Provisioning Multiple Devices

This chapter describes how to configure multiple devices, Layer 2 (L2) “switches” and Layer 3 (L3) “routers,” using the IP Solution Center (ISC) provisioning process. This chapter contains the following major sections:

- NPC Ring Topology, page 12-1
- Ethernet-To-The-Home, page 12-9

NPC Ring Topology

This section describes how to create a Ring Topology, connect the CE starting and PE-POP ending points, and configure the Named Physical Circuits (NPC) from end to end, using the IP Solution Center (ISC) provisioning process.

This section contains the following sections:

- Ring Topology Overview, page 12-1
- Creating a Ring of Three PE-CLE, page 12-2
- Configuring NPC Ring Topology, page 12-4

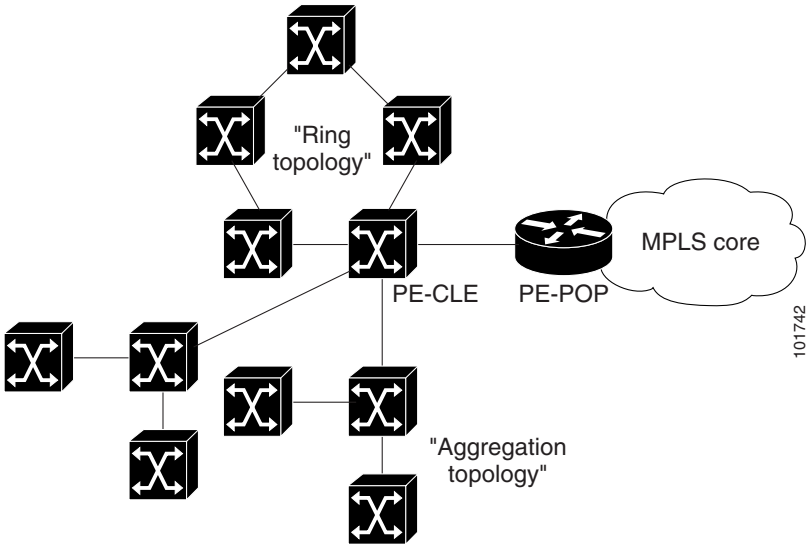
Ring Topology Overview

Service providers are now looking to offer L2 and L3 services that must integrate with a common MPLS infrastructure. ISC supports two basic L2 topologies to access L3 MPLS networks:

- Ring Topology
- Aggregation Topology (“Hub and Spoke”)

Figure 12-1 shows an example of these two basic L2 access topologies.

Figure 12-1 L2 Access Topologies

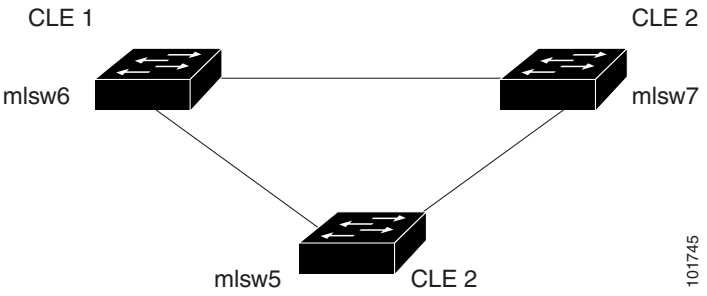


Creating a Ring of Three PE-CLE

In its simplest form, the Ring Topology is a tripartite structure that comprises at least three PE- CLE. A PE-POP and a Multi-VRF CE can also be part of a Ring.

Figure 12-2 shows an example ring of three Catalyst 3550 switches: mlsw5, mlsw6, and mlsw7.

Figure 12-2 A Ring of Three PE-CLE



To create a Ring Topology in ISC, follow these steps:

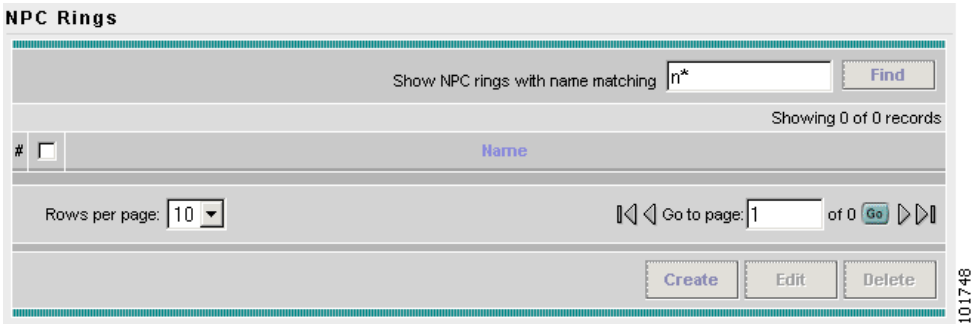
Step 1 Log in to ISC.

Step 2 Go to **Service Inventory > Inventory and Connection Manager**.

Step 3 Click **NPC Rings** in the TOC under **Named Physical Circuits**.

The NPC Rings window appears, as shown in Figure 12-3.

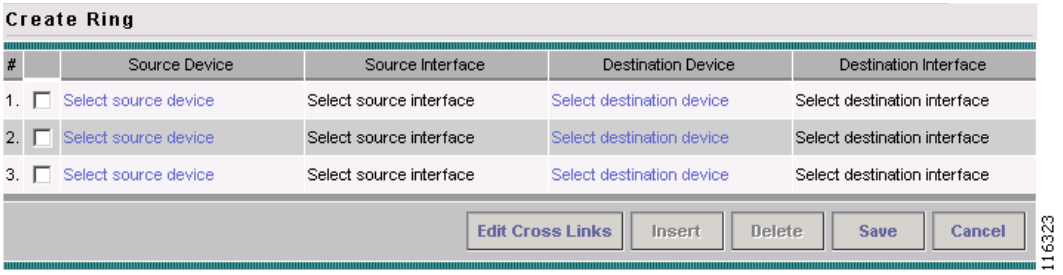
Figure 12-3 NPC Rings



Step 4 Click **Create** to continue.

The Create Ring window appears, as shown in Figure 12-4.

Figure 12-4 Create Ring

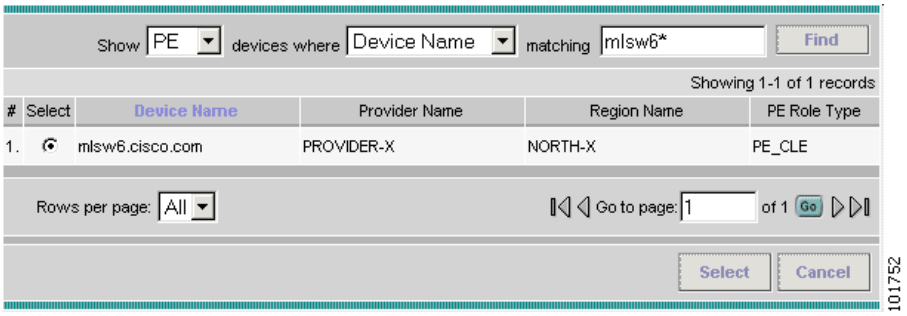


Step 5 Click **Select source device** in the first cell.

The Show Devices window appears, as shown in Figure 12-5.

Note The Show Devices drop-down window in Figure 12-5 should show *CLE* rather than *PE*. This is a known application error. You cannot initiate this process with a PE-POP or a CE. You must begin with a PE-CLE.

Figure 12-5 Show Devices

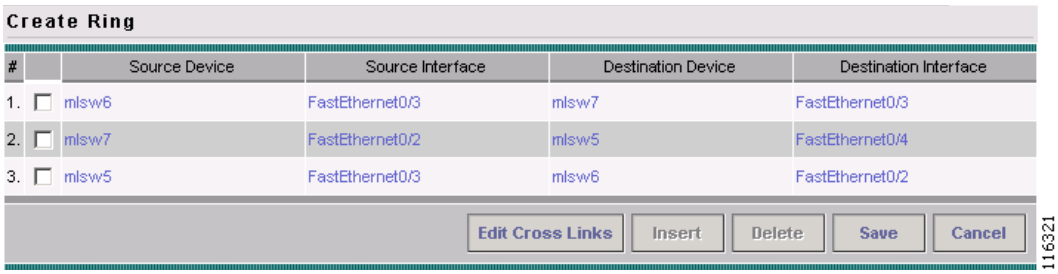


Step 6 To search for a specific CLE, enter the *source device* in the **matching** dialog-box and click **Find**.

Step 7 Choose the CLE and click **Select**.

The Create Ring window appears, as shown in Figure 12-6.

Figure 12-6 Create Ring



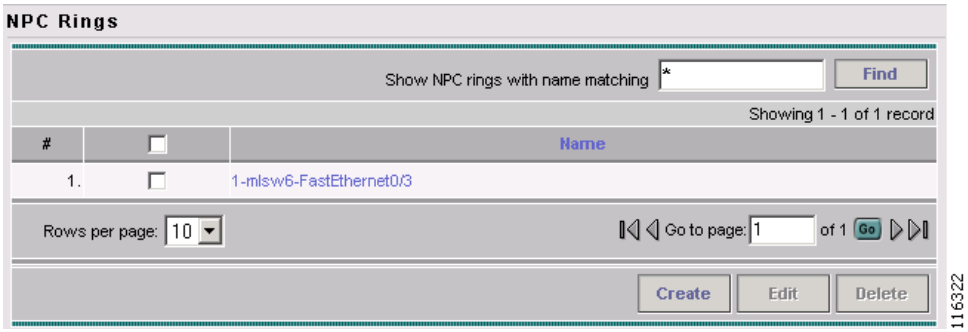
Step 8 Continue from left to right and from top to bottom to fill the table with the appropriate Device and Interface information, which would be based on a network diagram from your own environment.

Note If you had used the network diagram in Figure 12-8 to populate the Create Ring table, it would contain the above information at the end of this process.

Step 9 Click **Save** to save your ring in the Repository.

The NPC Rings window appears, as shown in Figure 12-7

Figure 12-7 NPC Rings

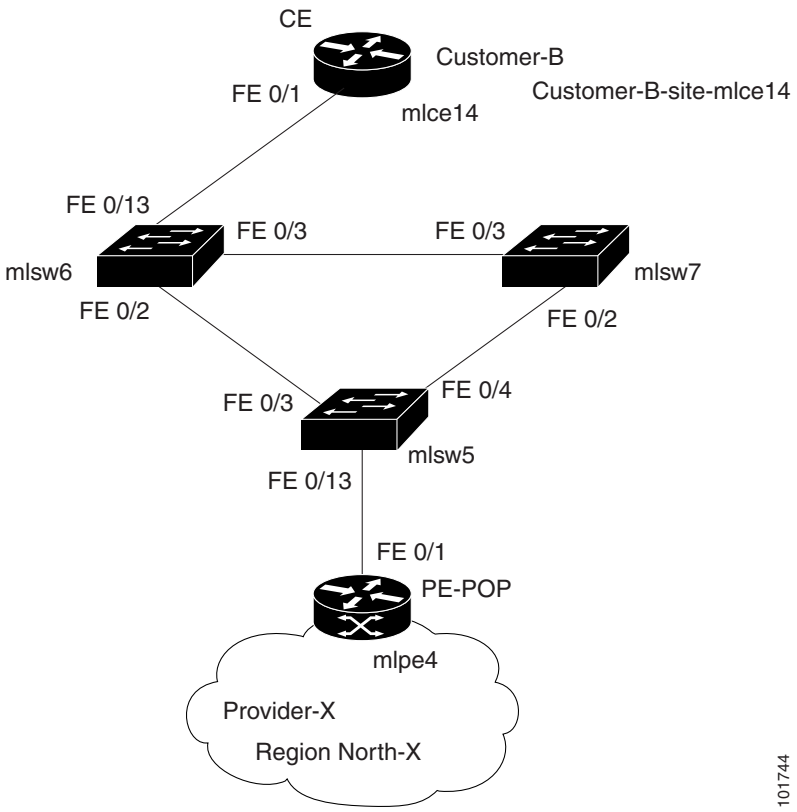


Proceed to Configuring NPC Ring Topology, page 12-4.

Configuring NPC Ring Topology

Figure 12-8 shows an example of the Ring Topology (three CLE) inserted between a CE (**mlce14**) and a PE-POP (**mlpe4**).

Figure 12-8 The Ring Topology



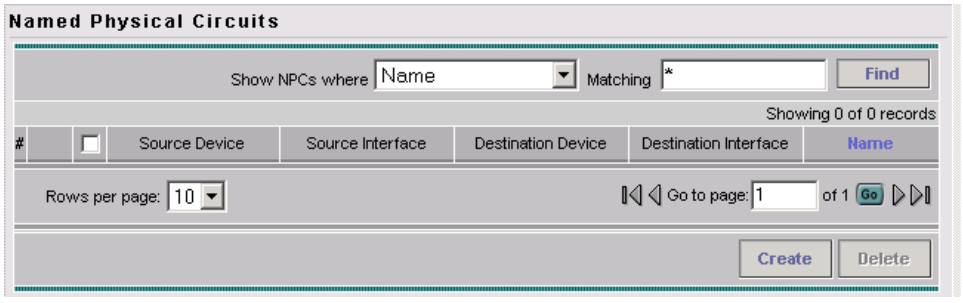
To configure end-to-end connectivity (CE > Ring (PE-CLE) > PE), follow these steps:

Step 1 Log in to ISC.

Step 2 Go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.

The Named Physical Circuits window appears, as shown in Figure 12-9.

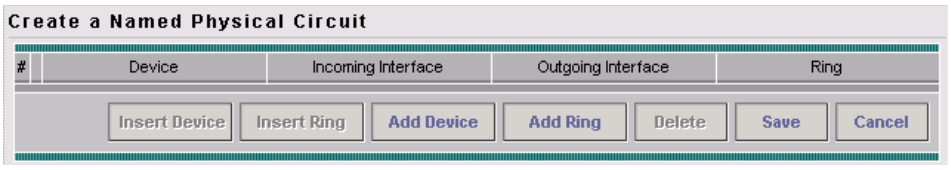
Figure 12-9 Named Physical Circuits



Step 3 Click **Create**.

The Create Named Physical Circuits window appears, as shown in Figure 12-10.

Figure 12-10 Create a Named Physical Circuit



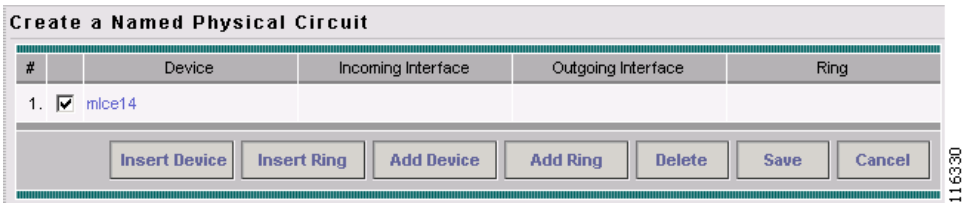
Step 4 Click **Add Device**.

The Select Devices window appears (not shown).

Step 5 Choose the CE and then click **Select**.

The Create a Named Physical Circuit window appears, as shown in Figure 12-11.

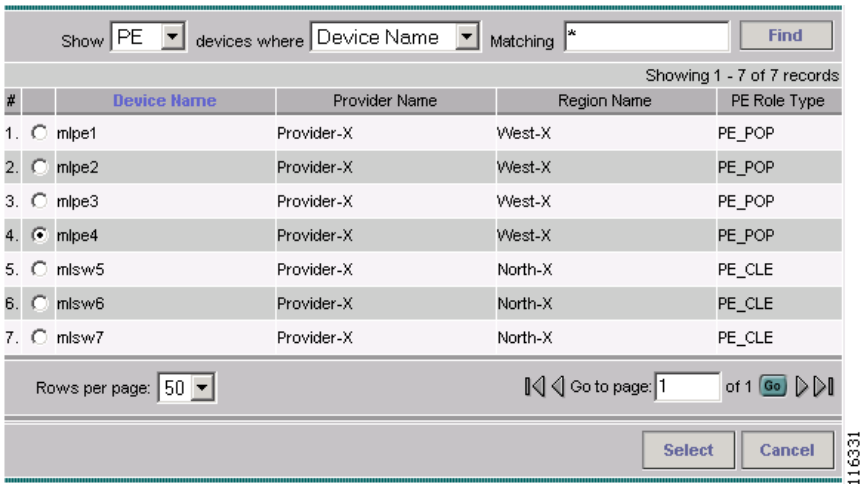
Figure 12-11 Create a Named Physical Circuit



Step 6 Click **Add Device**.

The Select Devices window appears, as shown in Figure 12-12.

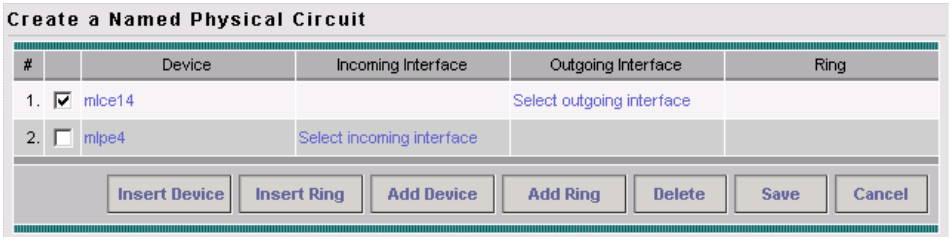
Figure 12-12 Choose Devices



Step 7 Choose the PE and then click **Select**.

The Create a Named Physical Circuit window appears, as shown in Figure 12-13.

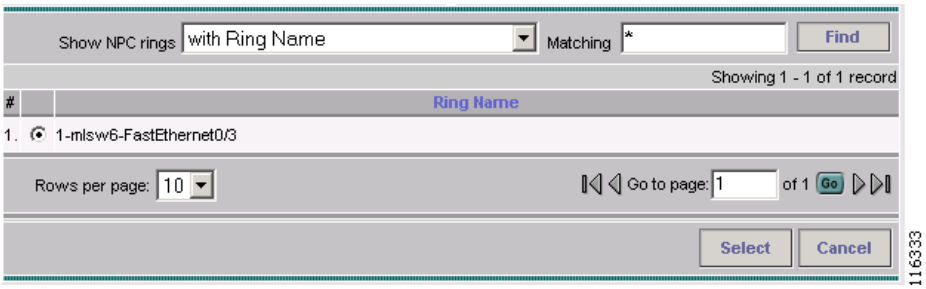
Figure 12-13 Create a Named Physical Circuit



Step 8 Click **Insert Ring**.

The Show NPC Rings window appears, as shown in Figure 12-14.

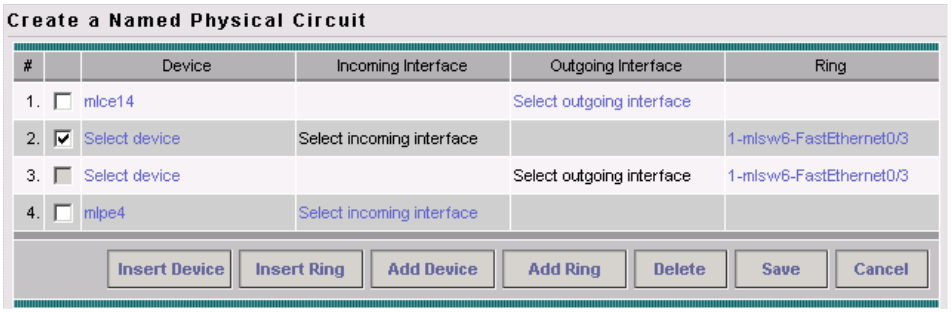
Figure 12-14 Create a Named Physical Circuit



Step 9 Choose an NPC Ring and click **Select**.

The Create a Named Physical Circuit window appears, as shown in Figure 12-15.

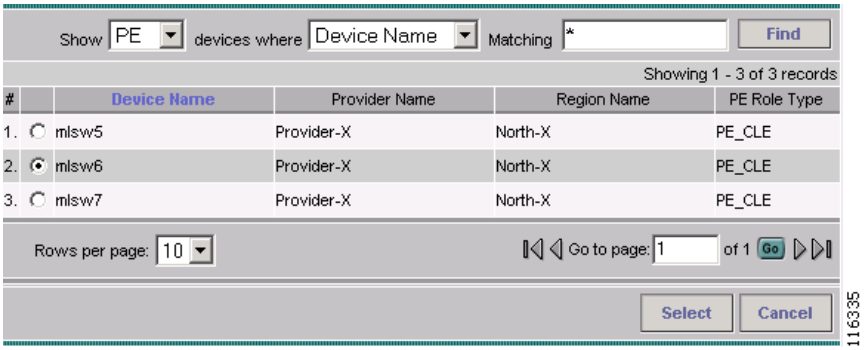
Figure 12-15 Create a Named Physical Circuit



Step 10 Choose a device with an available check box and click **Select device**.

The Show PE Devices window appears, as shown in Figure 12-16.

Figure 12-16 Show PE Devices



Step 11 Choose a PE-CLE and click **Select**.

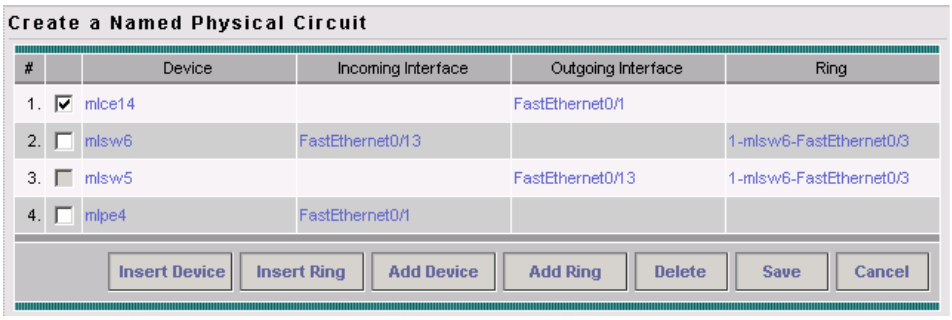
The Create a Named Physical Circuit window appears (not shown).

Step 12 Choose the incoming and outgoing interfaces for the CE, CLE, and PE until complete.

Step 13 Choose the remaining device with the darkened check box.

The Create a Named Physical Circuit window appears, as shown in Figure 12-17.

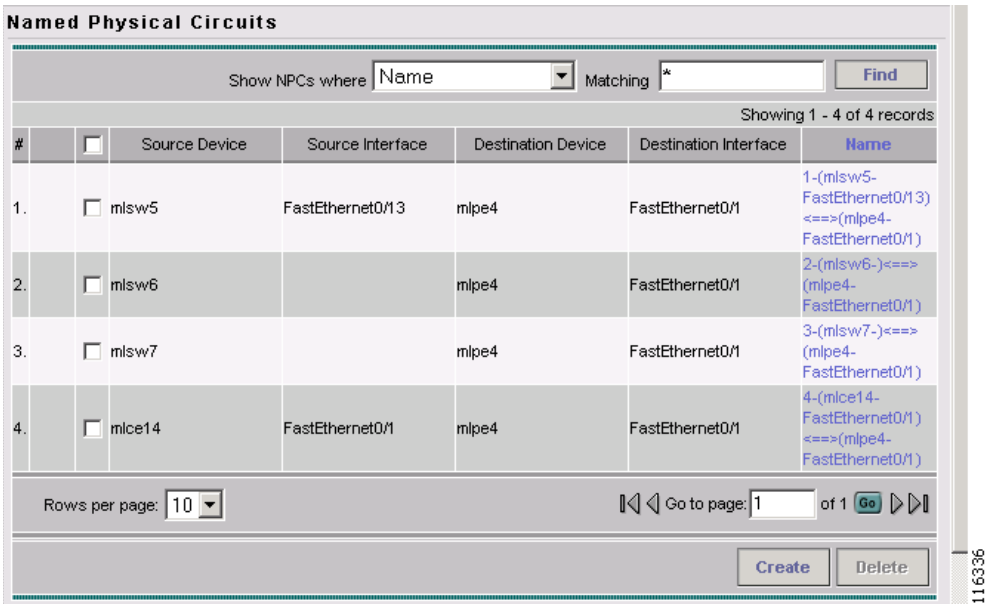
Figure 12-17 Create a Named Physical Circuit



Step 14 Click **Save**.

The Named Physical Interfaces window appears, with the Ring Topology displayed, as shown in Figure 12-18.

Figure 12-18 Named Physical Circuits



Ethernet-To-The-Home

This section describes how to configure Ethernet-To-The-Home (ETTH) using the IP Solution Center (ISC) provisioning process. This section contains the following sections:

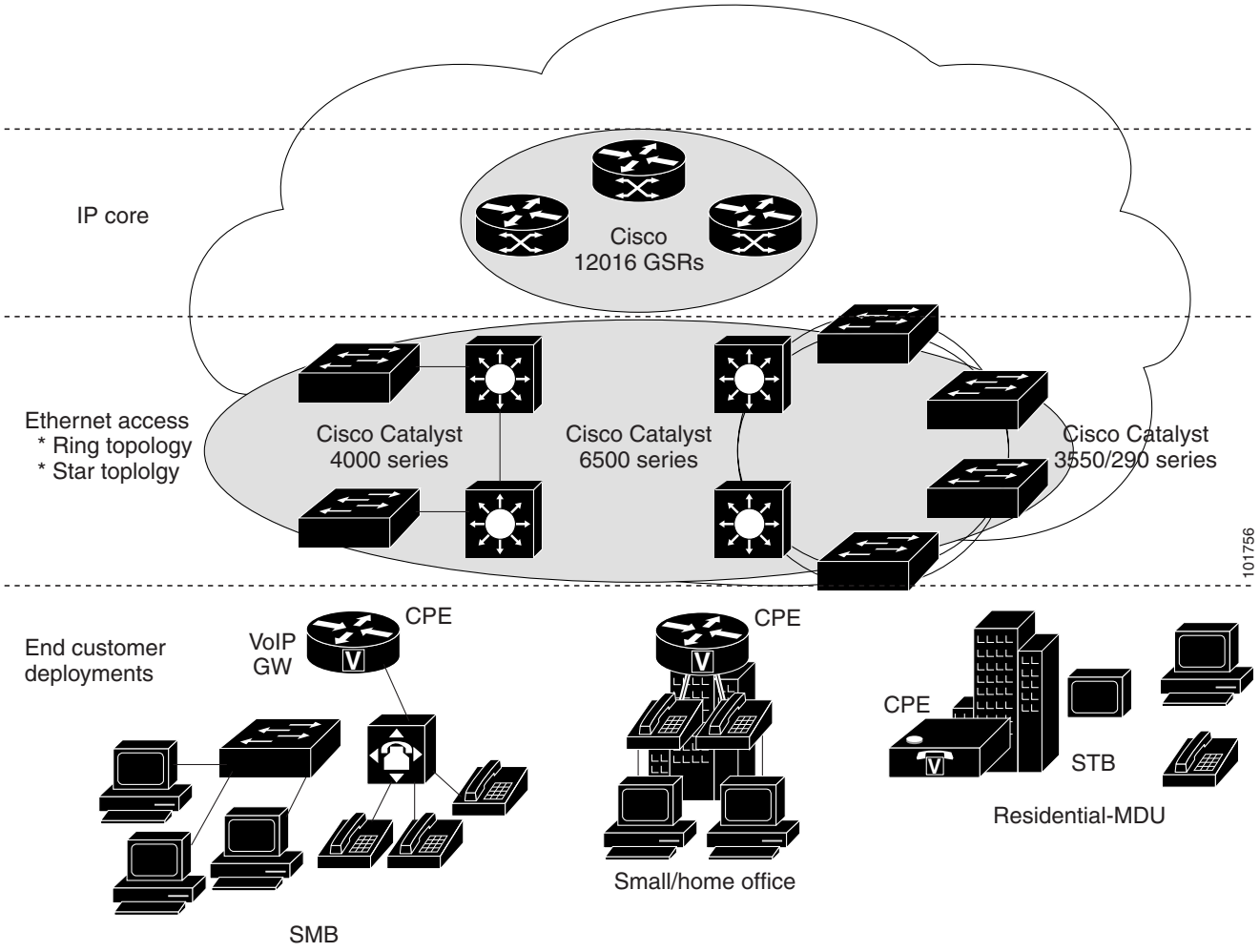
- ETTH Overview, page 12-9
- Configuring ETTH, page 12-11
- Residential Service, page 12-15

ETTH Overview

ETTH is part of the Cisco ETTx solution, which contains both ETTH and Ethernet-to-the-Business (ETTB). ETTB is supported in ISC with the L2VPN Metro Ethernet service feature. Unlike ETTB, whose customers are mainly business customers, ETTH is targeted at residential customers.

Figure 12-19 shows an overview of the Cisco ETTx solution.

Figure 12-19 Cisco ETTx Solution



From a provisioning standpoint, the main difference between ETTB and ETTH is the consideration of resource scalability. For example, with ETTB, each business customer is allocated one or more VLAN(s).

With ETTH, it is not practical to assign a unique VLAN to each residential customer. The practical solution is to have all, or a group of residential customers, share the same VLAN and use common technology, such as a private VLAN (PVLAN) or a protected port, to guarantee traffic isolation.

Another difference between ETTB and ETTH is that most of the ETTB customers use an Ethernet trunk port while ETTH customers use an access port. In ISC, the access port is fully supported, with CE present or with no CE.

ETTH needs to support multicast based services, such as video, on a shared media such as a ring. Typically, Internet Group Management Protocol (IGMP) with Multicast VLAN Registration (MVR) would be the technology used to support these services.

Access Domain Management

To provide more flexibility in managing an access domain, you can define a management VLAN. Once defined, the management VLAN is used to construct the list of VLANs allowed on the trunk port for all non-UNI ports.

You can also specify how the VLAN allowed list is constructed in a trunk port for a domain, if the list is not on the device. This feature is implemented for L2VPN DCPL parameter. It is available for Layer 2 access to MPLS VPN as well.

As a part of Layer 2 access management, ISC provides the ability to create MAC access lists by specifying the MAC addresses to be allowed or blocked.

ISC ETTH Implementation

The ISC MPLS VPN implementation of ETTH consists of the following three sub-features:

- PVLAN or Protected Port, page 12-11
- Access Port, page 12-11
- IGMP with MVR, page 12-11

PVLAN or Protected Port

This feature is used to isolate traffic within a PVLAN. It prevents traffic from flowing between two UNIs.

- PVLAN is only supported on the Catalyst 4500/6500 switches and Cisco 7600 router.
- Protected Port is only supported on the Catalyst 2950/3550 switches.

Access Port

In ISC, the untagged Ethernet default is supported in the CE present and no CE scenarios. You can choose between two encapsulations: Dot1q and Default.

The Default encapsulation only indicates that the traffic comes in from the CE is untagged. The UNI, which is always a Dot1q port, puts a tag on it before transmitting it. UNI has two options to handle this untagged traffic. It functions as an access port or a trunk port. For this reason, the GUI adds one more item for you to choose.

IGMP with MVR

This feature applies to a very specific user service and network topology. It is used for multicast video on a hub and spoke or ring network. However, it is not up to ISC to decide when it is used. ISC only makes it available and the network application running above ISC must invoke it when needed.

Configuring ETTH

To configure ETTH in ISC MPLS VPN, follow these steps:

Step 1 Log in to ISC.

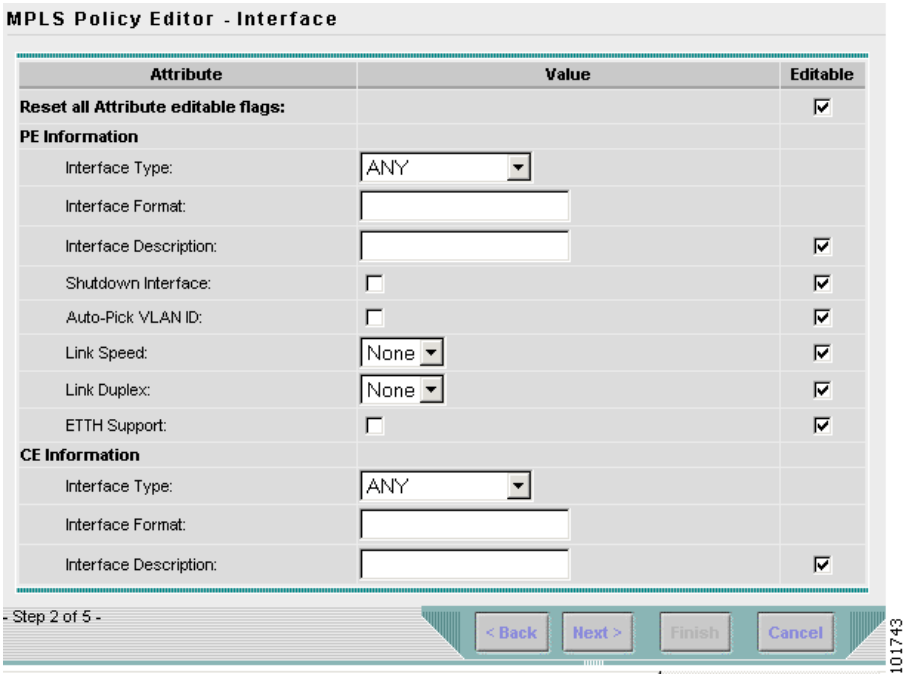
Step 2 Go to **Service Design > Policies**.

Step 3 From the Policies window, choose a Service Policy and click **Edit**.

Step 4 From the Policy Type window, click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in Figure 12-20.

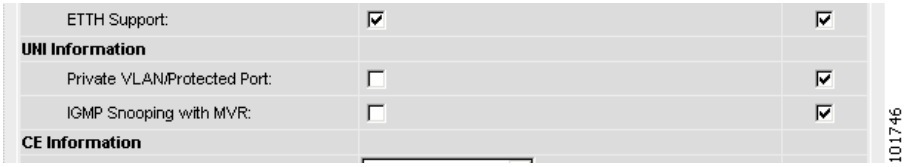
Figure 12-20 MPLS Policy Editor - Interface



Step 5 To enable ETTH, click the **ETTH Support** check box.

The ETTH UNI Information check boxes appear between the **ETTH Support** check box and the CE Information, as shown in Figure 12-21.

Figure 12-21 ETTH UNI Information

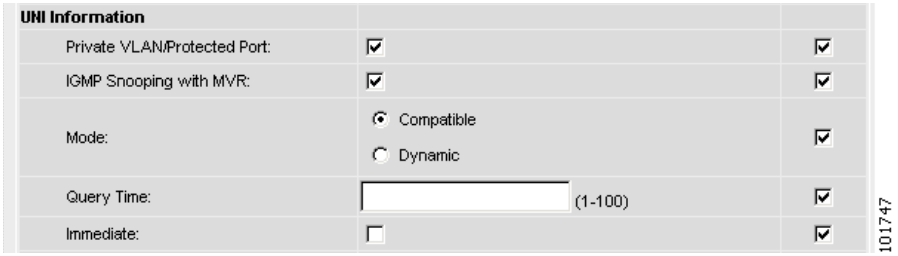


Step 6 To enable Private VLAN or Protected Port, click the **Private VLAN/Protected Port** check box.

Step 7 To enable IGMP Snooping with MVR, click the **IGMP Snooping with MVR** check box.

Three new UNI Information options appear, as shown in Figure 12-22.

Figure 12-22 ETTH UNI Information Options



Step 8 Choose UNI Information options:

- **Mode**
  - **Compatible**—Multicast addresses are statically configured on the device.
  - **Dynamic**—IGMP snooping is configured on the device.
- **Query Time**—Determines how often the device is queried for membership.
- **Immediate**—Removes the interface from the forwarding table immediately, when the session ends.

Step 9 Complete the standard steps and click **Save**.

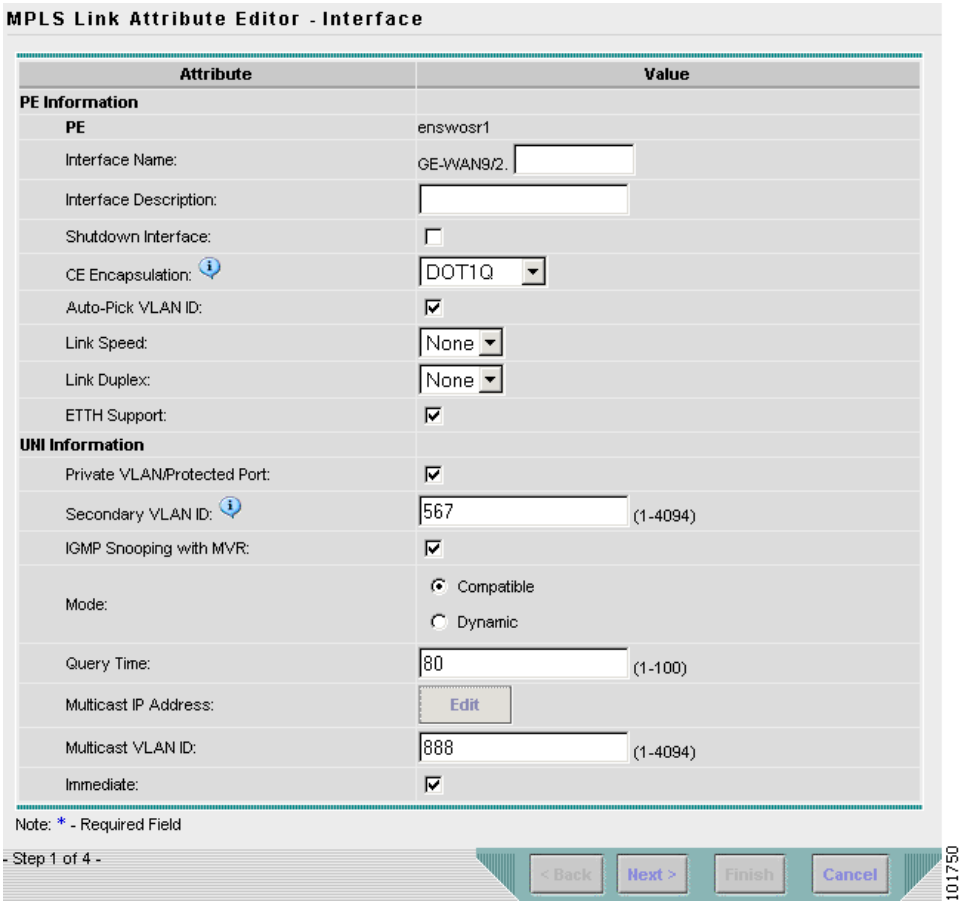
Step 10 Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

Step 11 From the Service Requests window, choose a Service Request and click **Edit**.

Step 12 From the MPLS Service Request Editor window, click the **Link Attribute** cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 12-23.

Figure 12-23 MPLS Link Attribute Editor - Interface



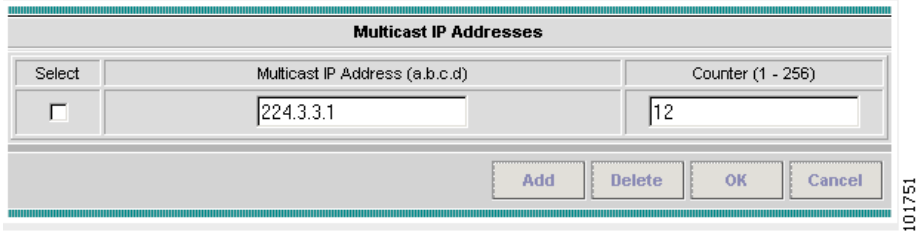
Step 13 Edit the following Link Attribute specific UNI Information:

- **Secondary VLAN ID**—Enter a *VLAN ID* for the Private VLAN, which is supported only on the Catalyst 4000 switch.
- **Multicast IP Address**—See Step 14.
- **Multicast VLAN ID**—Enter a *VLAN ID* for the Multicast VLAN.

Step 14 Click **EDIT**.

The Multicast IP Addresses dialog box appears, as shown in Figure 12-24.

Figure 12-24 Multicast IP Addresses



Step 15 Edit the following Link Attribute specific UNI Information:

- **Multicast IP Address**—Enter an *IP Address* for the join the multicast group, which allows users to have access to video on demand, for example.
- **Counter**—Enter a *count* to determine the number of contiguous IP addresses starting with the Multicast IP Address.

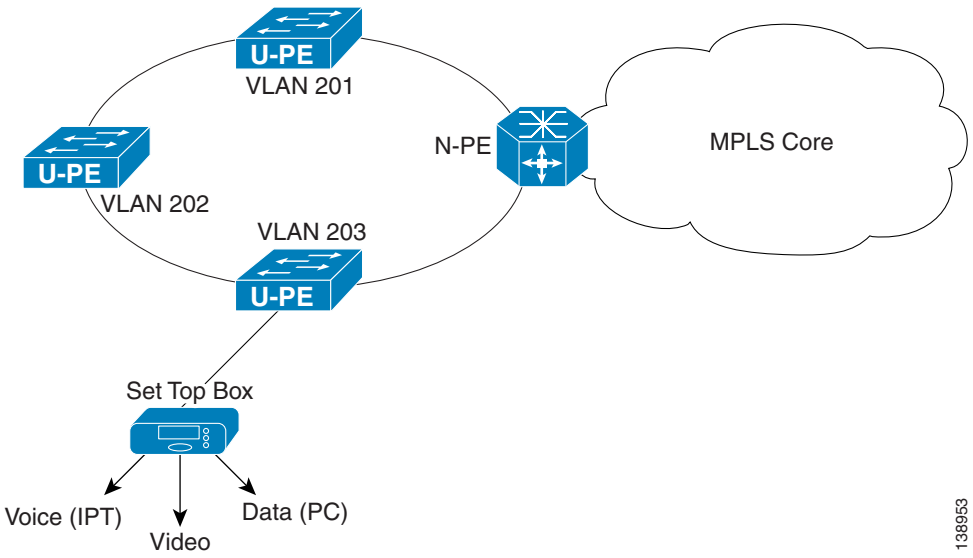
Step 16 Click **OK**.

Step 17 Complete the standard steps for creating an SR and click **Save**.

Residential Service

A group of residential customers can share the same VLAN on the same UNI switch with traffic isolation on different UNI interfaces. On an N-PE, a VRF SVI is defined for all the residential services from the same UNI switch (see Figure 12-25).

Figure 12-25 Residential Services



Policy for Residential Services Over Shared VLAN

A special policy must e created by enabling Shared VLAN.

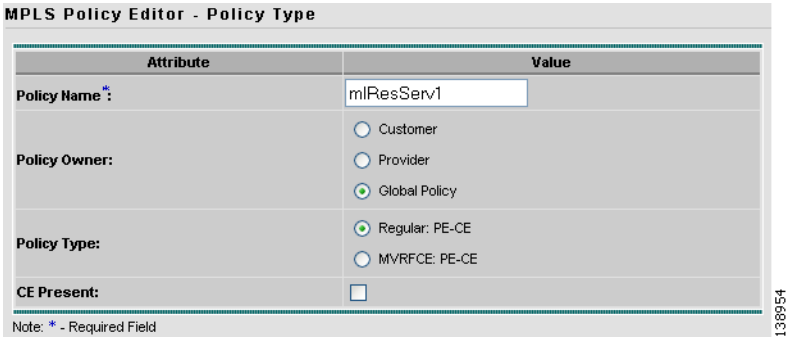
Step 1 Log in to ISC.

Step 2 Go to **Service Design > Policies**.

Step 3 From the Policies window, click **Create > MPLS Policy**.

The Policy Type window appears (see Figure 12-26).

Figure 12-26 Policy Type



Step 4 In the Policy Name field, enter a policy name.

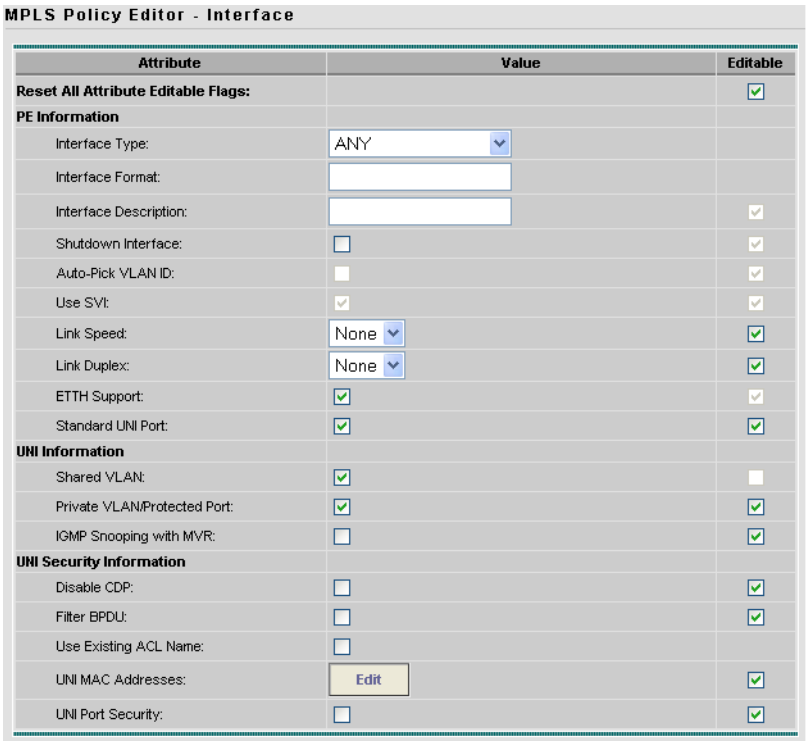
Step 5 Under Policy Owner, click the **Global Policy** radio button.

Step 6 Under Policy Type accept **Regular: PE-CE**.

Step 7 Under CE Present, uncheck the check box, then click **Next**.

The MPLS Policy Editor - Interface window appears (see Figure 12-27).

Figure 12-27 Interface Settings



Step 8 Check the **Use SVI:** check box, then wait for the screen to refresh.

Step 9 Check the **ETTH Support:** check box, then wait for the screen to refresh.

Step 10 Check the **Standard UNI Port:** check box, then wait for the screen to refresh.

Step 11 Check the **Shared VLAN:** check box, then wait for the screen to refresh.

Some fields are now grayed-out.

Note Because this policy enables ETTH Support and Shared VLAN, these attributes become unavailable at the link level.

Step 12 Check the **Private VLAN/Protected Port:** check box, wait for the screen to refresh, then click **Next**.

Step 13 In the IP Address Scheme window, you can continue by clicking **Next**.

Step 14 In the Routing Information window, you can continue by clicking **Next**.

Step 15 In the VRF and VPN Member window, you can finish creating this policy by clicking **Finish**.

Service Requests

Step 1 Log in to ISC.

Step 2 Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

Step 3 From the Service Requests window, click **Create > MPLS VPN**.

The Select MPLS Policy window appears.

Step 4 Choose the policy you configured for Shared VLAN Residential Services, then click **OK**.

The MPLS Service Request Editor window appears.

Step 5 In the MPLS Service Request Editor window, click **Add Link**, then wait for the window to refresh.

Step 6 Click the active field **Select U-PE**.

Step 7 Choose a PE device, then click **Select**.

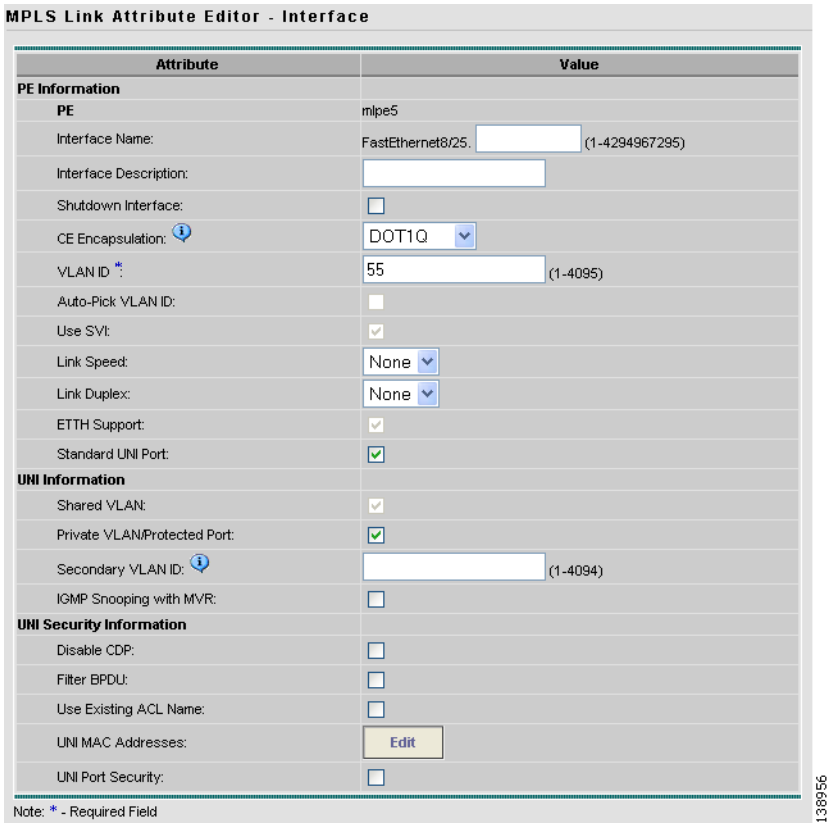
Step 8 From the active drop-down list, choose an interface, then wait for the window to refresh.

Step 9 Under Link Attributes column, click the active **Add** field.

The Interface window appears (see Figure 12-28).

Note Because the policy created for this feature enables ETTH Support and Shared VLAN, these attributes become unavailable at the link level.

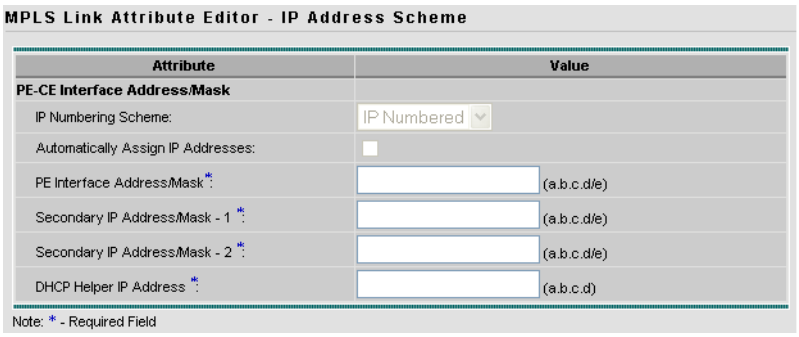
Figure 12-28 Interface Attributes



Step 10 Enter a valid **VLAN ID** value, then click **Next**.

The IP Address Scheme window appears (see Figure 12-29).

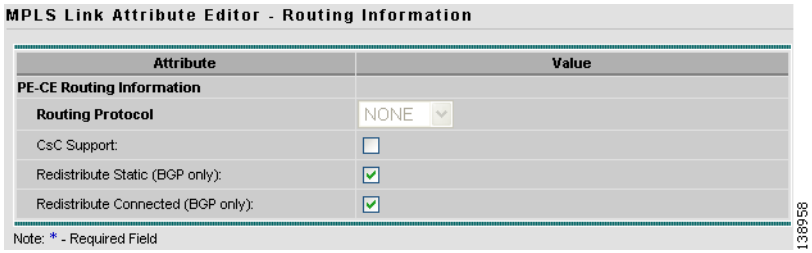
Figure 12-29 Entering IP Address Scheme



Step 11 Enter valid values for each required field, then click **Next**.

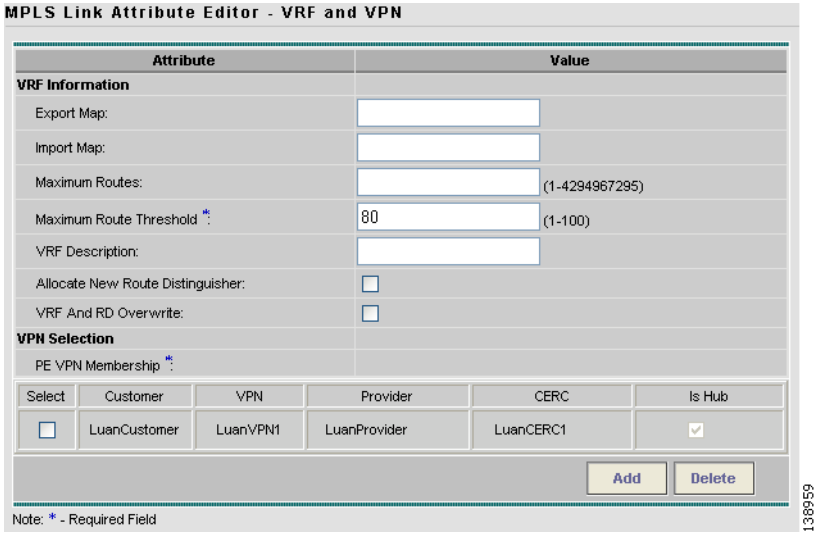
Step 12 In the Routing Information widow (see Figure 12-30), check any applicable items, then click **Next**.

Figure 12-30 Selecting Routing Information



Step 13 In the VRF and VPN window (see Figure 12-31), for Maximum Route Threshold (required field), accept the default value, or enter a new value.

Figure 12-31 Selecting VRF and VPN Attributes



Step 14 Under VPN Selection (required), click **Add**.

Step 15 From the CERC window, choose the desired PE VPN Membership, then click **Done**.

Step 16 Back in the VRF and VPN window, click **Finish**.

Step 17 To complete this task and save your changes, in the MPLS Service Request Editor window, click **Save**.