Setting Up the ISC Service

You define the service-related elements, such as target devices, VPNs, and network links. Normally, you create these elements once. This chapter contains the basic steps to set up the Cisco IP Solution Center (ISC) service for an L2VPN, L2TPv3, or VPLS service. It contains the following sections:

Note This chapter presents high-level information on ISC services that are relevant to L2VPN and VPLS. For more detailed information on setting up these and other basic ISC services, see *Cisco IP Solution Center Installation Guide, 4.1*.

Performing Device Settings to Support ISC

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

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

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

Configuring Switches in VTP Transparent Mode

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

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

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

```
Switch# Show vtp status
```

Setting the Loopback Addresses on N-PE Devices

See the section "Setting the Loopback Address" section on page 3-2 for information.

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

Every network element that ISC manages must be defined as a device in the system. An element is any device from which ISC can collect information. In most cases, devices are Cisco IOS routers that function as N-PE, U-PE, and P.

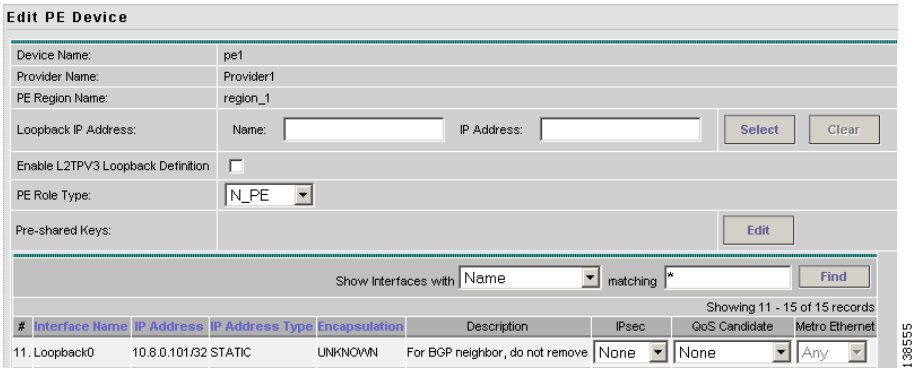
For detailed steps to create devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Setting the Loopback Address

The loopback address for the N-PE has to be properly configured for an AToMPLS connection. The IP address specified in the loopback interface must be reachable from the remote pairing PE. The LDP tunnels are established between the two loopback interfaces of the PE pair.

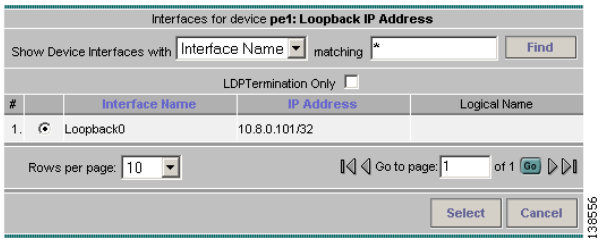
See Figure 3-1 for an example of a loopback address.

Figure 3-1 PE Loopback Address



To prevent a wrong loopback address being entered into the system, the loopback IP address field on the GUI is read only. You choose the loopback address with the help of a separate pop-up window, which you access by clicking the **Select** button. This ensures that you will select only a valid loopback address defined on the device. See Figure 3-2.

Figure 3-2 Select Device Interface



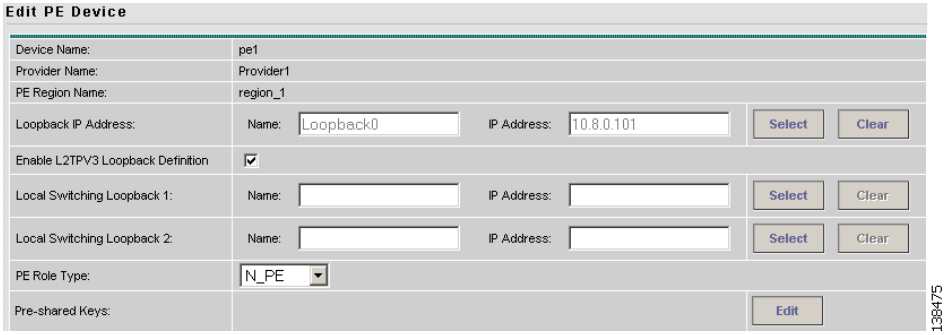
This feature ensures that a valid loopback address is set.

To further narrow the search, you can select the **LDPTermination Only** check box and click the **Select** button. This will then limit the list to the LDP-terminating loopback interface(s).

Setting the L2TPv3 Local Switching Loopback

Local switching requires that you select two loopback addresses. Each loopback must be unique. To set a second loopback address, select the **Enable L2TPV3 Loopback Definition** check box. See Figure 3-3.

Figure 3-3 PE Local Switching Loopback Addresses



This causes two additional GUI fields to appear, **Local Switching Loopback 1** and **Local Switching Loopback 2**. Use the **Select** button to set the local switching loopbacks.

Defining a Service Provider and Its Regions

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

For detailed steps to define the provider administrative domain, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining Customers and Their Sites

You must define customers and their sites before provisioning L2VPN. A customer is a requestor of a VPN service from an ISP. Each customer can own many customer sites. Each customer site belongs to one and only one Customer and can own many CPEs. For detailed steps to create customers, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining VPNs

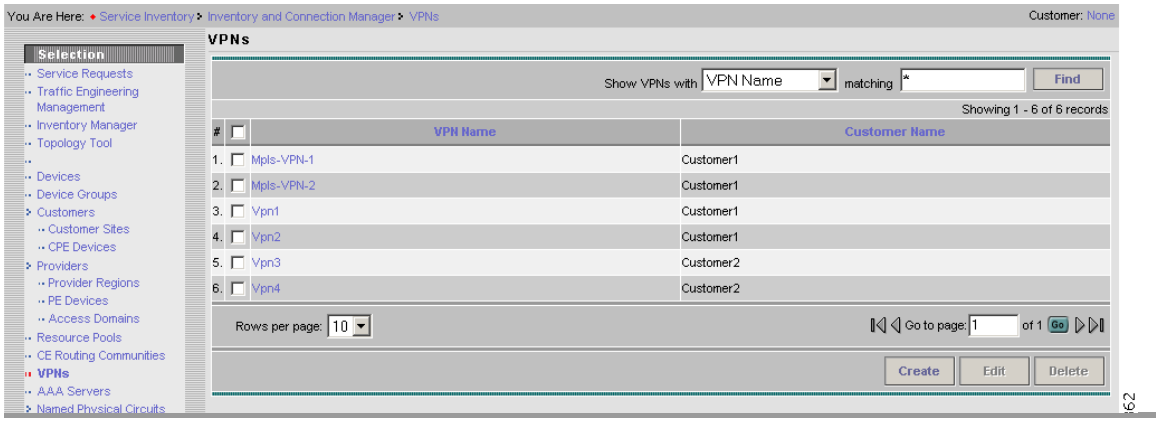
You must define VPNs before provisioning L2VPN or VPLS. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance.

To create a VPN, perform the following steps.

Step 1 Select **Service Inventory > Inventory and Connection Manager**.

Step 2 Click **VPNs** in the left column. The VPNs window appears as shown in Figure 3-4.

Figure 3-4 Defining a VPN



For detailed steps to create VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

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

Creating Access Domains

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

Note You do not create an access domain for L2TPv3.

For each Layer 2 access domain, you need a corresponding Access Domain object in ISC. During creation, you select all the N-PE devices that are associated with this domain. Later, one VLAN pool can be created for an Access Domain. This is how N-PEs are automatically assigned a VLAN. See Figure 3-5.

Before you begin, be sure that you:

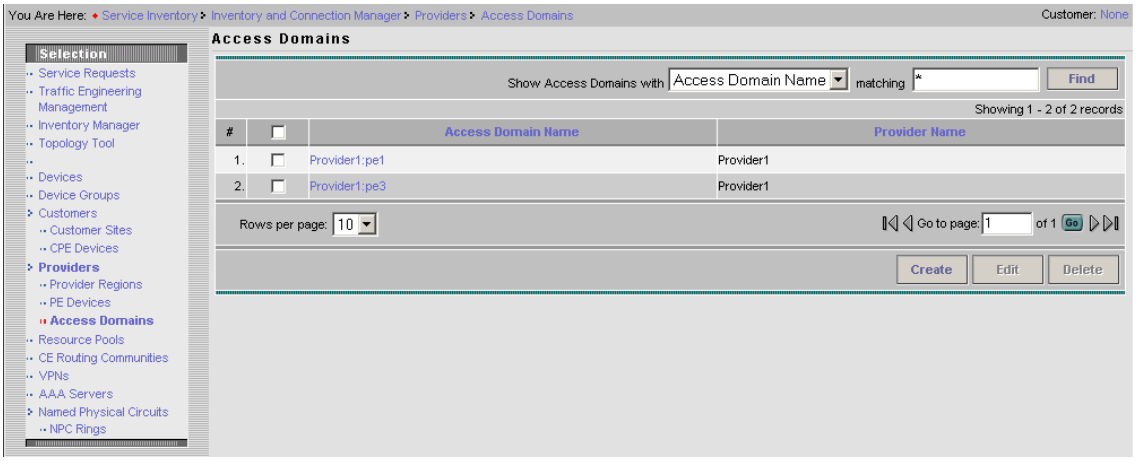
- Know the name of the access domain that you want to create.
- Have created a service provider to associate with the new access domain.
- Have created a provider region associated with your provider and PE devices.
- Have created PE devices to associate with the new access domain.
- Know the starting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

To create an Access Domain, perform the following steps.

Step 1 Select **Service Inventory > Inventory and Connection Manager**.

Step 2 Click **Access Domains** in the left column. The Access Domains window appears as shown in Figure 3-5.

Figure 3-5 Create an Access Domain



The Access Domains window contains the following:

- **Access Domain Name** Lists the names of access domains. The first character must be a letter. The name can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by access domain name.

- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- From the Access Domains window, you can create, edit, or delete access domains using the following buttons:
  - **Create—**Click to create new access domain. Enabled only if you do not select an access domain.
  - **Edit—**Click to edit the selected access domain (select by clicking the corresponding box). Enabled only if you select a a single access domain.
  - **Delete**—Click to delete the selected access domain (select by clicking the corresponding box). Enabled only if you select one or more access domains.

Creating VLAN Pools

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

You can also allocate VLAN IDs manually.

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

Note For L2TPv3, you do not create a VLAN pool.

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

Before you begin, be sure that you:

- Know each VLAN pool start number.
- Know each VLAN pool size.
- Have created an access domain for the VLAN pool (see Creating Access Domains, page 3-5).
- Know the name of the access domain to which each VLAN pool will be allocated.

Perform these steps if you want to have ISC automatically assign a VLAN to the links.

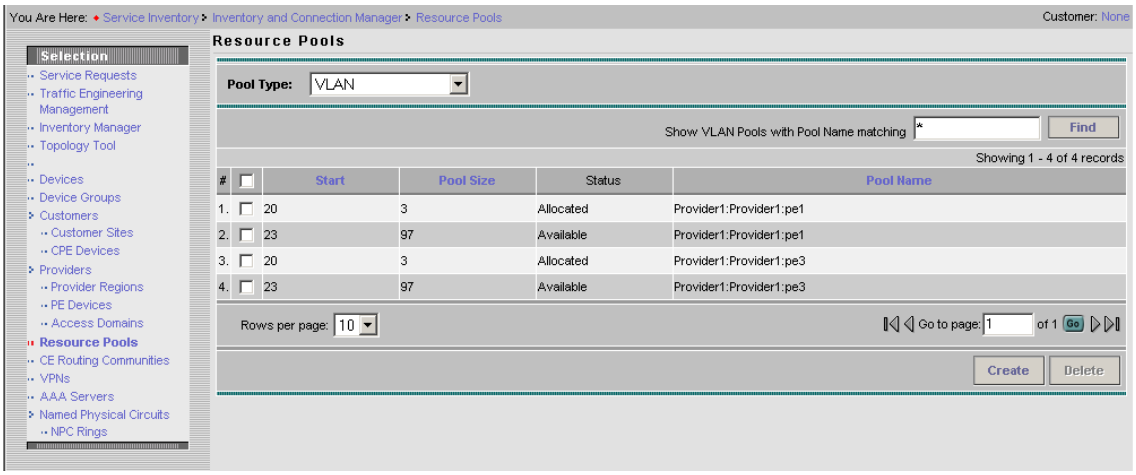
Step 1 Select **Service Inventory**.

Step 2 Select **Inventory and Connection Manager**.

Step 3 Select **Resource Pools**. The Resource Pools window appears.

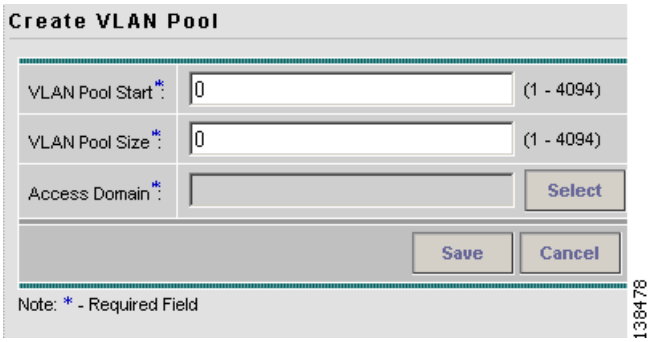
Step 4 Select **VLAN** from the drop-down **Pool Type** list as shown in Figure 3-6.

Figure 3-6 VLAN Resource Pools



Step 5 Click **Create**. The Create VLAN Pool window appears as shown in Figure 3-7.

Figure 3-7 Create VLAN Pool



Step 6 Enter a VLAN Pool Start number.

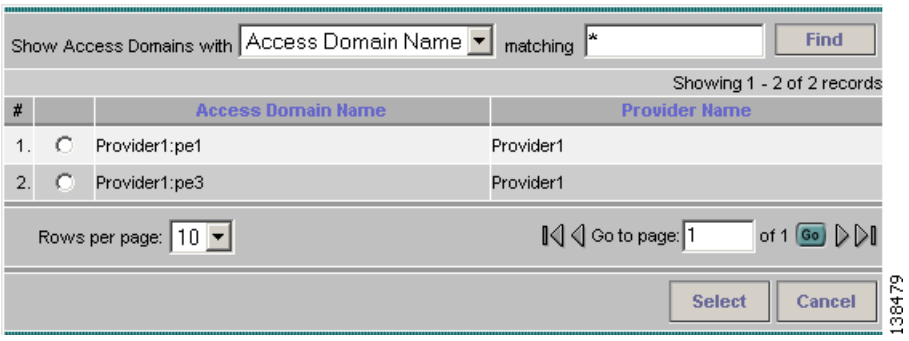
Step 7 Enter a VLAN Pool Size number.

Step 8 If the correct access domain is not showing in the Access Domain field, click **Select** to the right of Access Domain field.

The Access Domain for New VLAN Pool dialog box appears as shown in Figure 3-8.

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

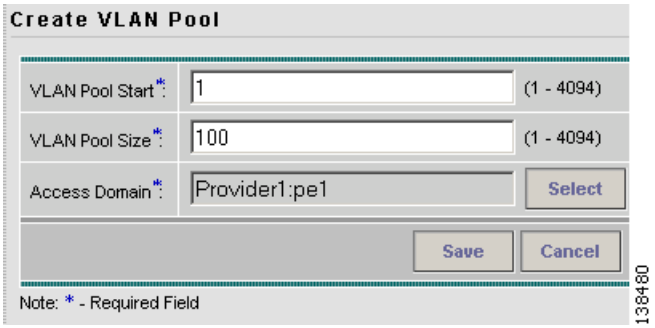
Figure 3-8 Access Domain for New VLAN Pool



a. Select an Access Domain Name by clicking the button in the Select column to the left of that Access Domain.

b. Click **Select**. The updated Create VLAN Pool window appears as shown in Figure 3-9.

Figure 3-9 Updated Create VLAN Pool



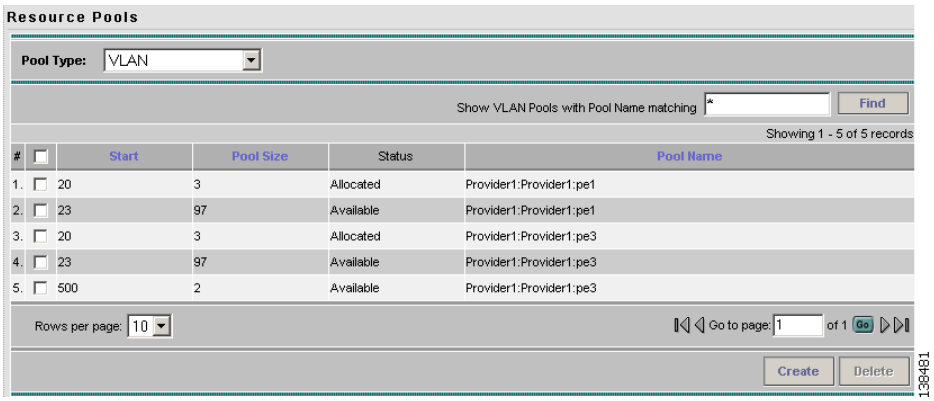
Step 9 Click **Save**.

The updated VLAN Resource Pools window appears as shown in Figure 3-10.

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

Note The Status field reads “Allocated” if you already filled in the Reserved VLANs information when you created the access domain. If you did not fill in the Reserved VLANs information when you created the access domain, the Status field reads “Available.” To allocate a VLAN pool, you must fill in the corresponding VLAN information by editing the access domain. (See Creating Access Domains, page 3-5.) The VLAN pool status automatically sets to “Allocated” on the Resource Pools window when you save your work.

Figure 3-10 Updated VLAN Resource Pools



Step 10 Repeat this procedure for each range you want to define within the VLAN.

Creating a VC ID Pool

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

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

Create one VC ID pool per network.

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

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

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

- The VC Pool start number
- The VC Pool size

Perform these steps for all L2VPN and VPLS services.

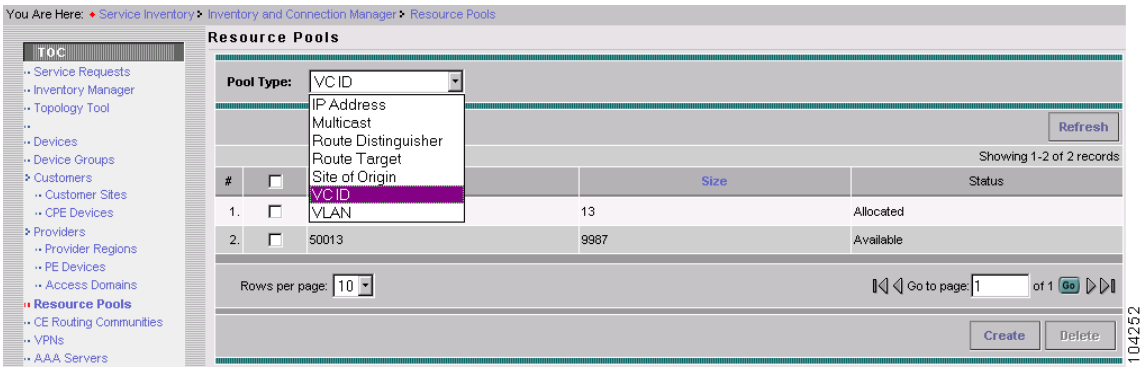
Step 1 Select **Service Inventory**.

Step 2 Select **Inventory and Connection Manager**.

Select **Resource Pools**. The Resource Pools window appears.

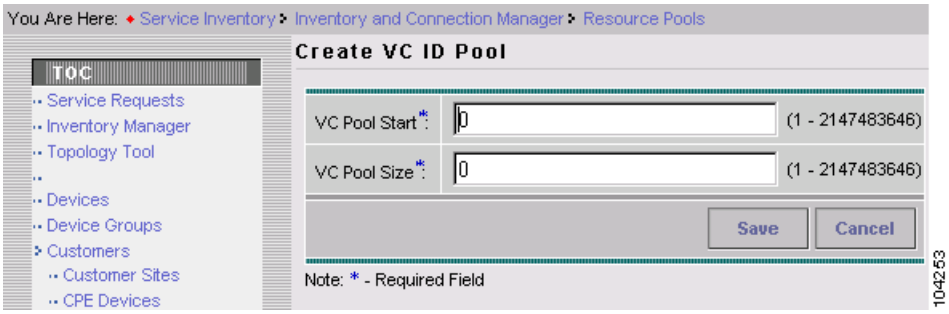
Step 3 Select **VC ID** from the drop-down **Pool Type** list as shown in Figure 3-11**.** Because this pool is a global pool, it is not associated with any other object.

Figure 3-11 VC ID Resource Pools



Step 4 Click **Create**. The Create VC ID Pool window appears as shown in Figure 3-12.

Figure 3-12 Create VC ID Pool

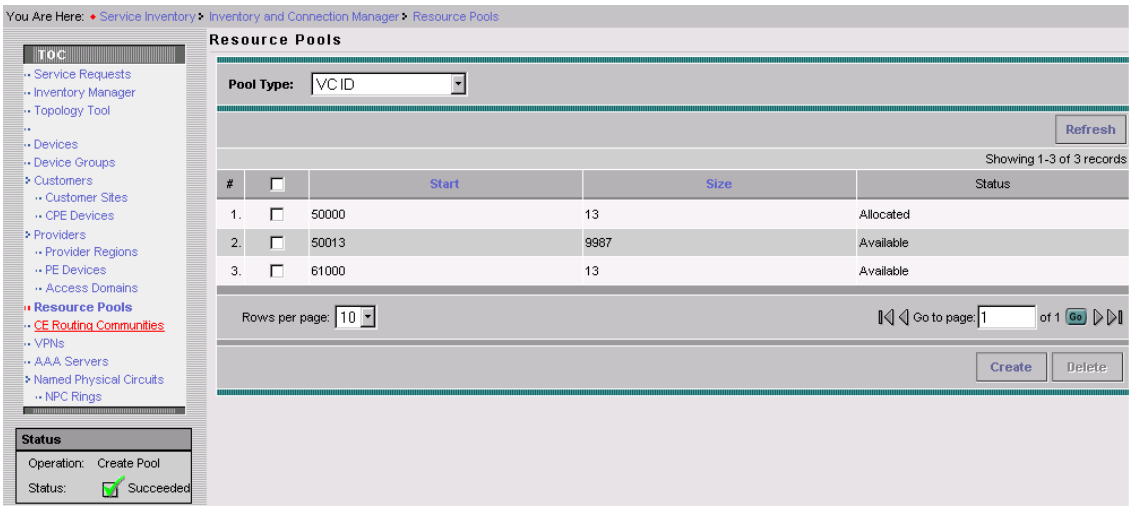


Step 5 Enter a VC pool start number.

Step 6 Enter a VC pool size number.

Step 7 Click **Save**. The updated VC ID Resource Pools window appears as shown in Figure 3-13.

Figure 3-13 Updated VC ID Resource Pools



Creating Named Physical Circuits

Before creating an L2VPN, L2TPv3, or VPLS service request, you must predefine the physical links between CEs and PEs. The Named Physical Circuit (NPC) represents a link going through a group of physical ports. Thus, more than one logical link can be provisioned on the same NPC; therefore, the NPC is defined once but used during several L2VPN or VPLS service request creations.

There are two ways to create the NPC links:

- Through an NPC GUI editor.
- Through the autodiscovery process.

An NPC definition must observe the following creation rules:

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

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

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

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

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

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

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

- Build the link that connects two ends:mlce1 and mlpe4 (as shown in Figure 3-25).
- Insert a device (enpe12) to the link you just made.
- Click **Insert Device** to insert the device.

Creating NPCs Through an NPC GUI Editor

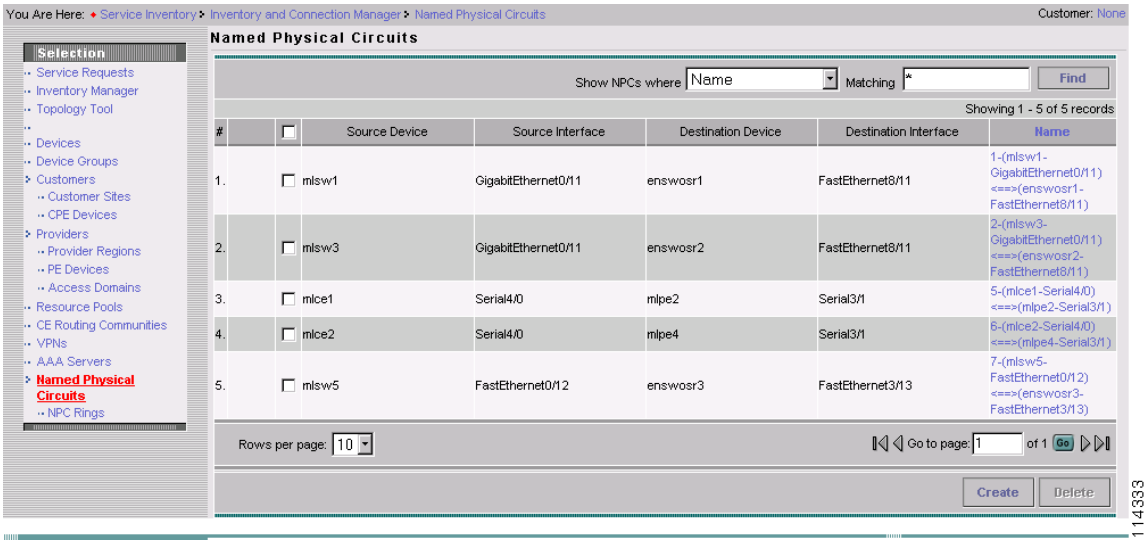
Perform the following steps to create NPCs through the NPC GUI editor.

Step 1 Select **Service Inventory**

Step 2 Select **Inventory and Connection Manager**

Step 3 Select **Named Physical Circuits**. The Named Physical Circuits window appears as shown in Figure 3-14.

Figure 3-14 Named Physical Circuit



To create a new NPC, you choose a CE as the beginning of the link and a N-PE as the end. If more than two devices are in a link, you can add or insert more devices (or a ring) to the NPC. Note that the new device or ring **added** is always placed after the device selected, while a new device or ring **inserted** is placed before the device selected.

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

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

Note Before adding or inserting a ring in an NPC, you must create a ring and save it in the repository. To obtain information on creating NPC rings, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

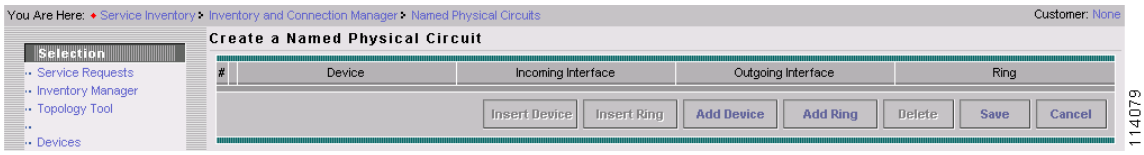
Source Device is the beginning of the link and **Destination Device** is the end of the link.

In the following example, there is a link with one end connecting a device called mlce1 on interface Ethernet0/0 and another link connecting to mlpe4 on interface FastEthernet0/0. Use the following steps to enter these devices.

Step 4 Click **Create**.

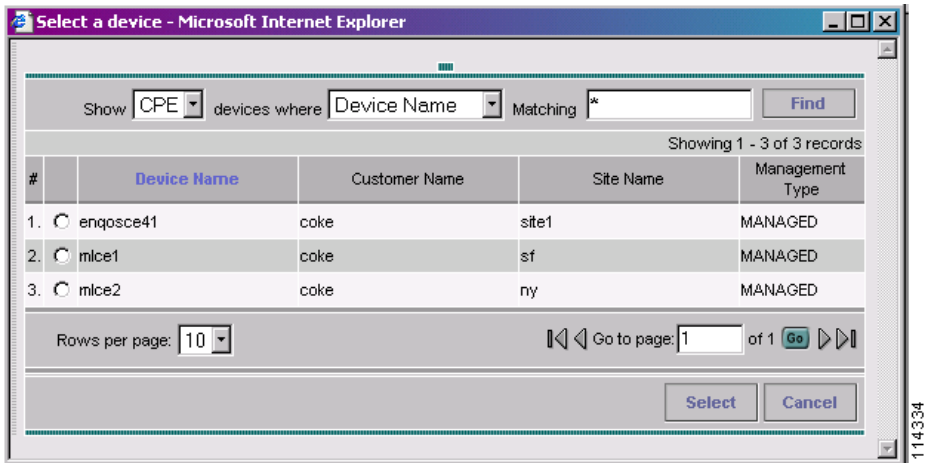
The Create a Named Physical Circuit window appears. See Figure 3-15.

Figure 3-15 Create a Named Physical Circuit



Step 5 Click **Add Device**. A list like the one in Figure 3-16 appears.

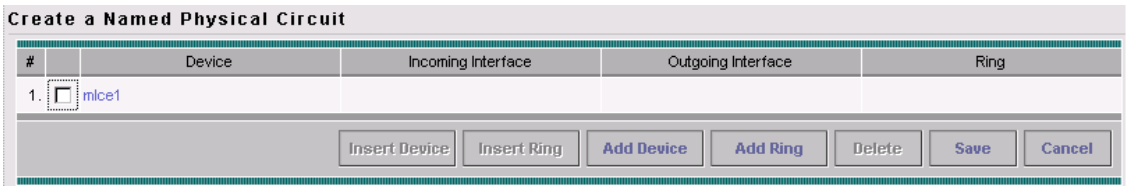
Figure 3-16 Choose a CPE



Step 6 Choose a CPE as the beginning of the link.

Step 7 Click **Select**. The device appears as shown in Figure 3-17.

Figure 3-17 Device Selected for NPC



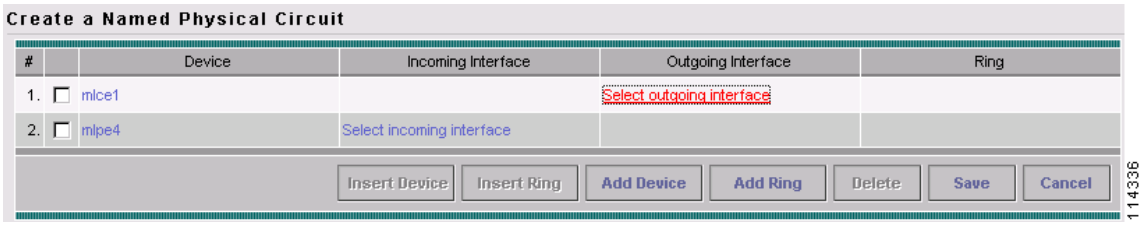
Step 8 To insert another device or a ring, click **Insert Device** or **Insert Ring**. To add another device or ring to the NPC, click **Add Device** or **Add Ring**.

For this example, click **Add Device** to add the N-PE.

Step 9 Choose a N-PE as the destination device.

Step 10 Click **Select**. The device appears as shown in Figure 3-18.

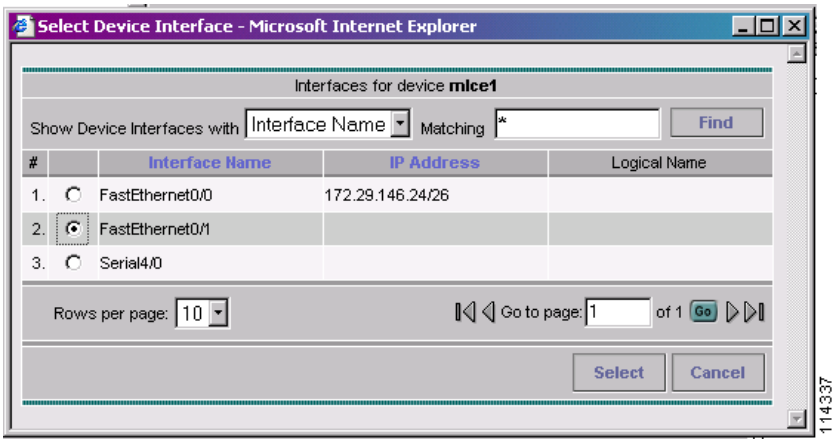
Figure 3-18 Second Device Selected for NPC



Step 11 In the Outgoing Interface column, click **Select outgoing interface**.

A list of interfaces, similar to the one in Figure 3-19, that were entered into the system appears.

Figure 3-19 Select Outgoing Interface

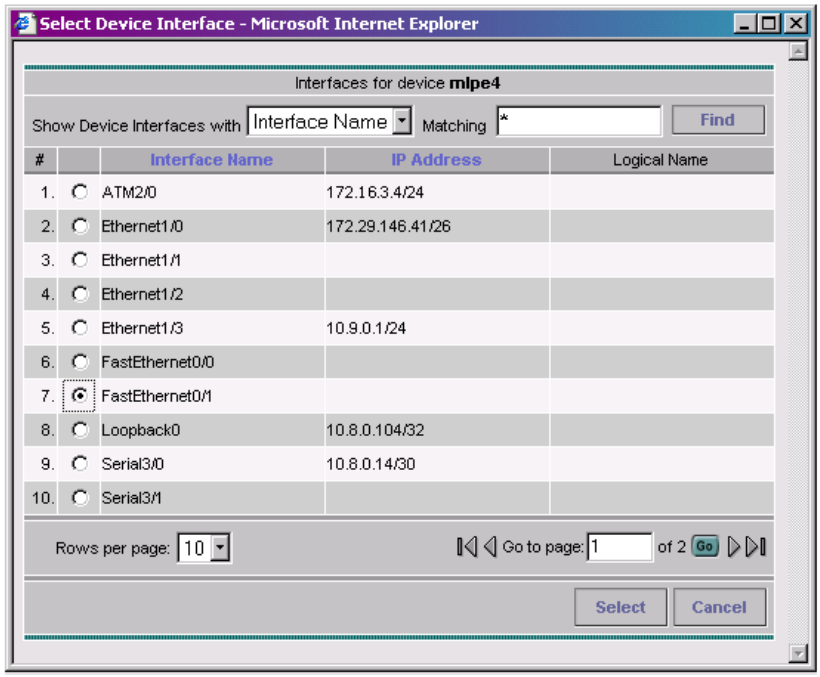


Step 12 Choose an interface from the list and click **Select**.

Step 13 In the Incoming Interface column, click **Select incoming interface**.

A list of interfaces, similar to the one in Figure 3-20, that were entered into the system appears.

Figure 3-20 Select Incoming Interface



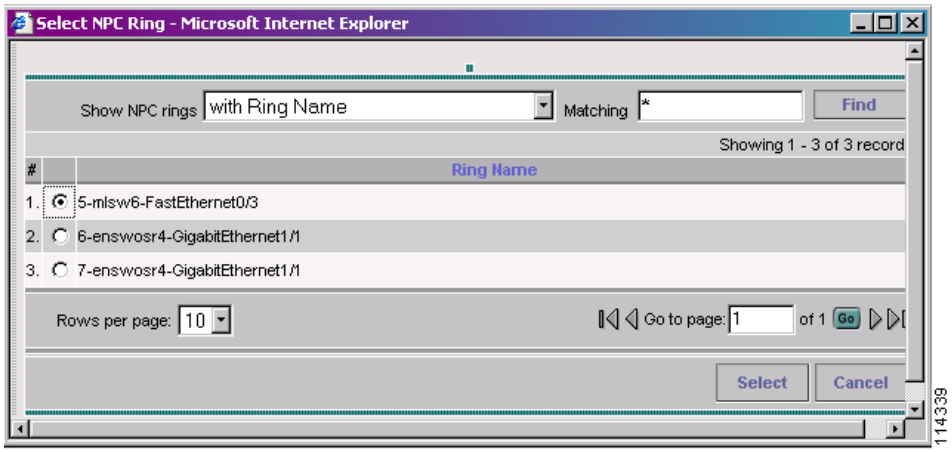
Step 14 Choose an interface from the list as the end of the link and click **Select**.

If you did not create a ring that you want to insert into the NPC, go to Step 25.

Step 15 If you created a ring to be used with the NPC, click **Add Ring** or **Insert Ring**. The Select NPC Ring window appears as shown in Figure 3-21.

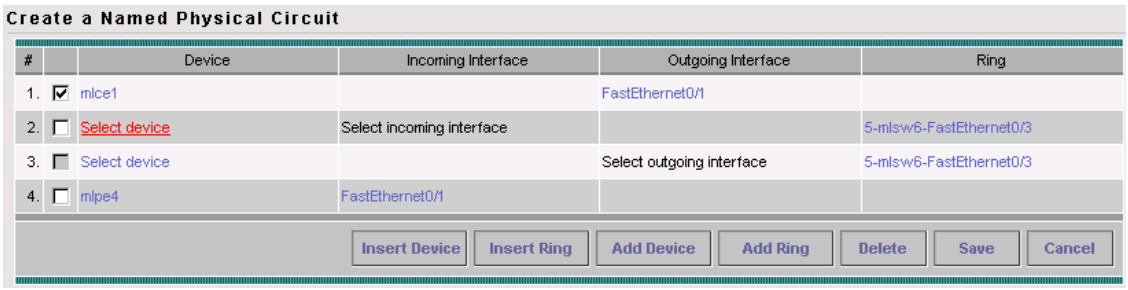
Note For L2TPv3, you cannot create rings.

Figure 3-21 Select NPC Ring



Step 16 Select a Ring Name and click **Select**. The Create a Named Physical Circuit window appears similar to the one in Figure 3-22.

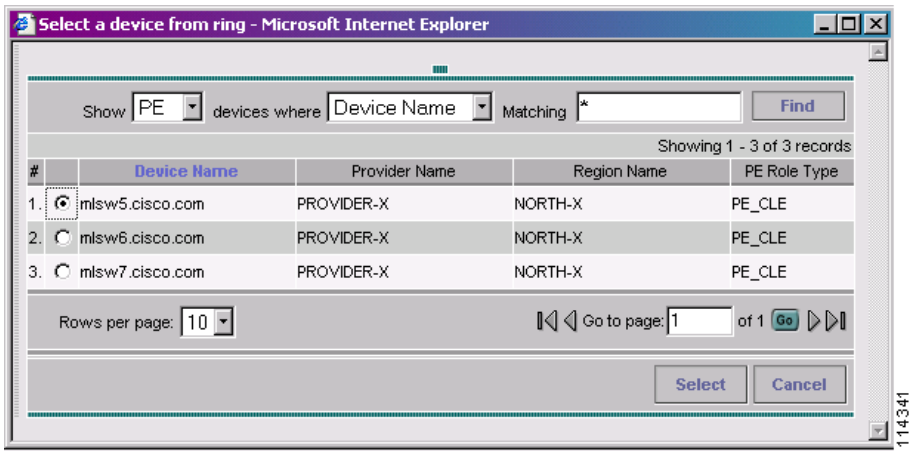
Figure 3-22 Create a Named Physical Circuit



Step 17 Click **Select device**.

Step 18 Select a Device from the ring to connect to mlce1 from a window like the one in Figure 3-23 and click **Select**.

Figure 3-23 Select a Device from the Ring



Step 19 Click **Select incoming interface**.

Step 20 Select the Interface and click **Select**.

Step 21 Click **Select device**.

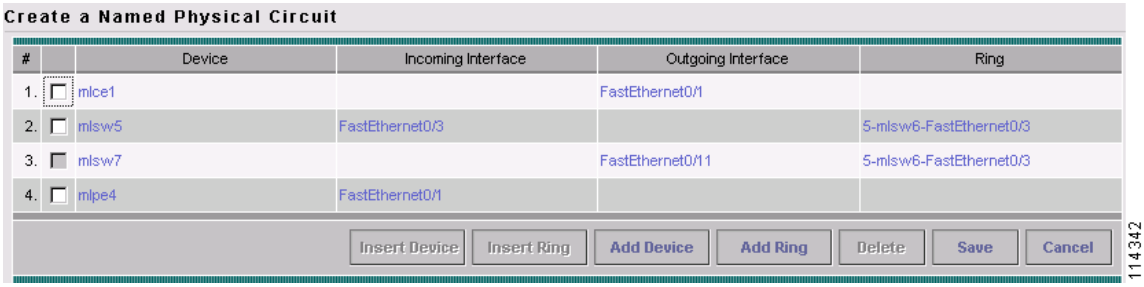
Step 22 Select a Device from the ring to connect to mlpe4 from a window like the one in Figure 3-23 and click **Select**.

Step 23 Click **Select outgoing interface**.

Step 24 Select the Interface and click **Select**.

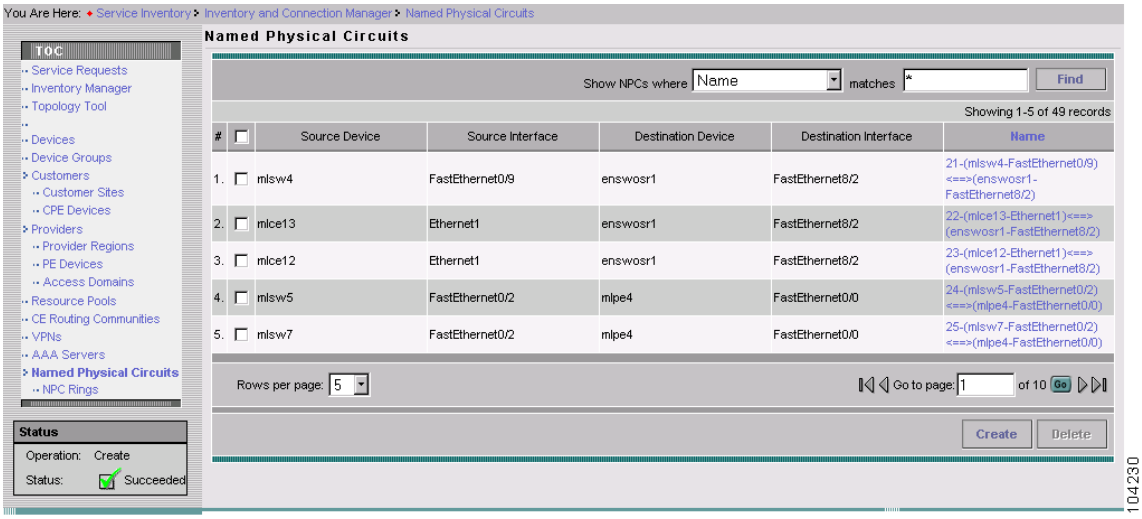
The NPC that includes the ring is now complete as shown in Figure 3-24.

Figure 3-24 Ring Complete



Step 25 Click **Save**. The Named Physical Circuits window now displays the NPC that you created as shown in Figure 3-25.

Figure 3-25 Created NPC



Creating a Ring-Only NPC

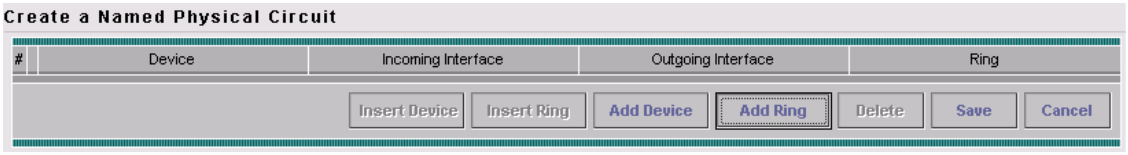
You can also create an NPC that contains only a ring without specifying CE.

Step 1 Select **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.

Step 2 Click **Create**.

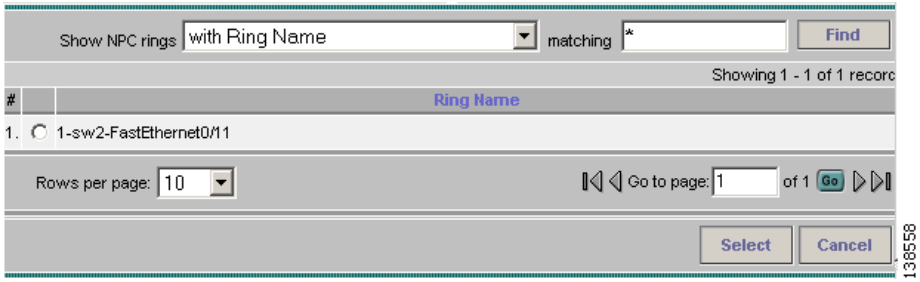
Step 3 The Create a Named Physical Circuit window appears, appears as shown in Figure 3-26.

Figure 3-26 Create an NPC that is a Ring



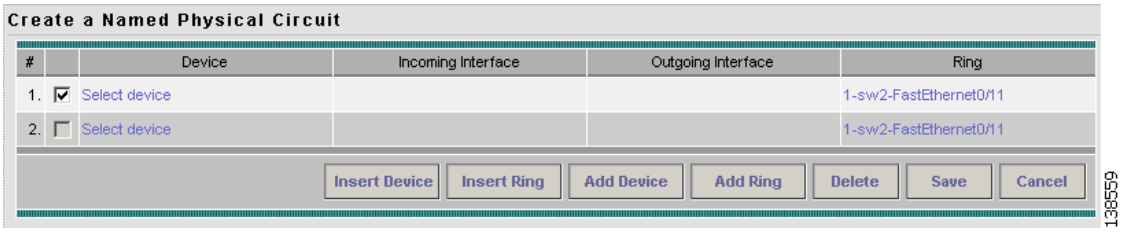
Step 4 Click **Add Ring**. The Select NPC Ring window (Figure 3-27) appears.

Figure 3-27 Select a Ring



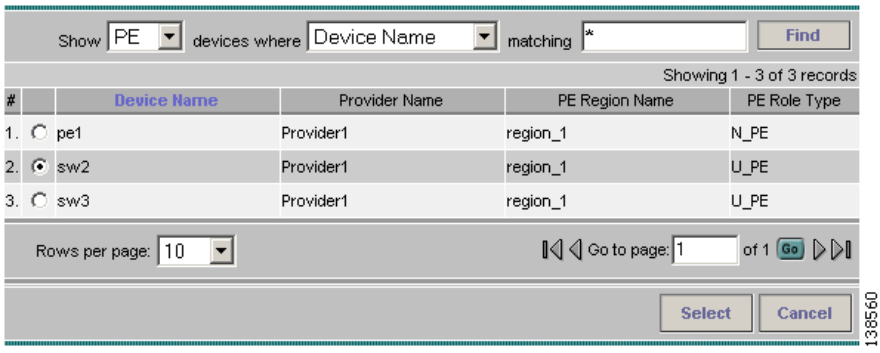
Step 5 Select a ring and click **Select**. The ring appears in a window like the one in Figure 3-28.

Figure 3-28 Select Device



Step 6 Click the **Select device** link to select the beginning of the ring. A window appears like the one in Figure 3-29, showing a list of devices.

Figure 3-29 Select the Beginning of the Ring



Step 7 Choose the device that is the beginning of the ring and click **Select**.

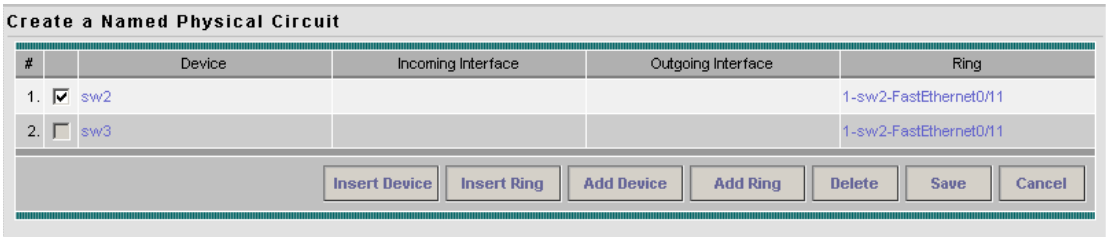
Step 8 Click the **Select device** link to choose the end of the ring.

Step 9 Choose the device that is the end of the ring and click **Select**.

Note The device that is the end of the ring in a ring-only NPC must be an N-PE.

Step 10 The Create a Named Physical Circuit window appears (Figure 3-30) showing the Ring-Only NPC.

Figure 3-30 Ring-Only NPC



Step 11 Click **Save** to save the NPC to the repository.

Creating NPC Links Through the Autodiscovery Process

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

For detailed steps to create NPCs using autodiscovery, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.