps of this procedure.

- Edit the VPN associated with the end-to-end wire.

    See Editing the VPN Associated with an End to End Wire, page E-55 for a description of this task.

- Split an existing end-to-end wire into two end-to-end wires

    See Splitting Layer 2 Service End to End Wires, page E-55 for a description of this task.

- Join existing end-to-end wires into a single end-to-end wire

    See Joining Layer 2 Service End to End Wires, page E-55 for a description of this task.

- Delete an existing end-to-end wire.

    See Viewing Discovered Layer 2 End to End Wires, page E-54 for instructions on this task.

Step 2 To view detailed information about a Layer 2 service, check the check box next to a UNI that has details you want to view, and then click the **Details** button.

Step 3 When you are finished viewing the link details, click the **Close** button.

Step 4 If you want to view the details of the interfaces in the end-to-end wire, click the interface name in either the AC1 UNI or AC2 UNI field.

If you click on an interface name, the Interface Detail window appears. The Interface Detail window shows details about the selected interface, such as the hostname of the host where the interface is located, the type of encapsulation used on the interface, and the switch mode used on the interface.

Step 5 When you are finished viewing the interface details, click the **Close** button.

Cisco Confidential — Draft Label

Editing the VPN Associated with an End to End Wire

From the Metro Ethernet End to End Wires window, you can also edit the VPN that is associated with the end-to-end wire.

Follow these steps to edit the VPN associated with an end-to-end wire:

Step 1   In the Metro Ethernet End to End Wires window, click a VPN name shown in the VPN name field.

The Edit VPN window appears.

Step 2   To edit the VPN name, enter a new VPN name in the VPN Name field.

Step 3   To edit the Customer Name, follow these steps:

   a.   Click the **Select** button next to the Customer Name.

   A list of customers appears.

   b.   Click the radio button next to the new Customer Name that you want to configure.

   c.   Click the **Save** button.

The new VPN name and/or Customer Name appears in the Metro Ethernet End to End Wires window.

Splitting Layer 2 Service End to End Wires

You can split off an existing end-to-end wire from the VPN that it is associated with and associate it with a new VPN.

Follow these steps to split an end-to-end wire from an existing VPN:

Step 1   In the Metro Ethernet End to End Wires window, check the check box next to an end-to-end wire entry that you want to split from a VPN.

> **Note**   If there is only one ID for the VPN associated with the end-to-end wire, then you cannot perform a split action on the wire.

Step 2   Click the **Split** button.

A message appears asking if you want to proceed.

Step 3   If you want to continue with the process, click **OK**.

The end-to-end wires are split and are associated with two new VPNs. These names of the VPNs are created by the system by adding a new number to the end of the existing VPN name.

Joining Layer 2 Service End to End Wires

You can join two existing end-to-end wires to a single VPN.

Follow these steps to join two existing end-to-end wires:

Step 1 In the Metro Ethernet End to End Wires window, check the check box next to several end-to-end wire entries that you want to join.

A message appears asking if you want to proceed.

Step 2 If you want to continue with the process, click **OK**.

The selected end-to-end wires are joined to a new VPN. The name for this VPN is created by the system by adding a new number to the end of the existing highest numbered VPN name.

Deleting Layer 2 Service End to End Wires

Follow these steps to delete an existing end-to-end wire:

Step 1 In the Metro Ethernet End to End Wires window, check the check box next to one or more end-to-end wires that you want to delete.

A message appears asking if you want to proceed.

Step 2 If you want to continue with the process, click **OK**.

The selected end-to-end wire (or wires) is deleted. Any Attachment Circuit(s) associated with the wire(s) are also deleted.

Step 3 Click **Close** to close the Metro Ethernet End to End Wires window.

Viewing Discovered Layer 2 VPLS Links

Follow these steps to view discovered Layer 2 VPLS links:

Step 1 In the L2VPN Discovery (Ethernet Services) window, click the **VPLS Links** button.

The VPLS Links window appears.

The VPLS Links window allows you to perform the following tasks:

- View detailed information about a VPLS link.

  This task is explained in the following steps of this procedure.

- Display a window that allows you to edit the configuration information for an existing VPLS link.

  See Editing Discovered Layer 2 VPLS Links, page E-57 for detailed instructions.

- Delete an existing Layer 2 VPN.

  See Deleting Discovered Layer 2 VPLS Links, page E-57 for instructions on this task.

Step 2 To view detailed information about a VPLS link, check the check box next to a VPLS link that has details you want to view, and then click the **Details** button.

The VPLS Link Detail window appears.

The VPLS Link Detail window shows the details about the discovered VPN and its link properties.

Step 3   When you are finished viewing the link details, click the **Close** button.

Editing Discovered Layer 2 VPLS Links

You can edit a discovered Layer 2 VPLS link to change the policy that is applied to the service. Follow these steps to edit a Layer 2 VPLS link:

Step 1   In the VPLS Links window, check the check box next to a VPLS link that you want to edit and then click the **Edit** button.

The Edit Link Policy window appears.

Step 2   To change the link policy for the link, follow these steps:

a.   Click the **Policy** button next to the Policy Name field.

A list of policies appears.

You can change the list of policies by choosing a filter from the pull-down list in the **Show VPN policies with** field and/or entering a search mask in the **Matching** field.

You can filter the policy list by Policy Name, Customer Name, Provider Name, or Global policy name. And you can limit the lists of policies displayed in the selected category by entering a value in the Matching field.

Step 3   Click the radio button next to a policy that you want to apply to the service, and then click **Select**.

Step 4   Do one of the following:

- Click **Save** to save your changes.
- Click **Cancel** to cancel the changes.

Deleting Discovered Layer 2 VPLS Links

Follow these steps to delete a VPLS link:

Step 1   In the VPLS Links window, check the check box next to a VPLS link that you want to delete and then click the **Delete** button.

The following message appears:

```
The selected link(s) will be deleted. Do you really want to Delete?
```

Step 2   If you are sure that you want to delete the VPLS, click **OK**; otherwise, click **Cancel**.

If you click **OK**, the VPLS link(s) are deleted.

Step 3   Click **Close** to close the VPLS links window.

Cisco Confidential — Draft Label

Saving the L2VPN Metro Ethernet Policy and Initiating Service Creation

After you are finished viewing or editing the discovered L2VPN Metro Ethernet topology, click the **Close** button to return to the L2VPN Discovery (Ethernet Services) window.

Click the **Continue** button to initiate the L2VPN Service Discovery process.

The Discovery Workflow window appears and indicates that the L2VPN Service Discovery process is **In Progress**. The status indicator is yellow.

After the L2VPN Service Discovery process is complete, the status indicator changes to green, and the Discovery Workflow window indicates that the L2VPN Service Discovery process is **Complete.**

Step 8: Commit Discovered Devices and Services to Prime Provisioning Repository

Click the **Continue** button to commit the discovered devices and services to the Prime Provisioning repository. Prior to this step, discovery workflow stores the discovered devices and services in a temporary repository, which gets committed to Prime Provisioning only at the last step of discovery workflow.

Step 9: Create and Run a Collect Config Task for the Discovered Devices

Before you view and edit services, follow these steps to run a Create Config task for the devices:

Note   For additional information on the Create Config task, see the Tasks, page 11-24 section of Chapter 11, "Monitoring".

Step 1   On the Prime Provisioning Start page, select **Monitoring**.

The Monitoring window appears.

Step 2   Select **Task Manager**.

The Tasks window appears.

Step 3   Click the **Create** button and choose **Collect Config** from the pull-down list.

The Create Task window appears.

Step 4   Click the **Next** button.

The Collect Config Task window appears.

Step 5   On the Collect Config task window, follow these steps to create and run a Collect Config task:

a.   Click the **Select/Deselect** button.

A dialog window appears, listing the devices that were discovered by the Discovery process.

b.   Select all of the devices shown on the list.

c.   Click the **Select** button.

Cisco Confidential — Draft Label

The Collect Config Task window appears again.

d. Specify the additional settings for the Collect Config task as required.

e. Click the **Submit** button.

You are now ready to view and edit services as described in the following section, Step 10: View and Edit Services, page E-59

Step 10: View and Edit Services

After you have successfully completed the MPLS VPN and/or L2VPN Metro Ethernet service creation process, you can view the services that were created and modify them using the service requests editors.

Follow these steps to view the L2VPN services:

Step 1   If the Service Inventory window is not currently active, click the **Operate > Service Request > Service Request Manager**.

The Service Request Manager window appears.

You can modify the service requests shown in the Service Requests window as required.

Note   If you need to edit MPLS VPNs as part of this process, see the Splitting a VPN, page E-48, Creating a VPN, page E-49, Viewing VPN Link Details, page E-50, and Saving the MPLS VPNs and Initiating MPLS VPN Service Creation, page E-51.

Step 2   For detailed information on modifying Service Requests for L2VPN Metro Ethernet networks, see Managing L2VPN and Carrier Ethernet Services, page 3-1.

Step 3   For general information on the release, see the *Cisco Prime Provisioning 6.4 Release Notes*, provided with the release.

Cisco Confidential — Draft Label