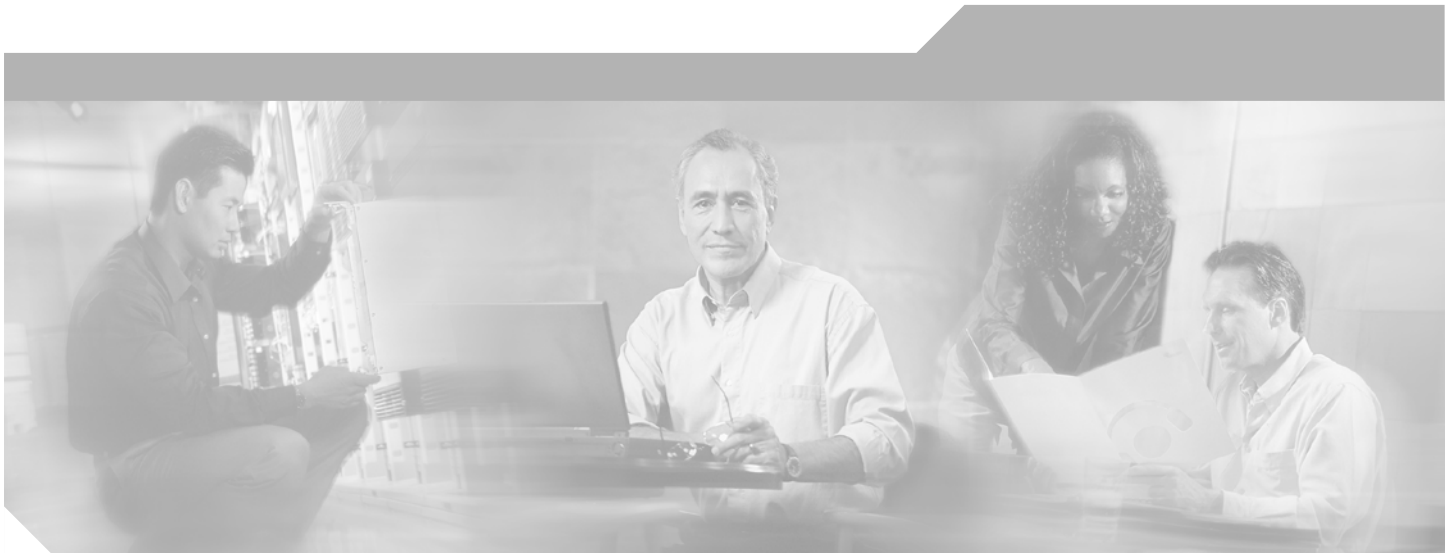


Cisco IP Solution Center L2VPN User Guide, 4.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7644-01

Cisco IP Solution Center L2VPN User Guide, 4.1

CONTENTS

About This Guide

This preface contains the following sections:

Audience

This guide is designed for service provider network managers and operators who are responsible for provisioning L2VPN or VPLS for their customers. Network managers and operators should be familiar with the following topics:

- Basic concepts and terminology used in internetworking.
- Layer 2 Virtual Private Network (L2VPN), Layer 2 Tunnel Protocol Version 3 (L2TPv3), Virtual Private LAN Service (VPLS), VPN, Multiprotocol Label Switching (MPLS), and terms and technology.
- Network topologies and protocols.

Purpose

Cisco IP Solution Center L2VPN User Guide, 4.1 contains information about creating an L2VPN, an L2TPv3, or a VPLS policy and about creating and deploying an L2VPN, L2TPv3, or VPLS service using an L2VPN, L2TPv3, or VPLS policy in the Cisco IP Solution Center (ISC). For additional information on related documentation, see Related Documentation, page xviii.

Organization

This guide is organized as follows:

- Chapter 1, "Getting Started with L2VPN" provides information on getting started tasks for using the L2VPN component of the Cisco IP Solution Center (ISC).
- Chapter 2, "ISC L2VPN and VPLS Concepts" provides an overview of the major concepts that structure the ISC L2VPN, L2TPv3, or VPLS service.
- Chapter 3, "Setting Up the ISC Service" provides information on setting up the ISC service.
- Chapter 4, "Creating an L2VPN Policy" provides information on creating an L2VPN policy
- Chapter 5, "Managing an L2VPN Service Request" provides information on creating an L2VPN service request, deploying L2VPN services, monitoring an L2VPN service, and saving an L2VPN service request.
- Chapter 6, "Creating an L2TPv3 Policy" provides information on creating an L2TPv3 policy.
- Chapter 7, "Managing an L2TPv3 Service Request" provides information on creating an L2TPv3 service request, deploying L2TPv3 services, monitoring an L2TPv3 service, and saving an L2TPv3 service request.
- Chapter 8, "Creating a VPLS Policy" provides information on creating a VPLS policy.
- Chapter 9, "Managing a VPLS Service Request" provides information on creating a VPLS service request, deploying VPLS services, monitoring an VPLS service, and saving a VPLS service requests.
- Chapter 10, "Using Autodiscovery for L2 Services" provides an overview of L2 service discovery.
- Chapter 11, "Generating L2 and VPLS Reports" provides information on how to set up, run, and format L2 and VPLS reports.
- Chapter 12, "Deploying, Monitoring and Auditing Service Requests" provides information on how to deploy, manage and audit service requests and how to access task logs.
- Appendix A, "Setting Up VLAN Translation" provides information on how to set up VLAN translation for L2VPN ERS services.
- Index

Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.1 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1

The following documents comprise the ISC 4.1 documentation set.

General documentation (in suggested reading order):

- *Cisco IP Solution Center Getting Started and Documentation Guide, 4.1*

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/docguide/index.htm
- *Release Notes for Cisco IP Solution Center, 4.1*

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/relnotes/index.htm
- *Cisco IP Solution Center Installation Guide, 4.1*

  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/install/index.htm

- *Cisco IP Solution Center Infrastructure Reference, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm
- *Cisco IP Solution Center System Error Messages, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mess/index.htm

Application and technology documentation (listed alphabetically):

- *Cisco IP Solution Center L2VPN User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/l2vpn/index.htm
- *Cisco IP Solution Center MPLS VPN User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mpls/index.htm
- *Cisco IP Solution Center Quality of Service User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/qos/index.htm
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/tem/index.htm
- *Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/trble/index.htm

API Documentation:

- *Cisco IP Solution Center API Programmer Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_gd/index.htm
- Index: *Cisco IP Solution Center API Programmer Reference, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_ref/index.htm

Note All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Getting Started with L2VPN

This chapter provides a road map to help you get started using the L2VPN component in ISC 4.1. It contains the following sections:

Overview

Before you can use the L2VPN component to provision Layer 2 services (L2VPN or VPLS), you must complete several installation and configuration steps, as outlined in this chapter. In addition, you should be familiar with basic concepts for ISC and L2VPN (or VPLS) services. The following sections provide a summary of the key tasks you must accomplish to be able to provision L2VPN or VPLS services using ISC. You can use the information provided below as a checklist. Where appropriate, references to other sections in this manual or to other manuals in the ISC documentation set are provided. See the referenced documentation for more detailed information. After the basic installation and configuration steps are completed for both ISC and the L2VPN component, you can refer to the subsequent chapters of this manual to create and provision L2VPN or VPLS services.

Installing ISC and Configuring the Network

Before you can use the L2VPN module in ISC to provision L2VPN or VPLS services, you must first install ISC and do the basic network configuration required to support ISC. Details on these steps are provided in *Cisco IP Solution Center Installation Guide, 4.1*. Refer to that manual for information about ISC installation and general network configuration requirements.

Note To use the L2VPN component within ISC, you must purchase and activate the L2VPN license.

Configuring the Network to Support Layer 2 Services

In additional to basic network configuration required for ISC, you must perform the following network configuration steps to support Layer 2 services. Information on doing these steps is not provided in the ISC documentation. See the documentation for your devices for information on how to perform these steps.

Step 1 Enable MPLS on the core-facing interfaces of the N-PE devices attached to the provider core.

Step 2 Set up /32 loopback addresses on N-PE devices. These loopback addresses should be the termination of the LDP connection(s).

Step 3 Set all L2 devices (switches) to VTP transparent mode. This is so that none of the switches will operate as VLAN servers. This will prevent VLAN information from automatically propagating through the network.

Setting Up Basic ISC Services

After the basic network configuration tasks are completed to support ISC and L2 services, you use ISC to define elements in the ISC repository, such as providers and regions, customers and sites, devices, VLAN and VC pools, NPCs, and other resources that are necessary to provision L2 services. Detailed steps to perform general ISC tasks are covered in *Cisco IP Solution Center Infrastructure Reference, 4.1*. You can also find a summary of some important ISC set up tasks in this manual in Chapter 3, "Setting Up the ISC Service." The information below is a checklist of basic ISC services you must set up before provisioning L2 services.

Setting Up Providers, Customers, and Devices

Perform the following steps to set up providers, customers and devices in the ISC repository. These are global resources that can be used by all ISC services.

Step 1 **Set up service providers and regions.** The region is important because a single provider could have multiple networks. The region is used as a further level of differentiation to allow for such circumstances. To create a provider and a region, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining a Service Provider and Its Regions, page 3-3.

Step 2 **Set up customers and customer sites.** 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 CEs. For detailed steps to create customers and sites, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining Customers and Their Sites, page 3-4.

Step 3 **Import or add raw devices.** Every network element that ISC manages must be defined as a device in the ISC repository. An element is any device from which ISC can collect information. In most cases, devices are Cisco IOS routers and switches. You can set up devices in ISC manually, through autodiscovery, or through importing device configuration files. For detailed steps to importing and adding devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Chapter 10, "Using Autodiscovery for L2 Services."

Step 4 **Assign devices roles as PE or CE.** After devices are created in ISC, must define them as customer (CE) or provider (PE) devices. You do this by editing the device attributes on individual devices or in batch editing through the ISC inventory manager. To set device attributes, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Setting Up the N-PE Loopback Address

Within ISC, you must set the loopback address on the N-PE device(s). For details about this procedure, see Setting the Loopback Address, page 3-2.

Setting Up ISC Resources for L2VPN and VPLS Services

Some ISC resources, such as access domains, VLAN pools and VC pools are set up to support ISC L2VPN and VPLS services only. Perform the following steps to set up these resources.

Step 1 **Create access domain(s).** 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. 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. For detailed steps to create access domains, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating Access Domains, page 3-5.

Step 2 **Create a VLAN pool(s).** A VLAN pool is created for each access domain. 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. For detailed steps to create VLAN pools, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating VLAN Pools, page 3-6.

Step 3 **Create VC pool(s).**VCID 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). Create one VC ID pool per network. For detailed steps to create VC pools, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating a VC ID Pool, page 3-9.

Setting Up NPCs

Before creating an L2VPN or VPLS service request, you must predefine the physical links between CEs and PEs or between U-PEs and N-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 by several L2VPN or VPLS service requests. For detailed steps to create NPCs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Creating Named Physical Circuits, page 3-11.

Setting Up VPNs

You must define VPNs before provisioning L2VPN or VPLS services. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance. To define VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*. See also Defining VPNs, page 3-4.

Working with L2VPN and VPLS Policies and Service Requests

After you have set up providers, customers, devices and resources in ISC, you are ready to create L2VPN or VPLS policies, provision service requests (SRs), and deploy the services. After the service requests are deployed you can monitor, audit and run reports on them. All of these tasks are covered in the *Cisco IP Solution Center L2VPN User Guide, 4.1* (this manual). Perform the following steps to accomplish these tasks.

Step 1 **Review overview information about L2 services concepts.** See Chapter 2, "ISC L2VPN and VPLS Concepts."

Step 2 **Set up a L2VPN or VPLS policy.** See the appropriate chapter, depending on the type of policy you want to create:

- Chapter 4, "Creating an L2VPN Policy."
- Chapter 6, "Creating an L2TPv3 Policy."
- Chapter 8, "Creating a VPLS Policy."

Step 3 **Provision the L2VPN or VPLS service request.** See the appropriate chapter, depending on the type service request you want to provision:

- Chapter 5, "Managing an L2VPN Service Request."
- Chapter 7, "Managing an L2TPv3 Service Request."
- Chapter 9, "Managing a VPLS Service Request."

Step 4 **Deploy the service request.** See Chapter 12, "Deploying, Monitoring and Auditing Service Requests."

Step 5 **Check the status of deployed services.** You can use one or more of the following methods:

- Monitor service requests. See to Chapter 12, "Deploying, Monitoring and Auditing Service Requests."
- Audit service requests. See to Chapter 12, "Deploying, Monitoring and Auditing Service Requests."
- Run L2 and VPLS reports. See to Chapter 11, "Generating L2 and VPLS Reports."

ISC L2VPN and VPLS Concepts

This chapter provides an overview of ISC L2VPN and VPLS service provisioning. It contains the following sections.

Overview

Layer 2 service provisioning for the IP Solution Center (ISC) 4.0 consists of the Layer 2 Virtual Private Network (L2VPN) Service and the Virtual Private LAN Service (VPLS).

L2VPN Services

L2VPN services are point-to-point. They provide Layer 2 point-to-point connectivity over either an MPLS or a pure IP (L2TPv3) core. These implementations, in turn, support service types, as follows:

- L2VPN over MPLS core:
  - Ethernet Wire Service (EWS)
  - Ethernet Relay Service (ERS)
  - ATM over MPLS (ATMoMPLS)
  - Frame Relay over MPLS (FRoMPLS)
- L2VPN over IP (L2TPv3) core:
  - ATM
  - Frame Relay

VPLS Services

VPLS services are multipoint. They provide multipoint connectivity over an MPLS or an Ethernet core. These implementations, in turn, support service types, as follows:

- VPLS over MPLS core:
  - Ethernet Wire Service (EWS). This is also sometimes referred to as EMS, or Ethernet Multipoint Service.
  - Ethernet Relay Service (ERS). This is also sometimes referred to ERMS, or Ethernet Relay Mulipoint Service.
- VPLS over Ethernet core:
  - Ethernet Wire Service (EWS)
  - Ethernet Relay Service (ERS).

The remaining sections of this chapter provide an overview of these services. Instructions on creating policies and service requests for these services are provided in subsequent chapters of the manual.

L2VPN Service Provisioning

This section provides and overview of ISC provisioning for L2VPN over both MPLS and IP (L2TPv3) infrastructures. It contain the following sections:

Any Transport over MPLS (AToM)

Cisco's Any Transport over MPLS (AToM) enables service providers to deliver profitable, comprehensive services to their customers. The L2VPN service provisioning available in ISC is in the following areas:

Point-to-Point Ethernet (EWS and ERS)

The EWS and ERS services are delivered with the Cisco Metro Ethernet offering. The same network architecture can simultaneously provide both ERS and EWS connections to diverse customers. Additionally, this Metro Ethernet infrastructure can be used for access to higher-level services, such as IP-based virtual private networking, public internet communications, Voice over IP, or a combination of all applications.

Ethernet Wire Service (EWS)

An Ethernet Virtual Circuit (EVC) connects two physical User-to-Network Interfaces (UNI) such that the connection appears like a virtual private line to the customer. VLAN transparency and control protocol tunnelling are supplied by the implementation of 802.1Q-in-Q tag-stacking technology. Packets received on one UNI are transported directly to the other corresponding UNI.

Ethernet Relay Service (ERS)

An Ethernet Virtual Circuit (EVC) is used to logically connect endpoints, but multiple EVCs could exist per single UNI. Each EVC is distinguished by 802.1q VLAN tag identification. The ERS network acts as if the Ethernet frames have crossed a switched network, and certain control traffic is not carried between ends of the EVC. ERS is analogous to Frame Relay where the CE-VLAN tag plays the role of a Data-Link Connection Identifier (DLCI).

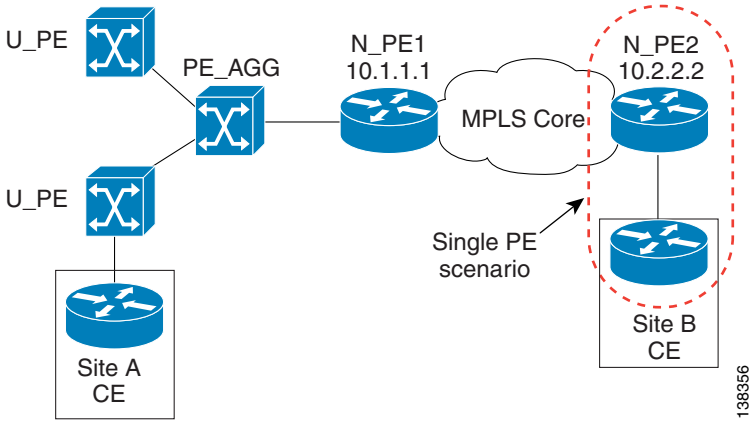
Topology for L2VPN Ethernet Over MPLS (ERS and EWS)

Ethernet Over MPLS (EoMPLS) is a tunnelling mechanism that allows the service provider to tunnel customer Layer 2 traffic though a Layer 3 MPLS network. It is important to remember that EoMPLS is a point-to-point solution only.

The following figures provide a reference for how EoMPLS is utilized. Ethernet Services can be distributed to the end customer in two ways.

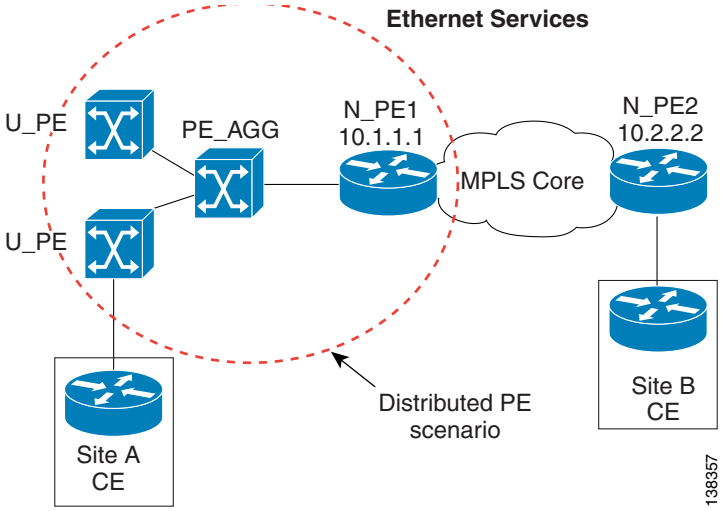
- Single PE scenario—The customer is directly connected to an Ethernet port on the N-PE in Figure 2-1.

Figure 2-1 Single PE scenario



- Distributed PE scenario—The end customer is connected through an Access Domain to the N-PE in Figure 2-2. That is, there is a Layer 2 switching environment in the middle of CE and N-PE.

Figure 2-2 Distributed PE Scenario



In both cases, a VLAN is assigned in one of the following ways:

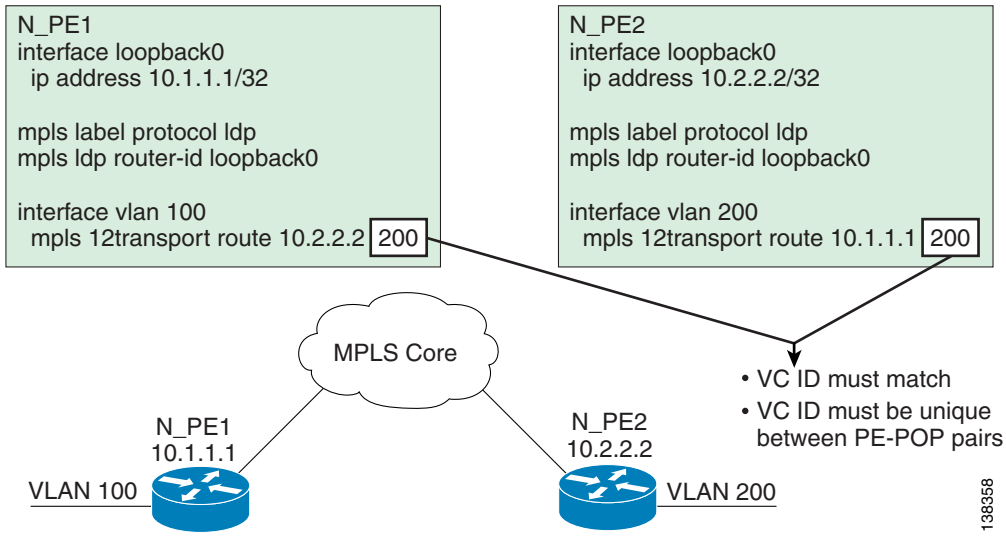
- Automatically assigned by ISC from the VLAN pool that is predefined by the user.
- Manually assigned by the user through the GUI or the North Bound Interface (NBI).

In EoMPLS, ISC creates a point-to-point tunnel and then targets the EoMPLS tunnel to the peer N-PE router through which the remote site can be reached. The remote N-PE is identified by its loopback address (in Figure 2-3, N-PE1 and N-PE2 have 10.1.1.1 and 10.2.2.2 as loopback addresses). In Figure 2-3, Site A has been allocated a VLAN-100 and Site B a VLAN-200. You can have different VLAN IDs at either end of the circuit because the VLANs have local significance only (that is, within the Ethernet access domain which is delimited by the N-PE).

For the N-PE that is serving Site A, a VLAN interface (Layer 3 interface) is created to terminate all L2 traffic for the customer, and an EoMPLS tunnel is configured on this interface. [1]

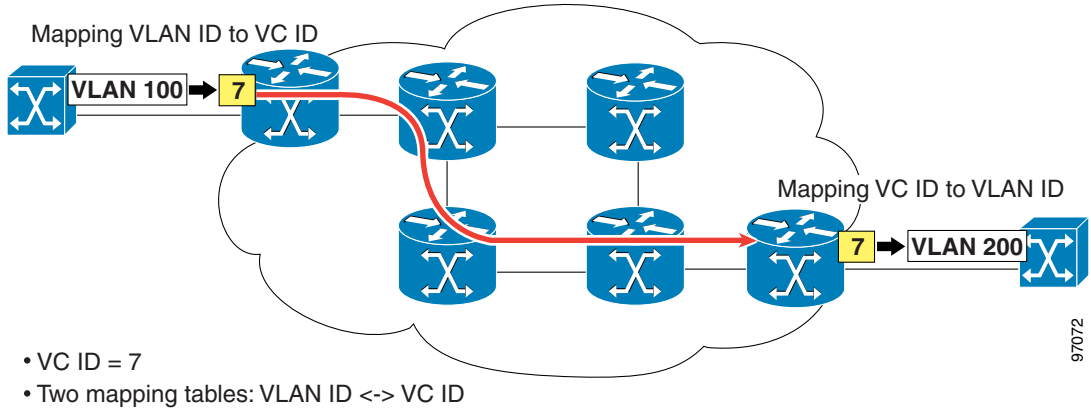
1. This configuration is based on the Cisco 7600 Optical Services Router. Other routers, such as the Cisco 7200, have different configurations.

Figure 2-3 Ethernet over MPLS Configuration



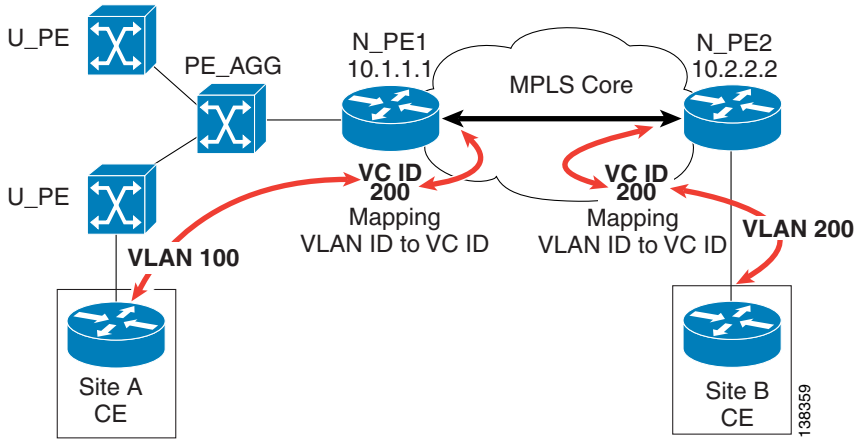
The VC ID that defines the EoMPLS tunnel is 200 as shown in Figure 2-3. Note that the VC ID has to be the same on both ends of the EoMPLS tunnel. On each N-PE, there is mapping done between the VLANs to the EoMPLS tunnel (Figure 2-4). For the overall connection, this mapping is: VLAN ID <-> VC ID <-> VLAN ID.

Figure 2-4 EoMPLS Tunnel



This VLAN-VC ID mapping lets the service provider reuse VLAN IDs in Access Domains (see Figure 2-5). The VLAN IDs allocated and used at each access domain do not have to be the same.

Figure 2-5 VLAN-VC ID Mapping



ATM over MPLS (ATMoMPLS)

With Cisco ATM over MPLS (ATMoMPLS), Cisco supports ATM Adaptation Layer 5 (AAL5) transport and Cell Relay over MPLS.

AAL5

AAL5 allows you to transport AAL5 PDUs from various customers over an MPLS backbone. ATM AAL5 extends the usability of the MPLS backbone by enabling it to offer Layer 2 services in addition to already existing Layer 3 services. You can enable the MPLS backbone network to accept AAL5 PDUs by configuring the provider edge (PE) routers at both ends of the MPLS backbone.

To transport AAL5 PDUs over MPLS, a virtual circuit is set up from the ingress PE router to the egress PE router. This virtual circuit transports the AAL5 PDUs from one PE router to the other. Each AAL5 PDU is transported as a single packet.

Cell Relay over MPLS

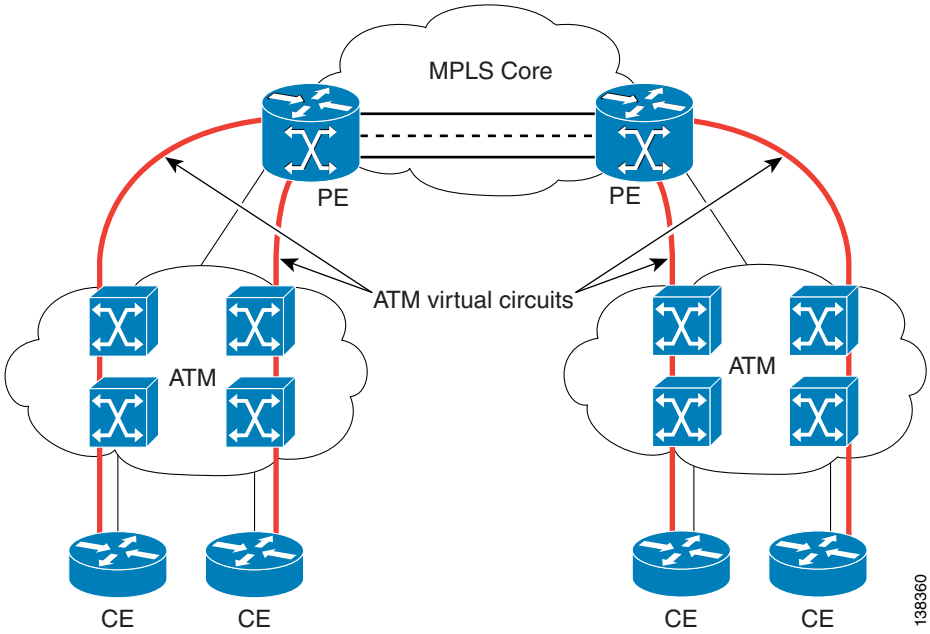
Cell Relay over MPLS allows you to transport ATM cells from various customers over an MPLS backbone. ATM Cell Relay extends the usability of the MPLS backbone by enabling it to offer Layer 2 services in addition to already existing Layer 3 services. You can enable the MPLS backbone network to accept ATM cells by configuring the provider edge (PE) routers at both ends of the MPLS backbone.

To transport ATM cells over MPLS, a virtual circuit is set up from the ingress PE router to the egress PE router. This virtual circuit transports the ATM cells from one PE router to the other. Each MPLS packet can contain one or more ATM cells. The encapsulation type is AAL0.

Topology for ATMoMPLS

Only the single PE scenario is supported as shown in Figure 2-6.

Figure 2-6 Configuring AAL5 and Cell Relay over MPLS



Frame Relay over MPLS (FRoMPLS)

With Cisco AToM for Frame Relay, customer Frame Relay traffic can be encapsulated in MPLS packets and forwarded to destinations required by the customer. Cisco AToM allows service providers to quickly add new sites with less effort than typical Frame Relay provisioning.

Frame Relay over MPLS enables a service provider to transport Frame Relay frames across an MPLS backbone. This extends the reachability of Frame Relay and allows service providers to aggregate frame transport across a common packet backbone. The service provider can integrate an existing Frame Relay environment with the packet backbone to improve operational efficiency and to implement the high-speed packet interfaces to scale the Frame Relay implementations.

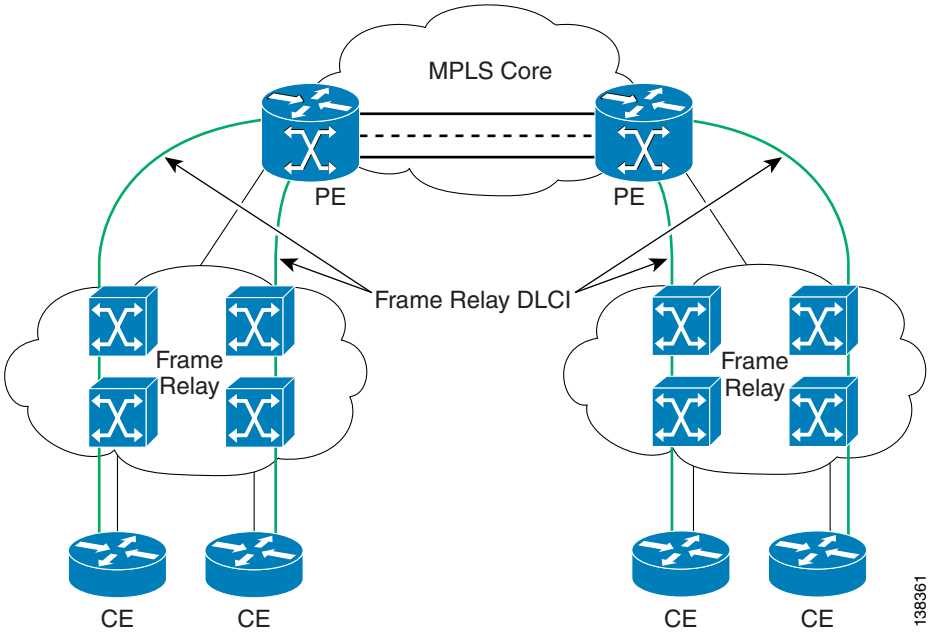
Transporting Frame Relay frames across MPLS networks provides a number of benefits, including:

- Frame Relay extended service.
- Aggregation to a higher speed backbone, such as OC-192, to scale Frame Relay implementations.
- Improved operational efficiency—the MPLS backbone becomes the single network that integrates the various existing networks and services.

Topology for FRoMPLS

Only the single PE scenario is supported as shown in Figure 2-7.

Figure 2-7 Frame Relay over MPLS



Layer 2 Tunnel Protocol Version 3 (L2TPv3)

IP-based Layer 2 Tunnel Protocol Version 3 (L2TPv3) provides Layer 2 point-to-point connectivity over a pure IP (non-MPLS) infrastructure. L2TPv3 concepts are covered in the following sections:

- Overview of L2TPv3, page 2-8
- L2TPv3 Session Parameters, page 2-10
- Frame Relay Transport, page 2-10
- ATM Transport, page 2-11

Overview of L2TPv3

L2TPv3 allows a service provider to replace a legacy switch-based core with an IP router-based core without any impact to a customer's existing Layer 2 connectivity.

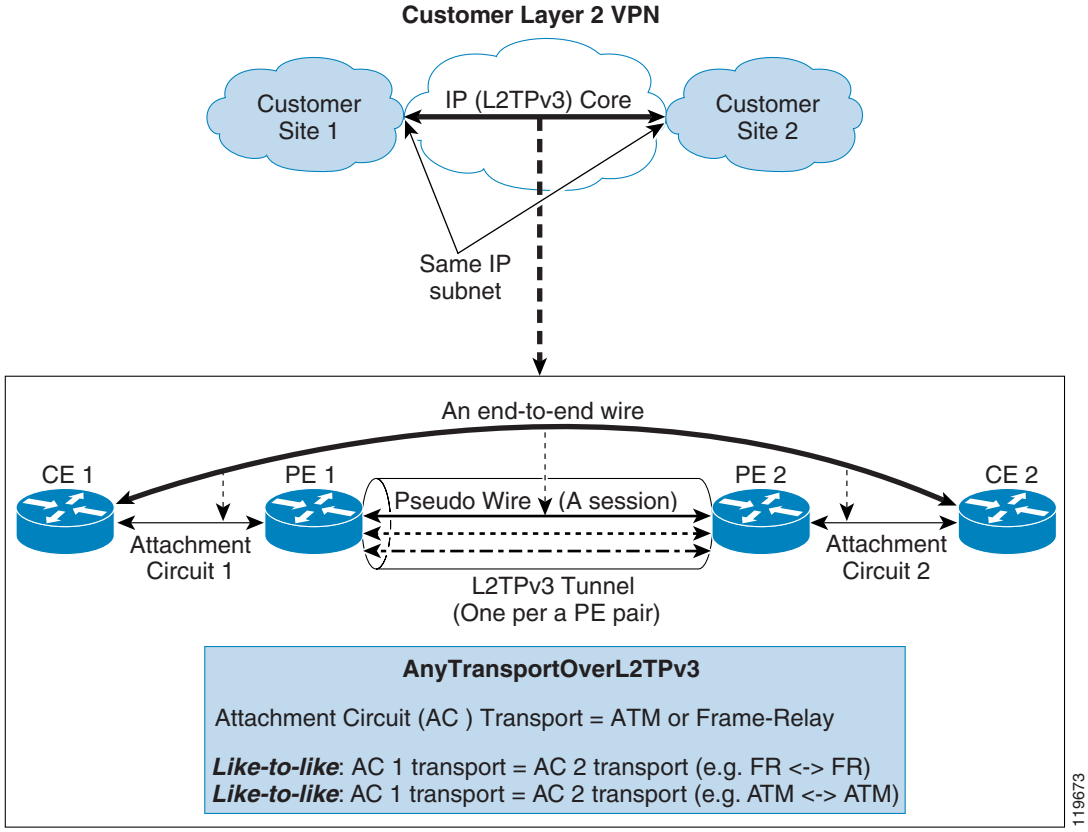
L2TPv3 uses a directed Control Channel session between edge routers for creating and maintaining connections. Forwarding occurs through the use of IP packet forwarding between two edge devices. An IP header and the L2TPv3 header are used to forward packets between routers. The external header is an IP header that routes tunneled packets over the IP backbone to the egress Provider Edge (PE) device. The L2TPv3 header determines the egress interface, and binds the Layer 2 egress interface to the tunnel.

L2TPv3 defines the L2TP protocol for tunnelling Layer 2 payloads over an IP core network using Layer 2 virtual private networks (VPNs). Benefits of this feature include the following:

- Simplifies deployment of VPNs.
- Does not require Multiprotocol Label Switching (MPLS) virtual private network (VPN).
- Supports Layer 2 tunnelling over IP for any payload.
- Supports data encapsulation directly over IP (IP protocol number 115), not using User Datagram Protocol (UDP)
- Supports point-to-point sessions, not point-to-multipoint or multipoint-to-point sessions
- Supports sessions between the same Layer 2 protocols, for example Frame Relay-to-Frame Relay or ATM-to-ATM.

Figure 2-8 shows an example of how the L2TPv3 feature is used for setting up VPNs using Layer 2 tunnelling over an IP network. All traffic between two customer network sites is encapsulated in IP packets carrying L2TP data messages and sent across an IP network. The backbone routers of the IP network treat the traffic as any other IP traffic and need not know anything about the customer networks.

Figure 2-8 L2TPv3 Operation



L2TPv3 Session Parameters

L2TPv3 sessions can be setup in either dynamic mode or static mode.

Static L2TPv3 Sessions

Typically, the L2TP control plane is responsible for negotiating session parameters, such as the session ID or the cookie, in order to set up the session. However, some IP networks require sessions to be configured so that no signaling is required for session establishment. You can, therefore, set up static L2TPv3 sessions for a PE router by configuring fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the attachment circuit to which the session is bound comes up.

Dynamic L2TPv3 Sessions

A dynamic L2TP session is established through the exchange of control messages containing attribute-value pairs (AVPs). Each AVP contains information about the nature of the Layer 2 link being forwarded, including the payload type, virtual circuit (VC) ID, and so on.

Multiple L2TP sessions (one for each forwarded Layer 2 circuit) can exist between a pair of PEs, and can be maintained by a single control channel. Session IDs and cookies are dynamically generated and exchanged as part of a dynamic session setup. Information such as sequencing configuration is also exchanged.

Sequencing

Although the correct sequence of received Layer 2 frames is guaranteed by some Layer 2 technologies (by the nature of the link, such as a serial line) or the protocol itself, forwarded Layer 2 frames can be lost, duplicated, or reordered when they traverse a network as IP packets. If the Layer 2 protocol does not provide an explicit sequencing mechanism, ISC lets you configure L2TPv3 to sequence its data packets.

Session Cookie

The L2TPv3 header contains a control channel cookie field that has a variable length of 0, 4, or 8 bytes according to the cookie length supported by a given platform for packet decapsulation. The control channel cookie length can be manually configured or auto-picked by ISC for static sessions, or dynamically determined for dynamic sessions.

The variable cookie length does not present a problem when the same platform is at both ends of an L2TPv3 control channel. However, when different platforms interoperate across an L2TPv3 control channel, both platforms must encapsulate packets with a 4-byte cookie length.

Frame Relay Transport

In L2TPv3 frame relay, traffic is encapsulated in IP/L2TPv3 packets and forwarded across the IP network. When encapsulating Frame Relay over IP, the Frame Relay header is passed in the payload of the packet. Thus the bits for Backward Explicit Congestion Notification (BECN), Forward Explicit Congestion Notification (FECN), Discard Eligibility (DE) and Command/Response (C/R) ar carried across the IP network.

- Frame relay trunking enables users to take all of the frame relay data and tunnel it across an IP core to a remote destination. It is used for interconnecting and transporting a frame relay point of presence (POP) across an IP core network.
- DLCI tunnelling allows for the tunnelling of individual frame relay PVCs. This method offers granularity of controlling which of the traffic is tunneled to a given destination.

ISC supports the Multilink Frame Relay (MFR) interface. It is a bundle interface that combines several frame relay interfaces into one super interface.

From a provisioning point of view, you only configure the MFR interface but do not create it. You precreate the bundle (MFR) and the bundle-links (the Frame Relay interfaces that make up the MFR interface).

ATM Transport

L2TPv3 supports two modes of ATM transport between two PEs: Virtual Path (VP) and Virtual Circuit (VC). In VP mode, cells coming into a predefined PVP on the ATM interface to be transported over an L2TPv3 pseudowire to a predefined PVP on the egress ATM interface. This task binds a PVP to an L2TPv3 pseudowire for Xconnect service. In VC mode, L2TPv3 can be used to carry any type of AAL traffic over the pseudowire. It will not distinguish OAM cells from user data cells. In this mode, PM and Security OAM cells are also transported over the pseudowire.

The encapsulations of an ATM cell can be either AAL5 or cell relay (AAL0). In cell relay mode, the ATM interface receives cells and transports them across the IP core. Cell relay with cell packing is used to send multiple cells in one IP frame, which improves the efficiency of cell transport. The signaling is transparently passed through the IP cloud, rather than being terminated at the PE.

VPLS Service Provisioning

VPLS is a multipoint Layer 2 VPN that connects two or more customer devices using EoMPLS bridging techniques. VPLS EoMPLS is an MPLS-based provider core, that is, the PE routers have to cooperate to forward customer Ethernet traffic for a given VPLS instance in the core.

A VPLS essentially emulates an Ethernet switch from a user's perspective. All connections are peers within the VPLS and have direct communications. The architecture is actually that of a distributed switch.

Multiple attachment circuits have to be joined together by the provider core. The provider core has to simulate a virtual bridge that connects these multiple attachment circuits together. To achieve this, all PE routers participating in a VPLS instance form emulated VCs among them.

A Virtual Forwarding Instance (VFI) is created on the PE router for each VPLS instance. PE routers make packet-forwarding decisions by looking up the VFI of a particular VPLS instance. The VFI acts like a virtual bridge for a given VPLS instance. More than one attachment circuit belonging to a given VPLS can be connected to this VFI. The PE router establishes emulated VCs to all the other PE routers in that VPLS instance and attaches these emulated VCs to the VFI. Packet forwarding decisions are based on the data structures maintained in the VFI. All the PE routers in the VPLS domain use the same VC-ID for establishing the emulated VCs. This VC-ID is also called the VPN-ID in the context of the VPLS VPN. For more information, see the following sections:

- Multipoint EWS for an MPLS-Based Provider Core, page 2-12
- Multipoint ERS for an MPLS-Based Provider Core, page 2-12
- Topology for MPLS-Based VPLS, page 2-12

Multipoint EWS for an MPLS-Based Provider Core

With multipoint EWS, the PE router forwards all Ethernet packets received from an attachment circuit, including tagged, untagged, and Bridge Protocol Data Unit (BPDU) to either:

- Another attachment circuit or an emulated VC if the destination MAC address is found in the L2 forwarding table (VFI).
- All other attachment circuits and emulated VCs belonging to the same VPLS instance if the destination MAC address is a multicast/broadcast address or not found in the L2 forwarding table.

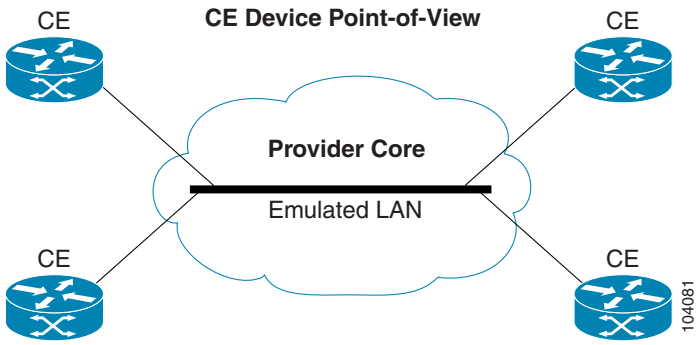
Multipoint ERS for an MPLS-Based Provider Core

With multipoint ERS, the PE router forwards all Ethernet packets with a particular VLAN tag received from an attachment circuit, excluding BPDU, to another attachment circuit or an emulated VC if the destination MAC address is found in the L2 forwarding table (VFI). If the destination MAC address is not found or if it is a broadcast/multicast packet, then it is sent on all other attachment circuits and emulated VCs belonging to the VPLS instance. The demultiplexing VLAN tag used to identify a VPLS domain is removed prior to forwarding the packet to the outgoing Ethernet interfaces or emulated VCs because it only has local significance.

Topology for MPLS-Based VPLS

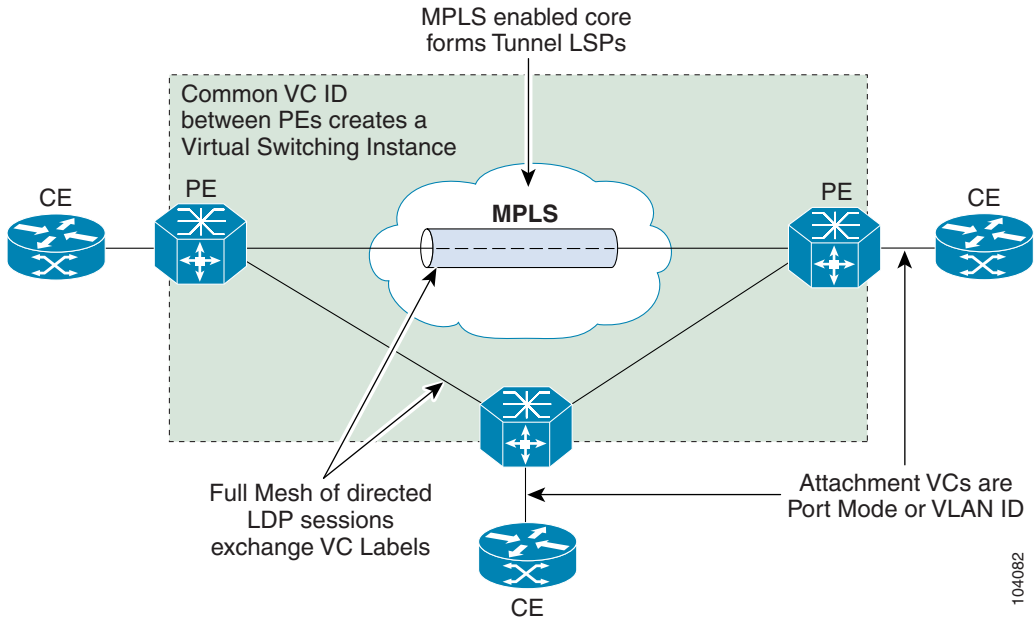
From a customer point of view there is no topology for VPLS. All the CE devices are connected to a logical bridge emulated by the provider core. Therefore, the CE devices see a single emulated LAN as shown in Figure 2-9.

Figure 2-9 MPLS-Based VPLS Topology



The PE routers must create a full-mesh of emulated virtual circuits (VCs) to simulate the emulated LAN seen by the CE devices. Forming a full-mesh of emulated VCs simplifies the task of emulating a LAN in the provider core. One property of a LAN is to maintain a single broadcast domain. That is, if a broadcast, multicast, or unknown unicast packet is received on one of the attachment circuits, it has to be sent to all other CE devices participating in that VPLS instance. The PE device handles this case by sending such a packet on all other attachment circuits and all the emulated circuits originating from that PE. With a full-mesh of emulated VCs, such a packet will reach all other PE devices in that VPLS instance. See Figure 2-10.

Figure 2-10 Full Mesh of Emulated VCs



VPLS for an Ethernet-Based (L2) Provider Core

With an Ethernet-based provider core, customer traffic forwarding is trivial in the core. VPLS for an Ethernet-based provider core is a multipoint Layer 2 VPN that connects two or more customer devices using 802.1Q-in-Q tag-stacking technology. A VPLS essentially emulates an Ethernet switch from a users perspective. All connections are peers within the VPLS and have direct communications. The architecture is actually that of a distributed switch.

For more information on VPLS for an Ethernet-based provided core, see the following sections:

- Multipoint EWS for an Ethernet-Based Provider Core, page 2-13
- Multipoint ERS for an Ethernet-Based Provider Core, page 2-14
- Topology for Ethernet-Based VPLS, page 2-14

Multipoint EWS for an Ethernet-Based Provider Core

Multipoint EWS is a service that emulates a point-to-point Ethernet segment. The EWS service encapsulates all frames that are received on a particular User to Network Interface (UNI) and transports these frames to a single egress UNI without reference to the contents contained within the frame. This service operation means that EWS can be used for untagged or VLAN tagged frames and that the service is transparent to all frames offered. Because the EWS service is unaware that VLAN tags might be present within the customer frames, the service employs a concept of “All to One” bundling.

Multipoint ERS for an Ethernet-Based Provider Core

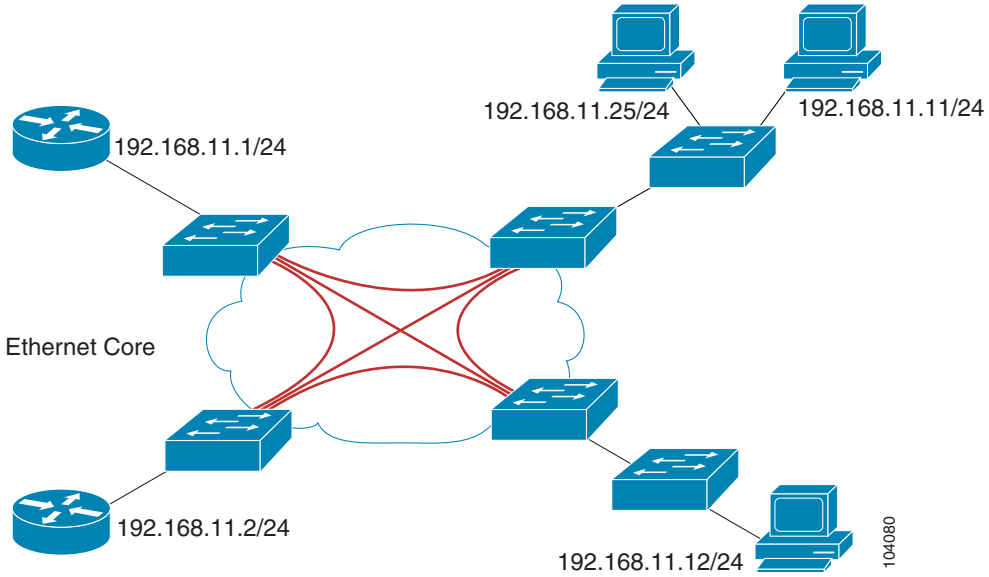
Multipoint ERS models the connectivity offered by existing Frame Relay networks by using VLAN indices to identify virtual circuits between sites. ERS does, however, offer a far greater degree of QoS functionality depending upon the service provider's implementation and the customer's acceptance of VLAN indices that are administratively controlled by the service provider. Additionally, ERS service multiplexing capability offers lower cost of ownership for the enterprise as a single interface can support many virtual interfaces.

Topology for Ethernet-Based VPLS

Ethernet-based VPLS differs from the point-to-point L2VPN definitions of EWS and ERS by providing a multipoint connectivity model. The VPLS service does not map an interface or VLAN to a specific point-to-point pseudo-wire, but instead it models the operation of a virtual Ethernet switch. VPLS uses the customer’s MAC address to forward frames to the correct egress UNI within the service provider’s network for the EWS.

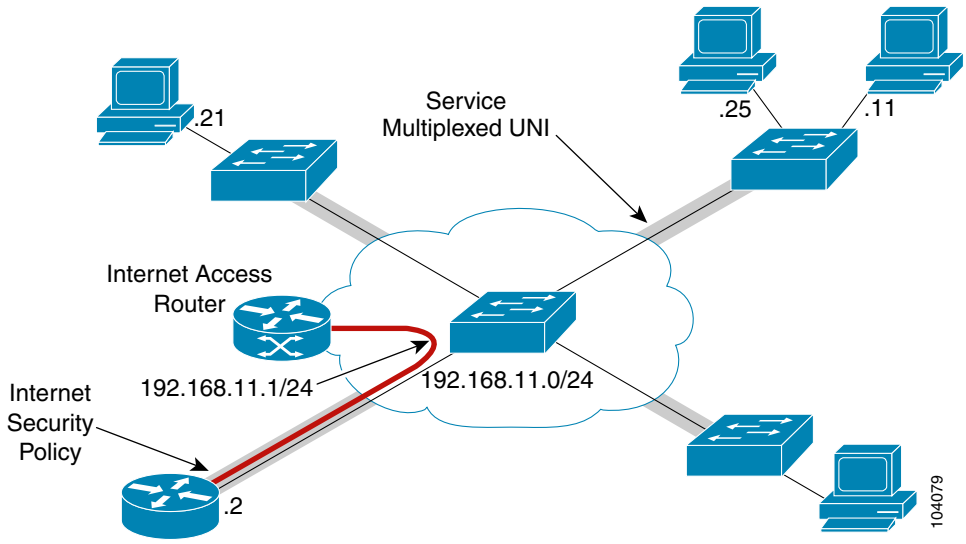
The EWS service emulates the service attributes of an Ethernet switch and learns source MAC to interface associations, flooding unknown broadcast and multicast frames. Figure 2-11 illustrates an EWS VPLS topology.

Figure 2-11 VPLS EWS Topology



The Ethernet Relay Service (ERS) offers the any-to-any connectivity characteristics of EWS and the service multiplexing. This combination enables a single UNI to support a customer's intranet connection and one or more additional EVCs for connection to outside networks, ISPs, or content providers. Figure 2-12 illustrates an ERS VPLS multipoint topology.

Figure 2-12 VPLS ERS Multipoint Topology



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.

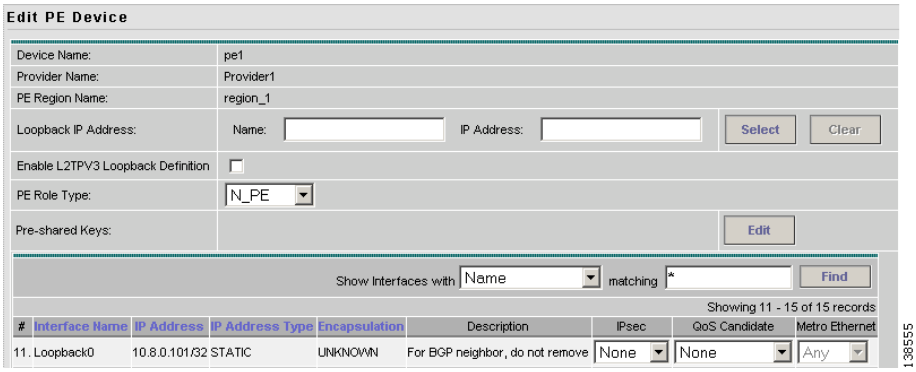
For detailed steps to create devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

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.

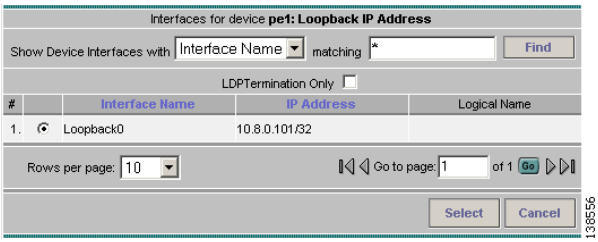
See Figure 3-1 for an example of a loopback address.

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



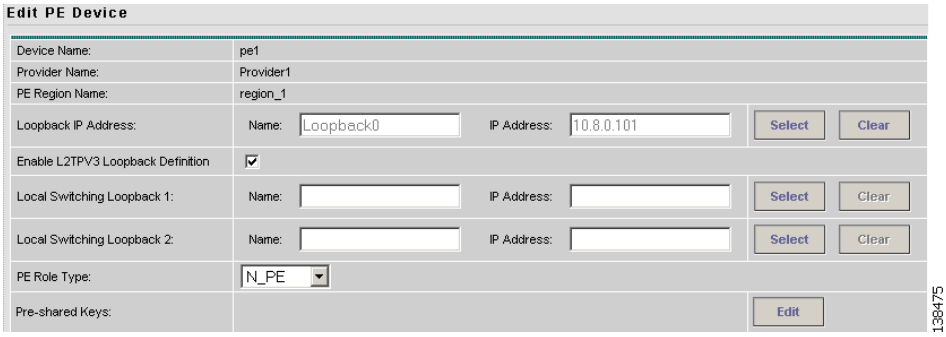
This feature ensures that a valid loopback address is set.

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

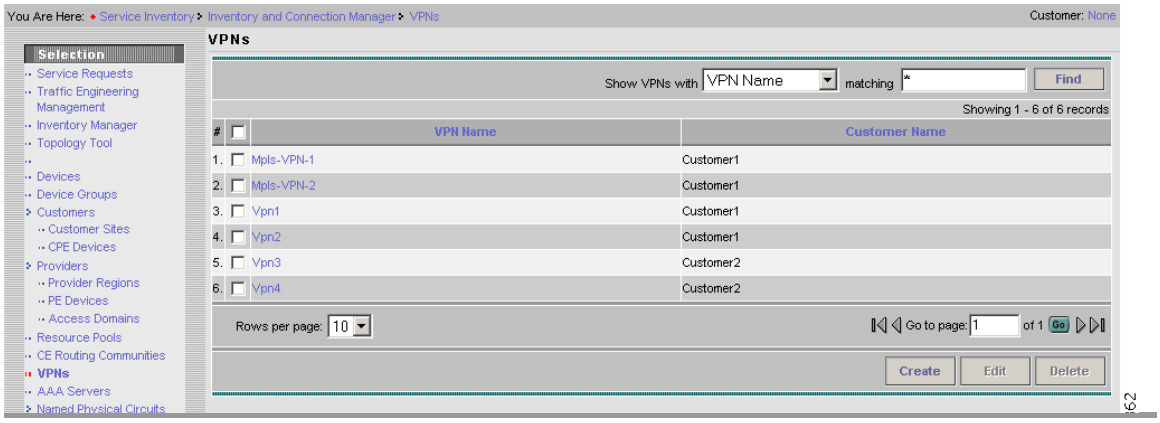
You must define VPNs before provisioning L2VPN or VPLS. In L2VPN, one VPN can be shared by different service types. In VPLS, one VPN is required for each VPLS instance.

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:

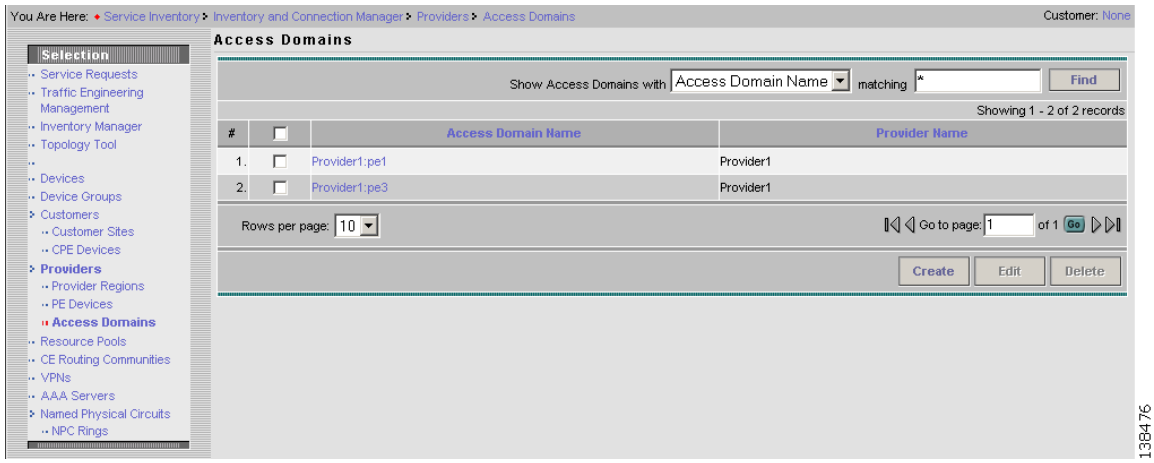
- Know the name of the access domain that you want to create.
- Have created a service provider to associate with the new access domain.
- Have created a provider region associated with your provider and PE devices.
- Have created PE devices to associate with the new access domain.
- Know the starting 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.

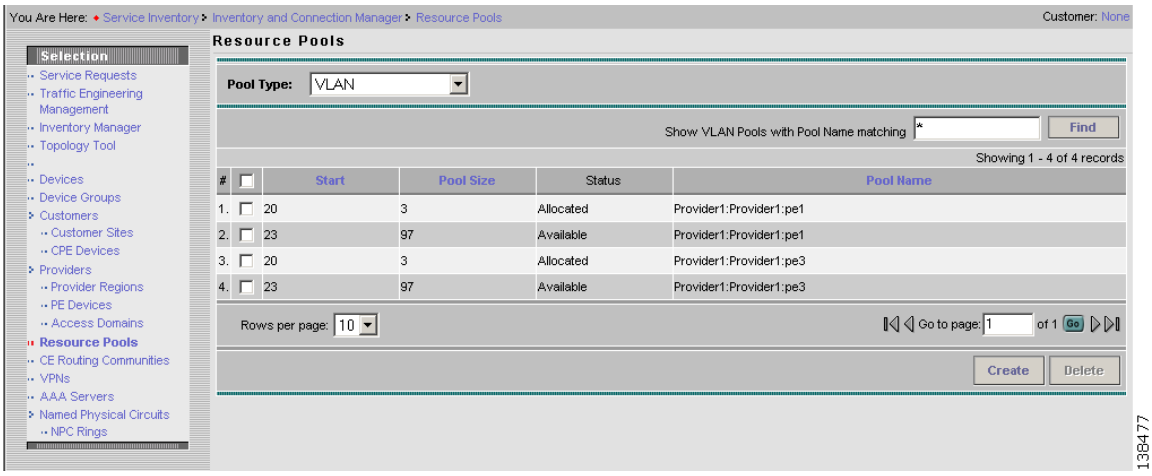
Step 1 Select **Service Inventory**.

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

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

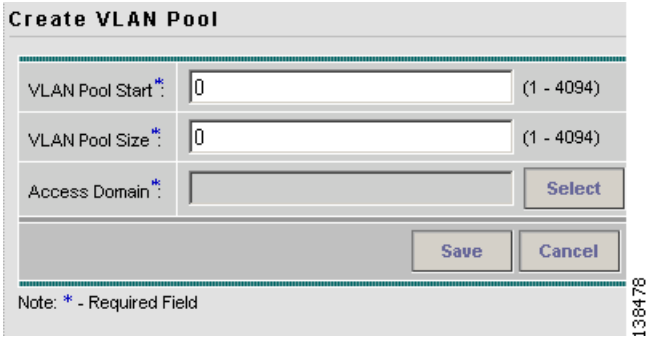
Step 4 Select **VLAN** from the drop-down **Pool Type** list as shown in Figure 3-6.

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.

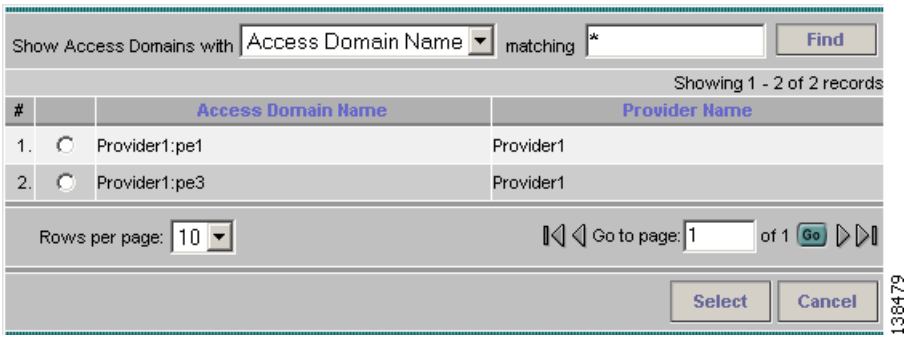
Step 7 Enter a VLAN Pool Size number.

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.

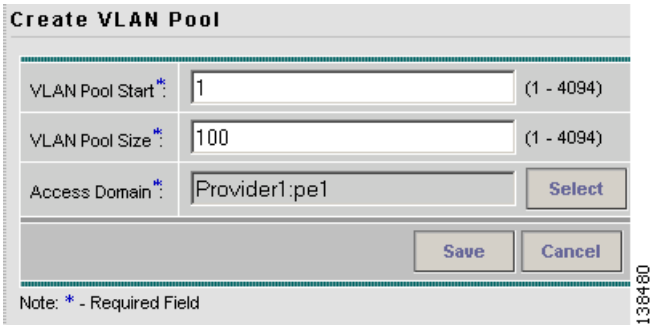
Figure 3-8 Access Domain for New VLAN Pool



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



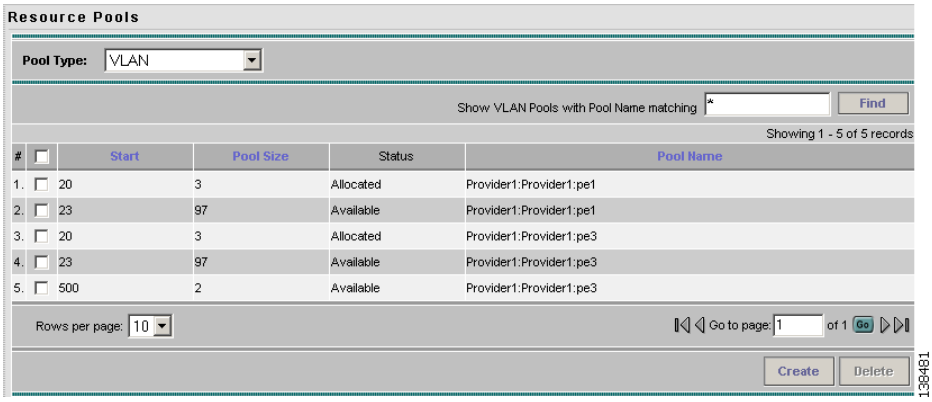
Step 9 Click **Save**.

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.

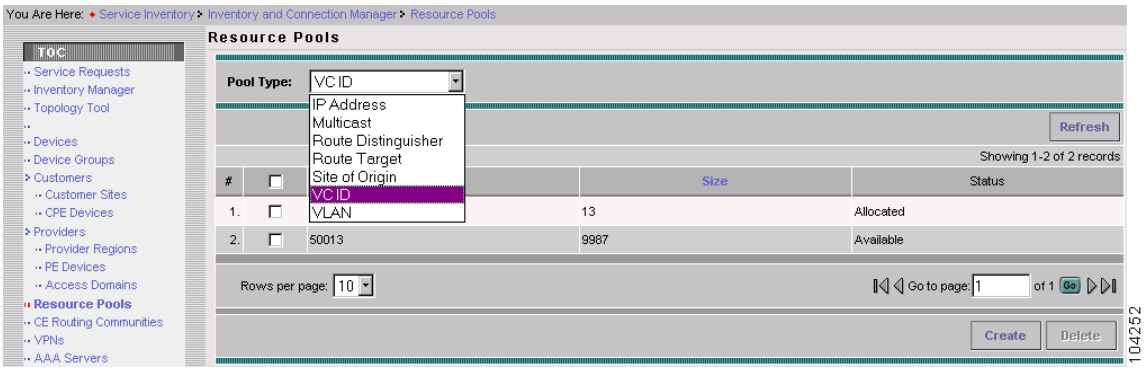
Step 1 Select **Service Inventory**.

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

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

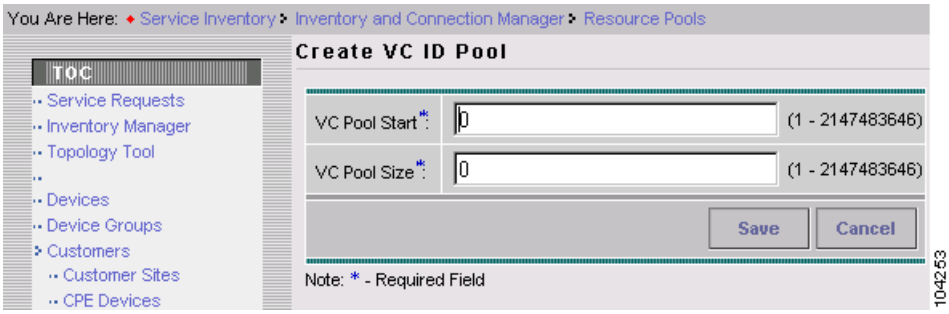
Step 3 Select **VC ID** from the drop-down **Pool Type** list as shown in Figure 3-11**.** Because this pool is a global pool, it is not associated with any other object.

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

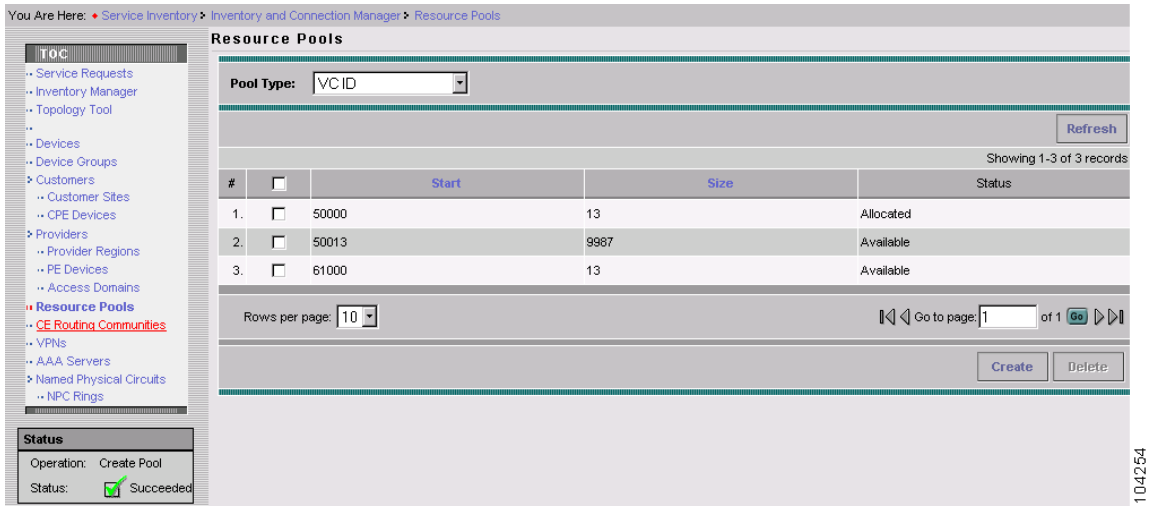


Step 5 Enter a VC pool start number.

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

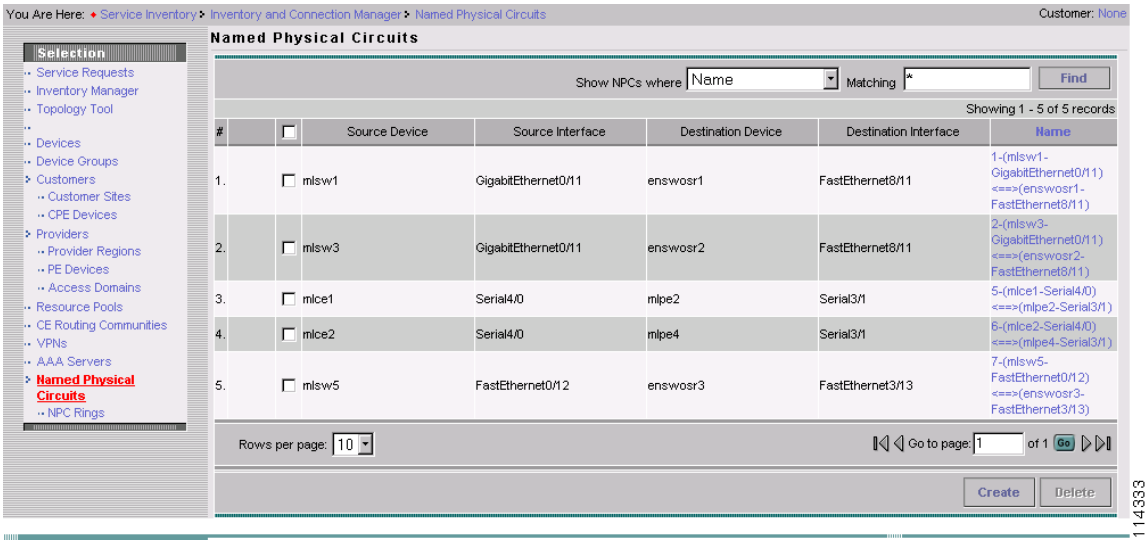
Perform the following steps to create NPCs through the NPC GUI editor.

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*.

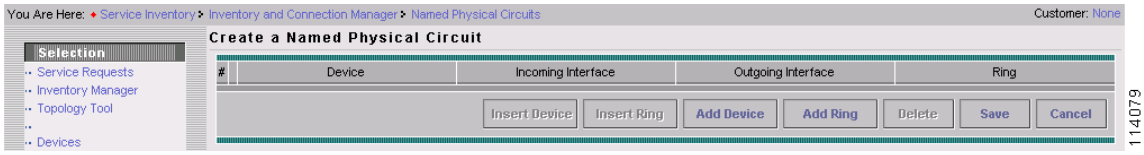
Source Device is the beginning of the link and **Destination Device** is the end of the link.

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**.

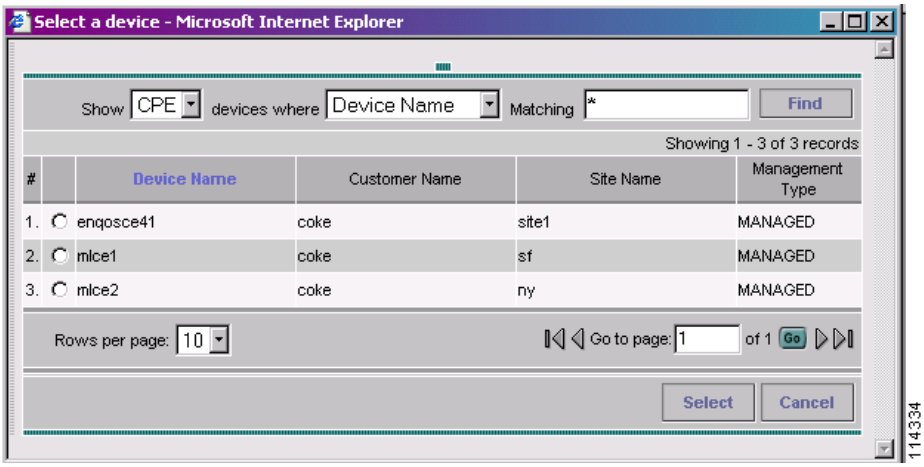
The Create a Named Physical Circuit window appears. See Figure 3-15.

Figure 3-15 Create a Named Physical Circuit



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

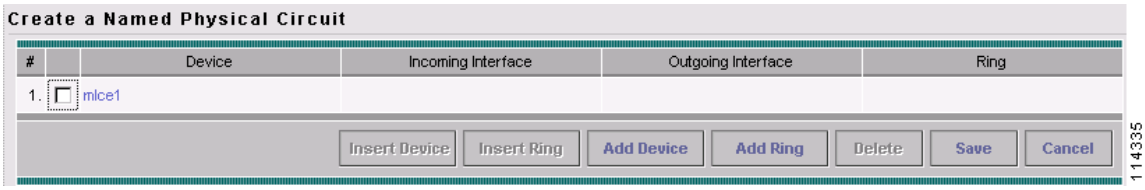
Figure 3-16 Choose a CPE



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



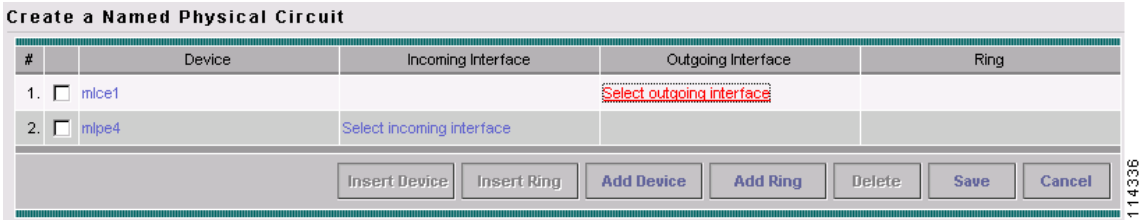
Step 8 To insert another device or a ring, click **Insert Device** or **Insert Ring**. To add another device or ring to the NPC, click **Add Device** or **Add Ring**.

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.

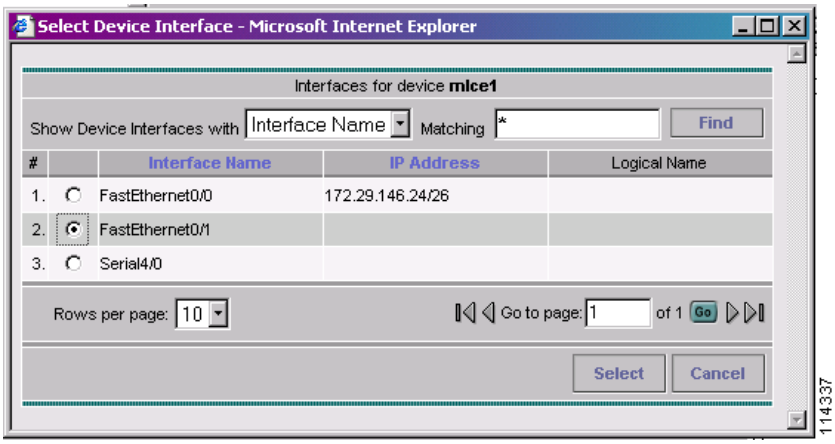
Figure 3-18 Second Device Selected for NPC



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

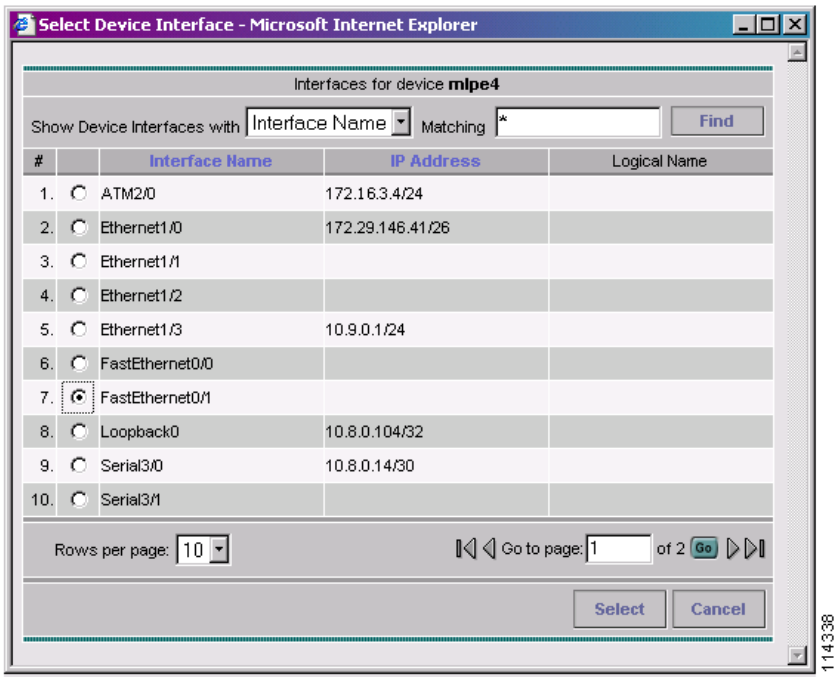


Step 12 Choose an interface from the list and click **Select**.

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



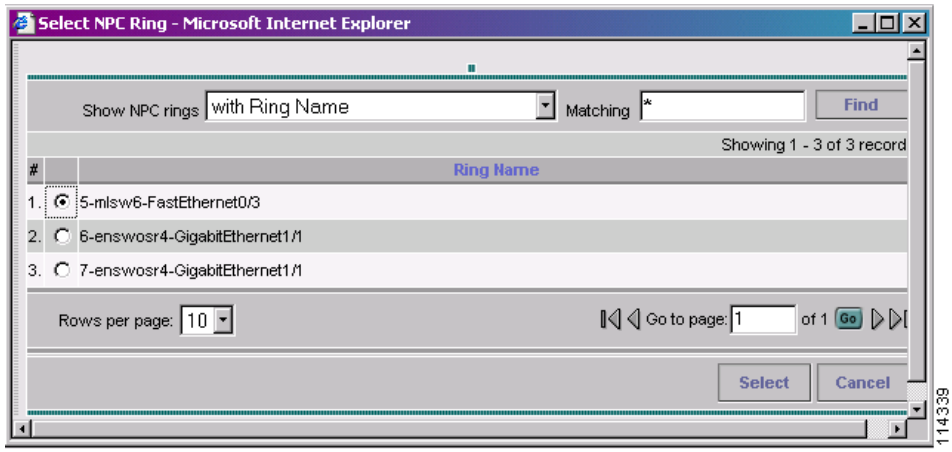
Step 14 Choose an interface from the list as the end of the link and click **Select**.

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.

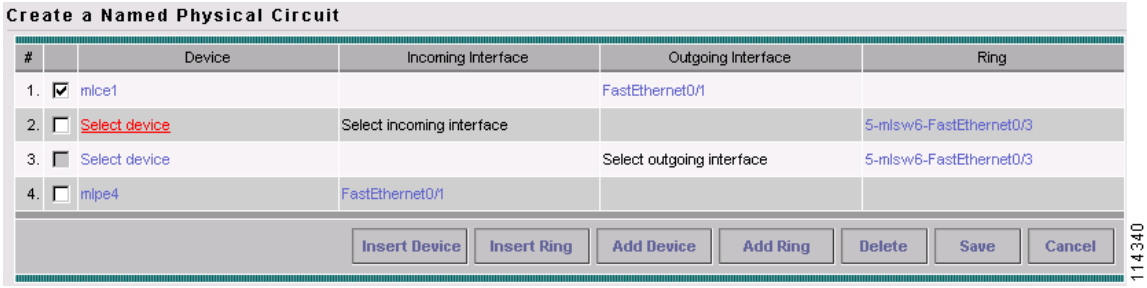
Note For L2TPv3, you cannot create rings.

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.

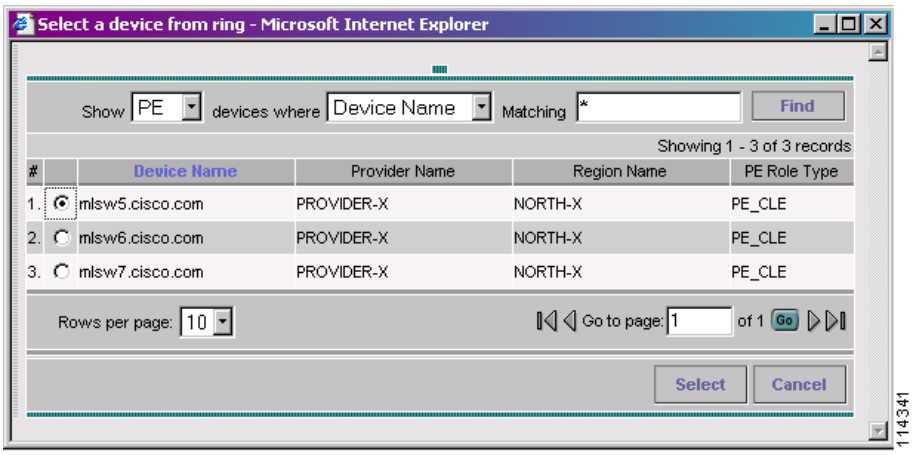
Figure 3-22 Create a Named Physical Circuit



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**.

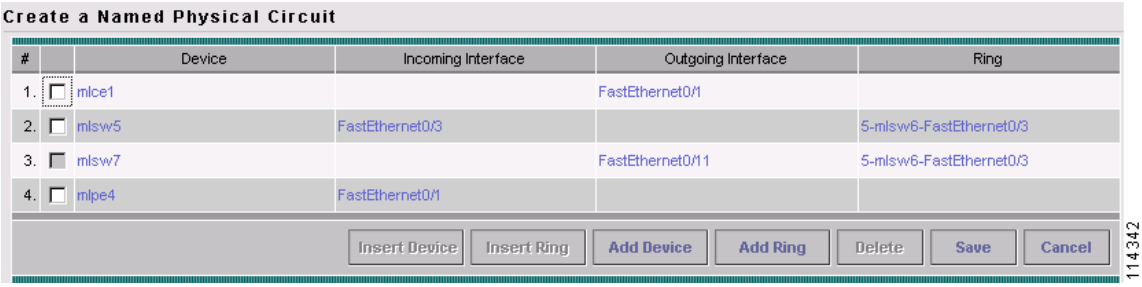
Step 22 Select a Device from the ring to connect to mlpe4 from a window like the one in Figure 3-23 and click **Select**.

Step 23 Click **Select outgoing interface**.

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

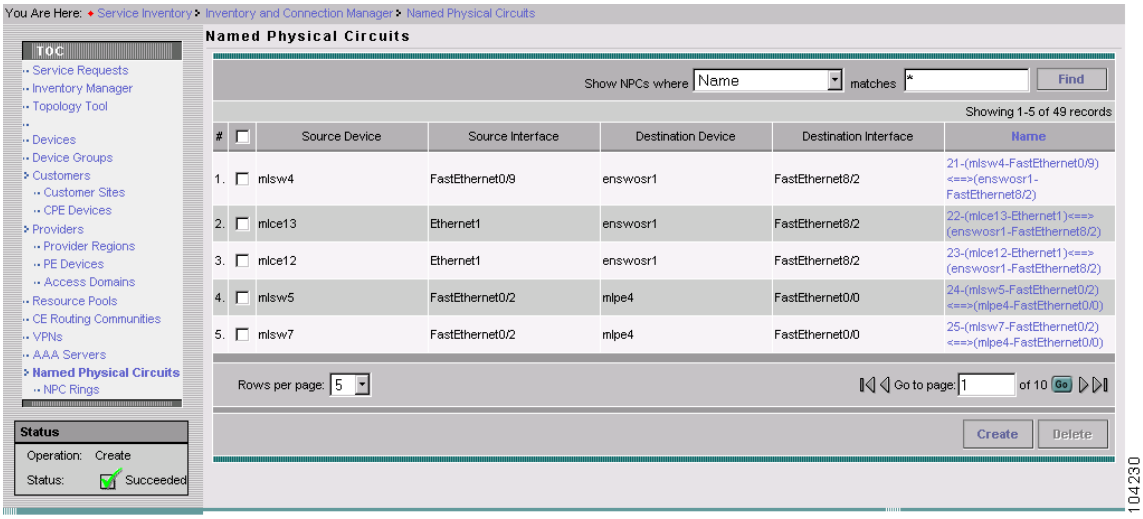
The NPC that includes the ring is now complete as shown in Figure 3-24.

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

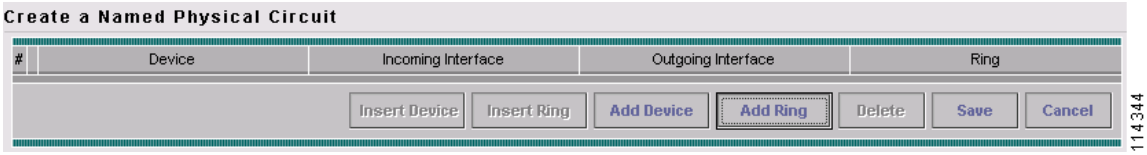
You can also create an NPC that contains only a ring without specifying CE.

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

Step 2 Click **Create**.

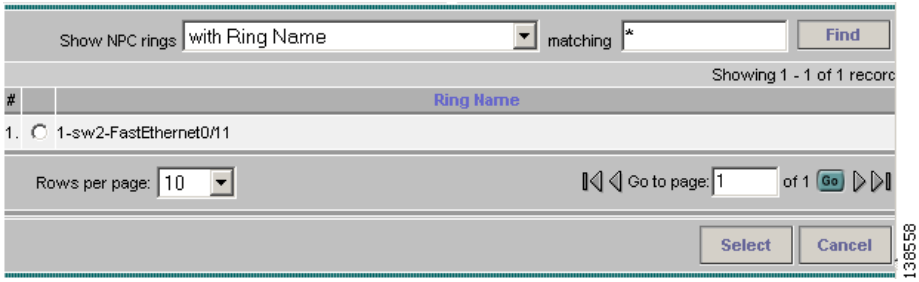
Step 3 The Create a Named Physical Circuit window appears, appears as shown in Figure 3-26.

Figure 3-26 Create an NPC that is a Ring



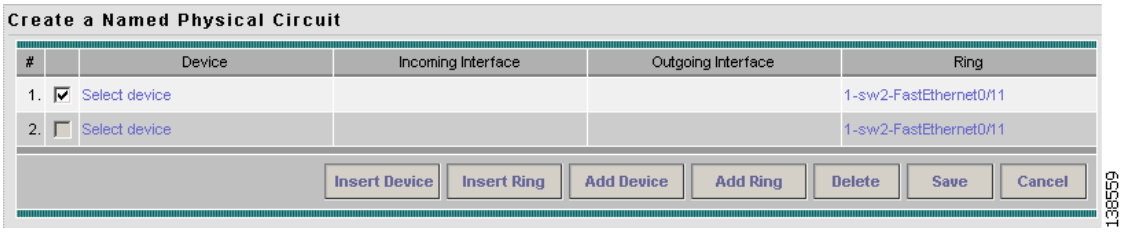
Step 4 Click **Add Ring**. The Select NPC Ring window (Figure 3-27) appears.

Figure 3-27 Select a Ring



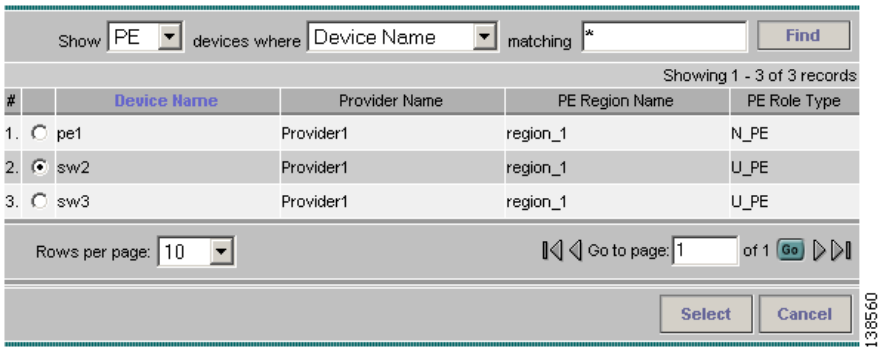
Step 5 Select a ring and click **Select**. The ring appears in a window like the one in Figure 3-28.

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**.

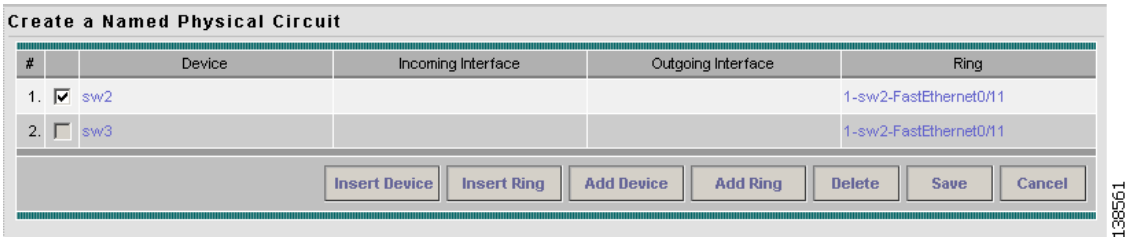
Step 8 Click the **Select device** link to choose the end of the ring.

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*.

Creating an L2VPN Policy

This chapter covers the basic steps to create an L2VPN policy. It contains the following sections:

Defining an L2VPN Policy

You must define an L2VPN policy before you can provision a Cisco IP Solution Center (ISC) service. An L2VPN policy defines the common characteristics shared by the end-to-end wire attributes and Attachment Circuit (AC) attributes.

Note If you are defining an L2TPv3 policy, seeChapter 6, “Creating an L2TPv3 Policy.”

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is *not* set to editable, the service request creator cannot change the policy item.

The four major categories of an L2VPN policy correspond to the four major services that L2VPN provides:

- Point-to-point Ethernet Relay Service (ERS)
- Point-to-point Ethernet Wire Service (EWS)
- Frame Relay over MPLS (FRoMPLS)
- ATM over MPLS (ATMoMPLS)

A policy is a template of most of the parameters needed to define an L2VPN service request. After you define it, an L2VPN policy can be used by all the L2VPN service requests that share a common set of characteristics.

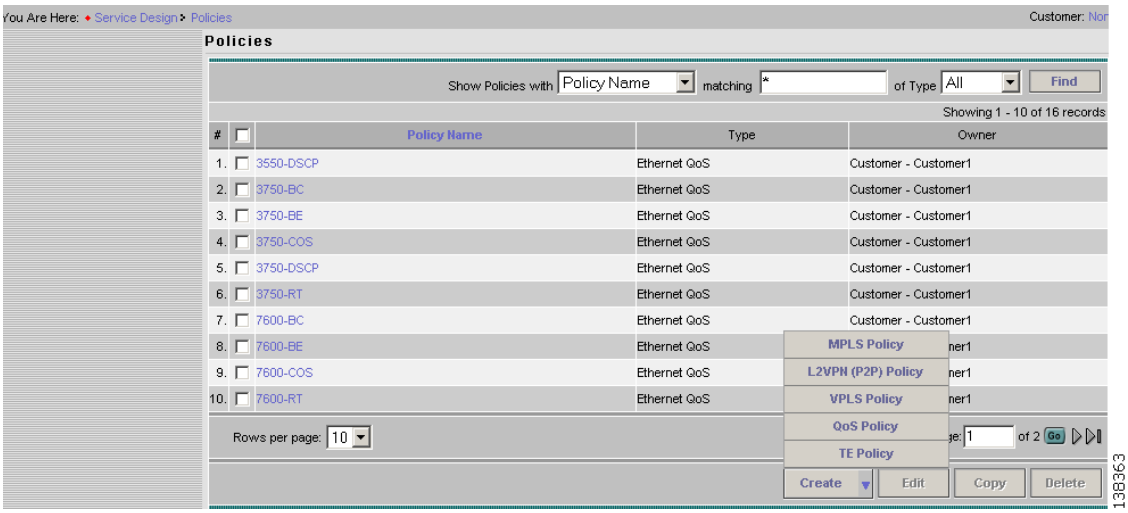
You create a new L2VPN policy whenever you create a new type of service or a service with different parameters. L2VPN policy creation is normally performed by experienced network engineers.

To define an L2VPN policy in ISC, use the following steps. See Figure 4-1.

Step 1 Select **Service Design > Policies**. The Policies window appears as shown in Figure 4-1.

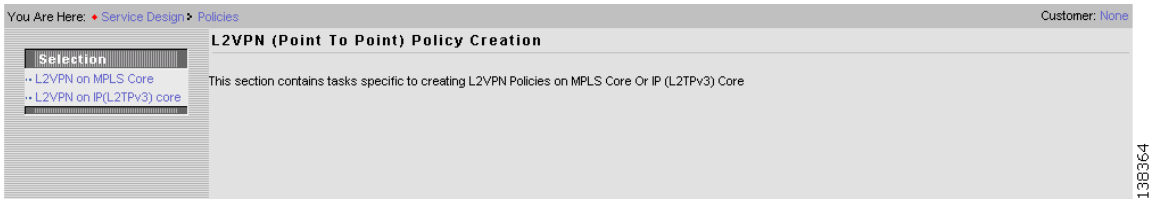
Step 2 Click **Create**.

Figure 4-1 Creating an L2VPN Policy



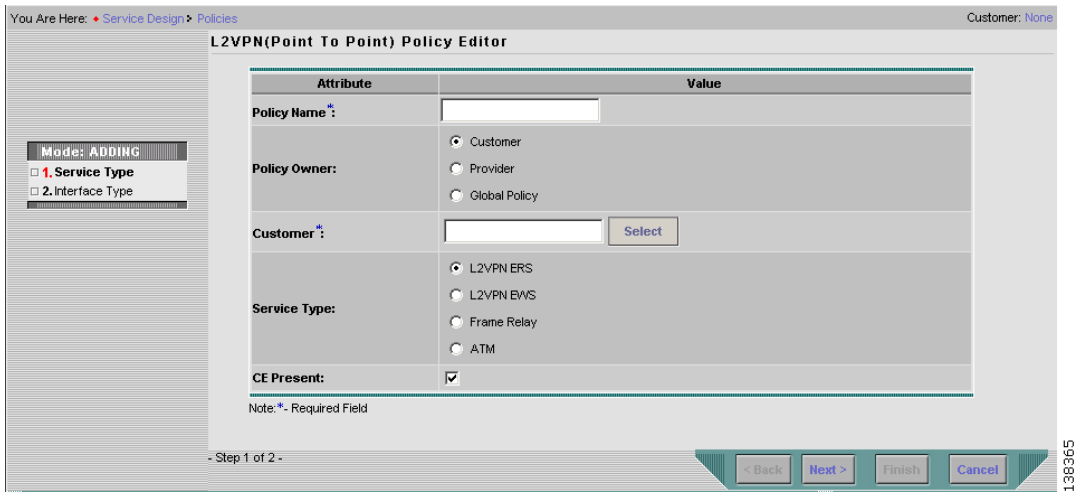
Step 3 Select **L2VPN (P2P) Policy**. When you select **L2VPN (P2P) Policy**, the window in Figure 4-3 appears.

Figure 4-2 Choosing a Policy Type



Step 4 Select **L2VPN on MPLS Core**. The window in Figure 4-3 appears.

Figure 4-3 Creating an L2VPN Policy



Step 5 Enter a **Policy Name** for the L2VPN policy.

Step 6 Choose the **Policy Owner** for the L2VPN policy.

There are three types of L2VPN policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this L2VPN policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, an L2VPN policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 7 Click **Select** to choose the owner of the L2VPN. (If you choose Global ownership, the Select function is not available.) The Select Customer window or the Select Provider window appears and you can choose an owner of the policy and click **Select**.

Step 8 Choose the **Service Type** of the L2VPN policy.

There are four service types for L2VPN policies:

- L2VPN ERS
- L2VPN EWS
- Frame Relay
- ATM

Subsequent sections of this chapter cover setting up the policies for each of these services.

Step 9 Select the **CE Present** check box if you want ISC to ask the service operator who uses this L2VPN policy to provide a CE router and interface during service activation. The default is CE present in the service.

If you do not select the **CE Present** check box, ISC asks the service operator, during service activation, only for the U-PE or the N-PE router and customer-facing interface.

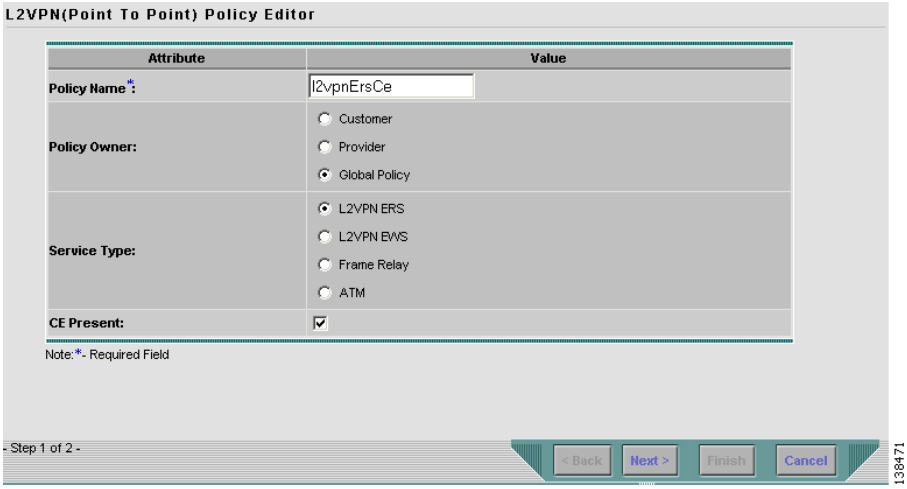
Step 10 Click **Next**.

The next sections contain examples of setting policies for the service types, with and without a CE present.

Defining an Ethernet ERS Policy with a CE

This section describes defining an Ethernet ERS policy with CE present. Figure 4-4 is an example of the first page of this policy.

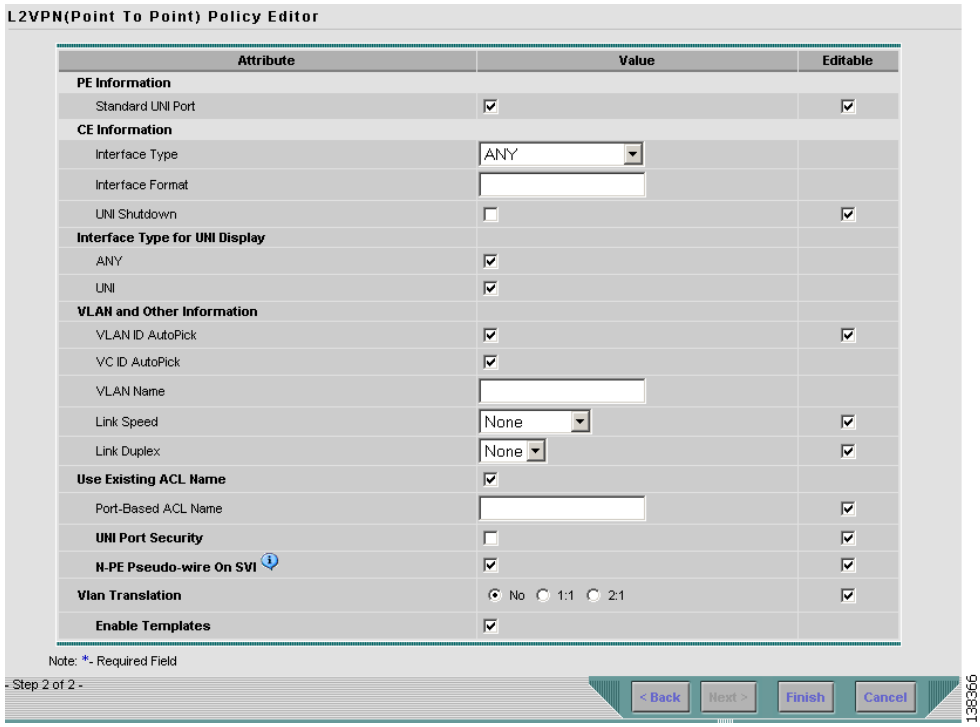
Figure 4-4 Ethernet ERS Policy with a CE



Step 1 Click **Next**. The window in Figure 4-5 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-5 Ethernet ERS with CE Policy Attributes



Step 2 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 3 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a U-PE, or N-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 10 Select the **VC ID AutoPick** check box if you want ISC to choose a VC ID. If you do not select this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 11 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this box is unselected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 17 Choose a **UNI Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Note Enter a UNI Port Type only if the encapsulation type is DEFAULT.

Step 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-6) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

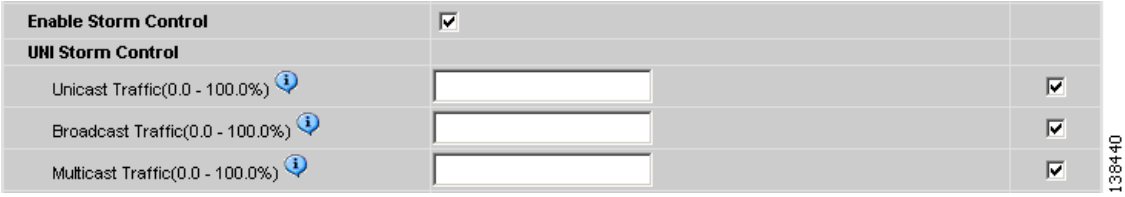
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-6 UNI Port Security

Step 20 Select the **Enable Storm Control** check box (see Figure 4-7) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 4-7 Enable Storm Control



Step 21 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 22 Specify the type of **VLAN Translation** for this policy by selecting the appropriate radio button. The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.

Note For detailed coverage of setting up VLAN translation, see Appendix A, "Setting Up VLAN Translation."

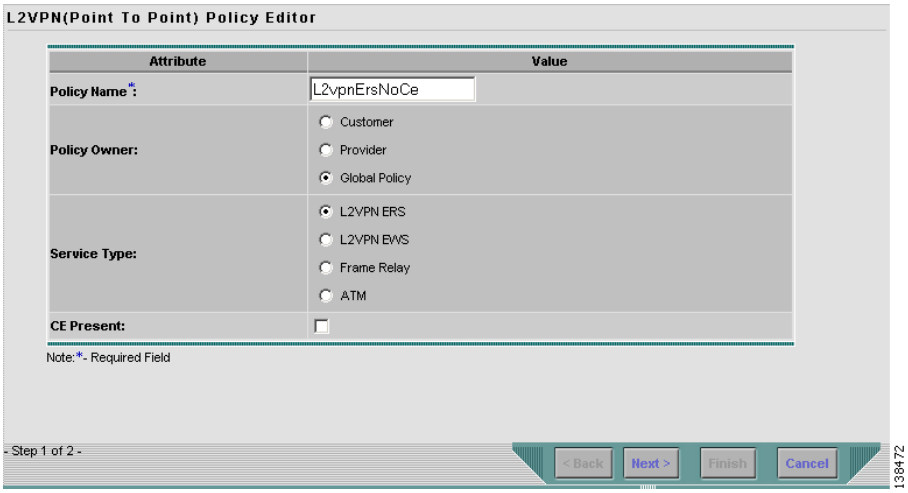
Step 23 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 24 Click **Finish**.

Defining an Ethernet ERS Policy without a CE

This section describes defining an Ethernet ERS policy with out a CE present. Figure 4-6 is an example of the first page of this policy.

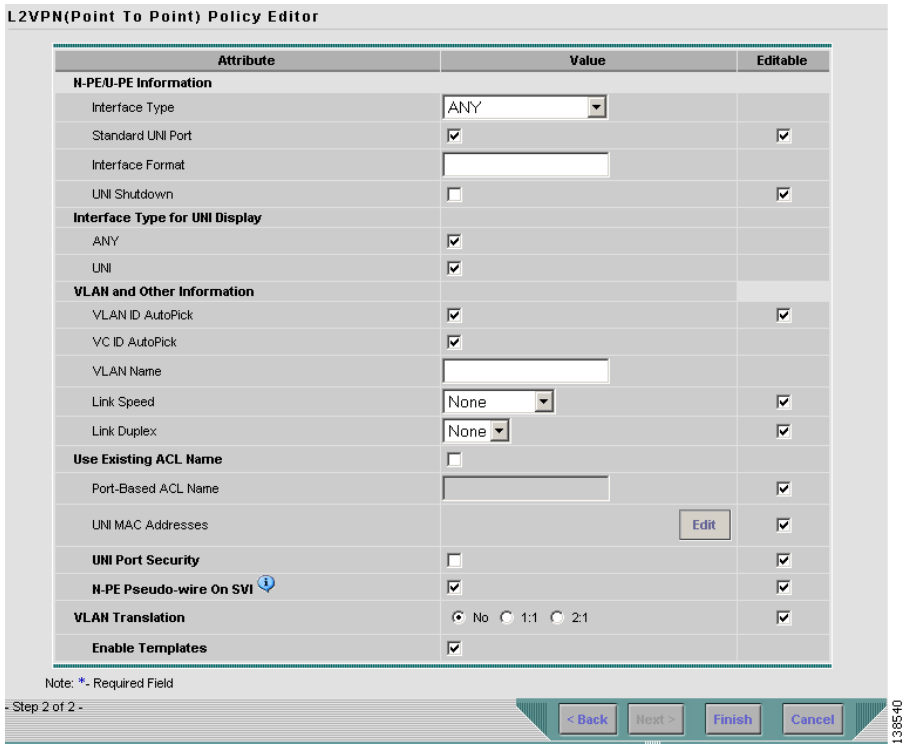
Figure 4-8 Ethernet ERS Policy without a CE



Step 1 Click **Next**. The window in Figure 4-9 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-9 Ethernet ERS without CE Policy Attributes



Step 2 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose to select a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 10 Select the **VC ID AutoPick** check box if you want ISC to choose a VC ID. If you do not select this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 11 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is unselected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 17 Choose a **UNI Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Note Enter a UNI Port Type only if the encapsulation type is DEFAULT.

Step 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-10) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

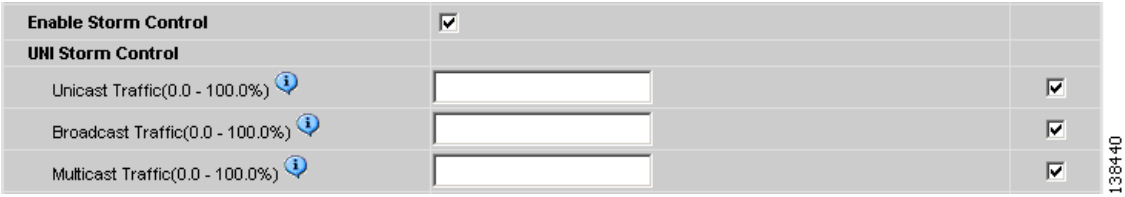
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-10 UNI Port Security

Step 20 Select the **Enable Storm Control** check box (see Figure 4-11) to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 4-11 Enable Storm Control



Step 21 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If you deselect the check box, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 22 Specify the type of **VLAN Translation** for this policy by selecting the appropriate radio button. The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.

Note For detailed coverage of setting up VLAN translation, see Appendix A, "Setting Up VLAN Translation."

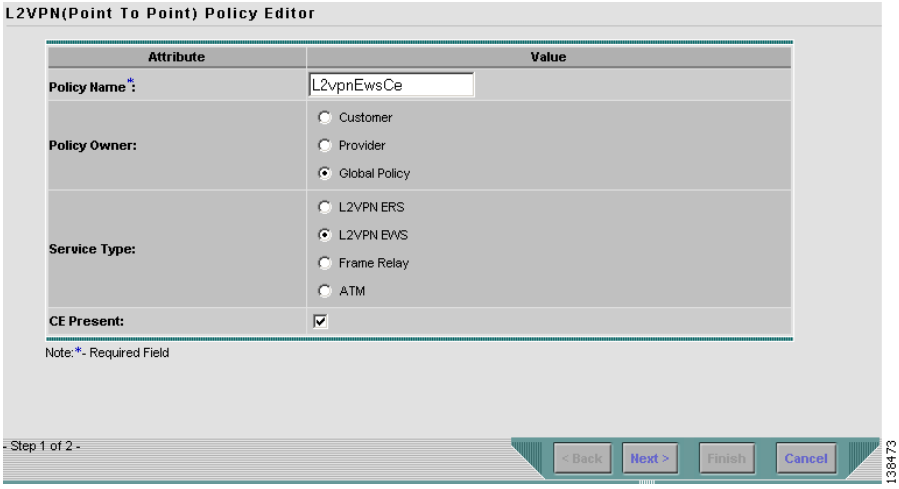
Step 23 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 24 Click **Finish**.

Defining an Ethernet EWS Policy with a CE

This section describes defining an Ethernet EWS policy with CE present. Figure 4-12 is an example of the first page of this policy.

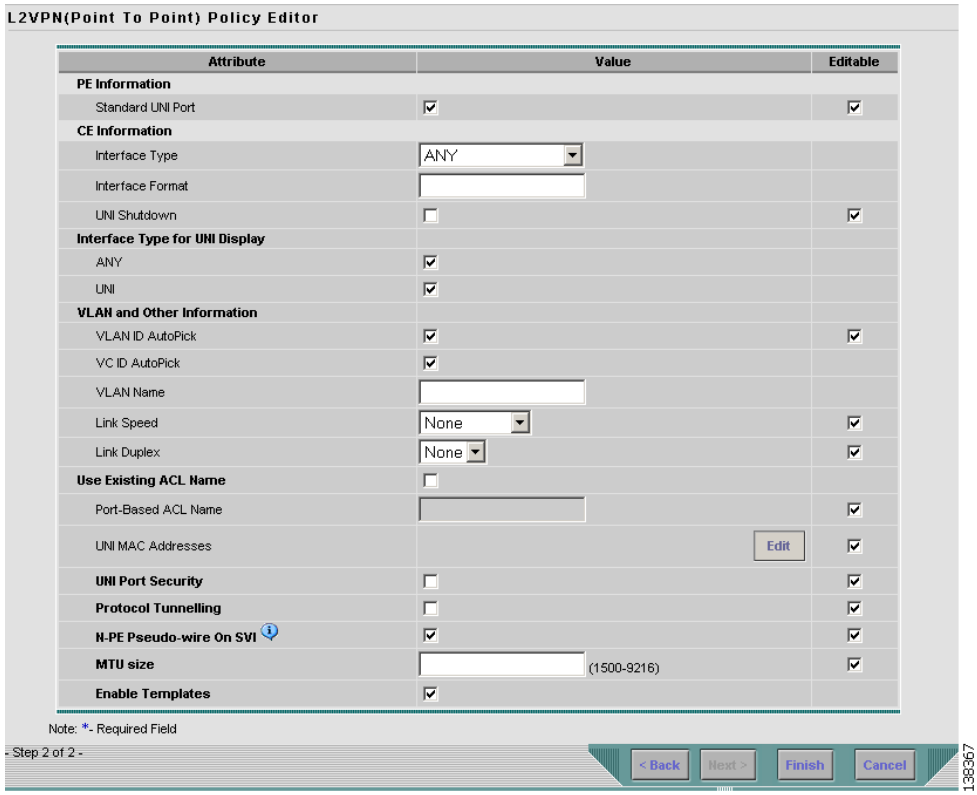
Figure 4-12 Ethernet EWS Policy with a CE



Step 1 Click **Next**. The window in Figure 4-13 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-13 Ethernet EWS with CE Policy Attributes



Step 2 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 3 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a U-PE or N-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 10 Select the **VC ID AutoPick** check box if you want ISC to choose a VC ID. If you do not select this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 11 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 12 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 13 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 14 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 15 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this the check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 16 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 17 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-14) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

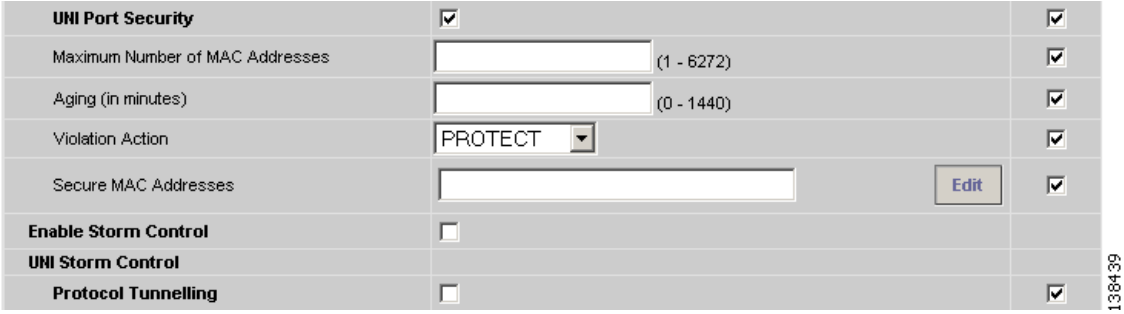
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

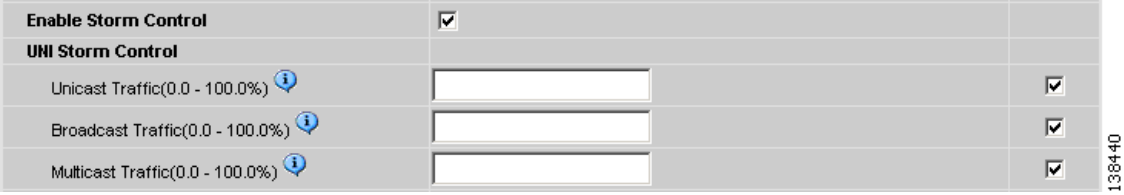
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-14 UNI Port Security



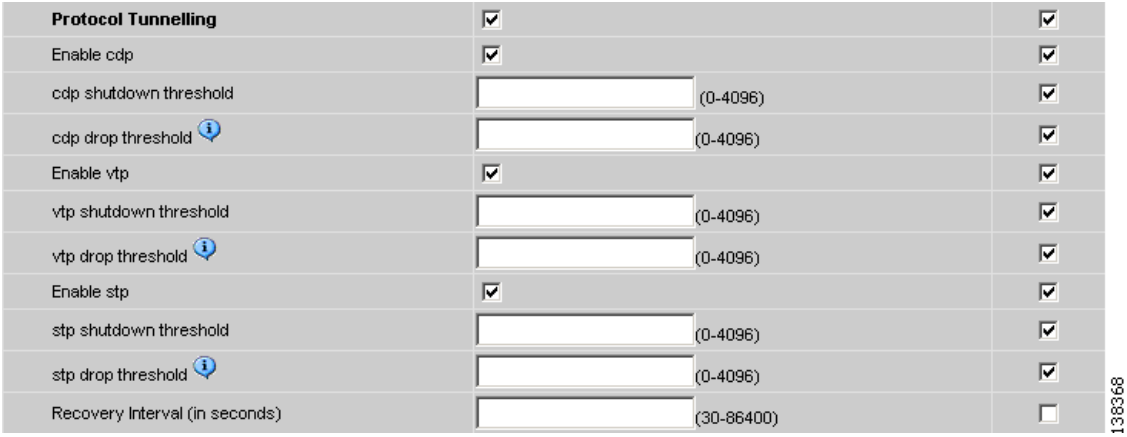
Step 20 Select the **Enable Storm Control** check box (see Figure 4-15) to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 4-15 Enable Storm Control



Step 21 Select the **Protocol Tunnelling** check box (see Figure 4-16) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 4-16 Protocol Tunnelling



For each protocol that you select, enter the shutdown threshold and drop threshold for that protocol:

a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **cdp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Enable stp—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **stp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 22 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 23 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 4.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

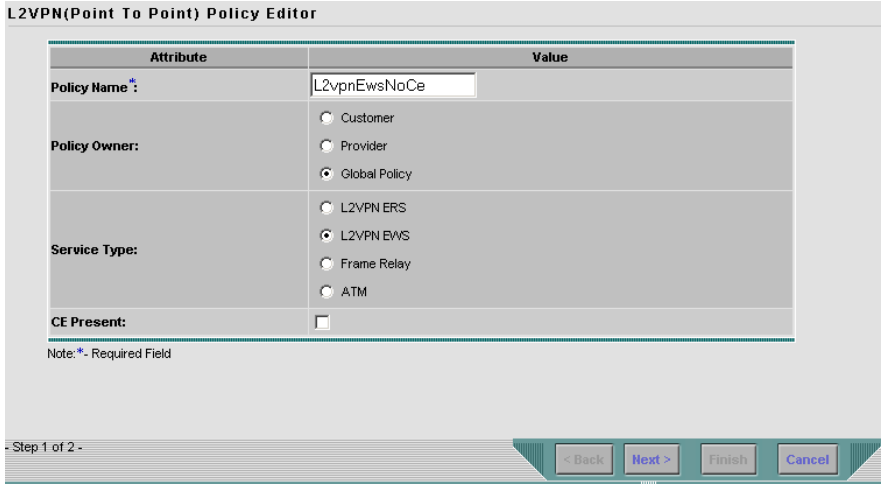
Step 24 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 25 Click **Finish**.

Defining an Ethernet EWS Policy without a CE

This section describes how to define an Ethernet EWS policy without a CE present. Figure 4-17 is an example of the first page of this policy.

Figure 4-17 Ethernet EWS Policy without a CE

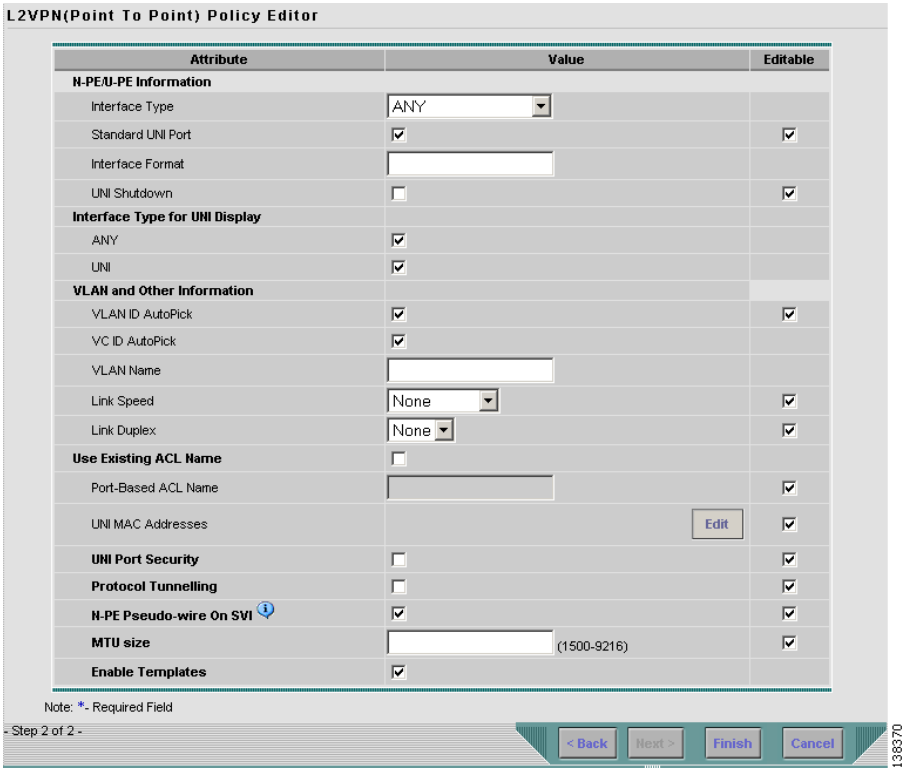


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-18 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-18 Ethernet EWS without CE Policy Attributes



Step 2 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose to select a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is not selected by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is not selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 10 Select the **VC ID AutoPick** check box if you want ISC to choose a VC ID. If you do not select this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 11 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 17 Select the **UNI Port Security** check box (see Figure 4-6) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

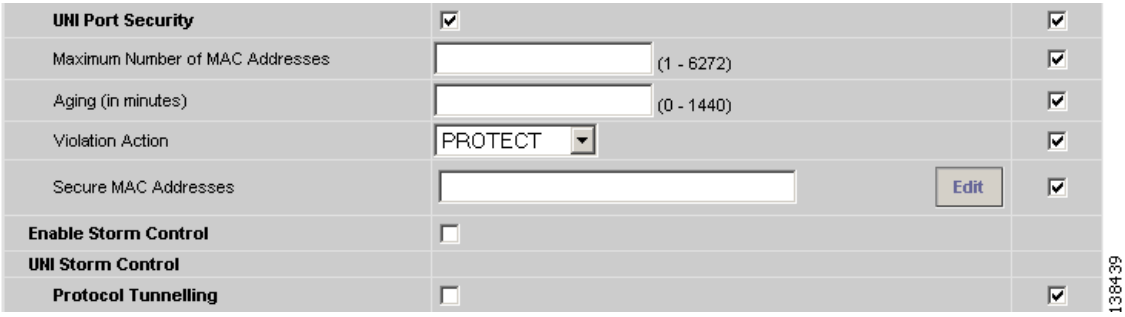
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

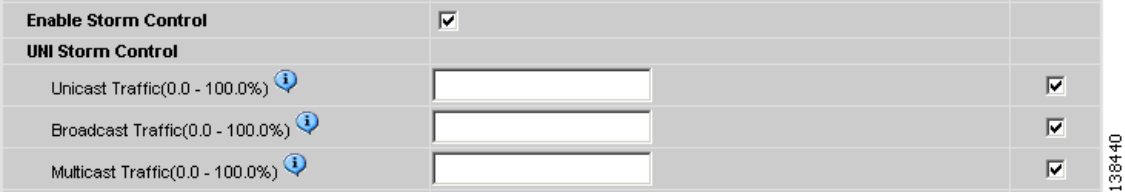
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-19 UNI Port Security



Step 18 Select the **Enable Storm Control** check box (see Figure 4-20) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 4-20 Enable Storm Control



Step 19 Select the **Protocol Tunnelling** check box (see Figure 4-16) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 4-21 Protocol Tunnelling

Protocol Tunnelling	☑		☑
Enable cdp	☑		☑
cdp shutdown threshold		(0-4096)	☑
cdp drop threshold		(0-4096)	☑
Enable vtp	☑		☑
vtp shutdown threshold		(0-4096)	☑
vtp drop threshold		(0-4096)	☑
Enable stp	☑		☑
stp shutdown threshold		(0-4096)	☑
stp drop threshold		(0-4096)	☑
Recovery Interval (in seconds)		(30-86400)	☐

138368

For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **cdp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Enable stp—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **stp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 20 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 21 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 4.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

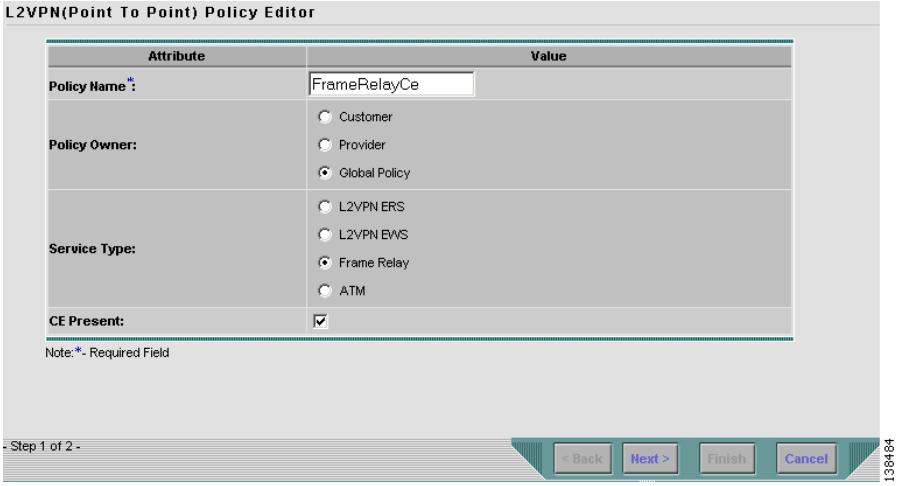
Step 22 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 23 Click **Finish**.

Defining a Frame Relay Policy with a CE

This section describes how to define a Frame Relay policy with CE present. Figure 4-22 is an example of the first page of this policy.

Figure 4-22 Frame Relay Policy with a CE

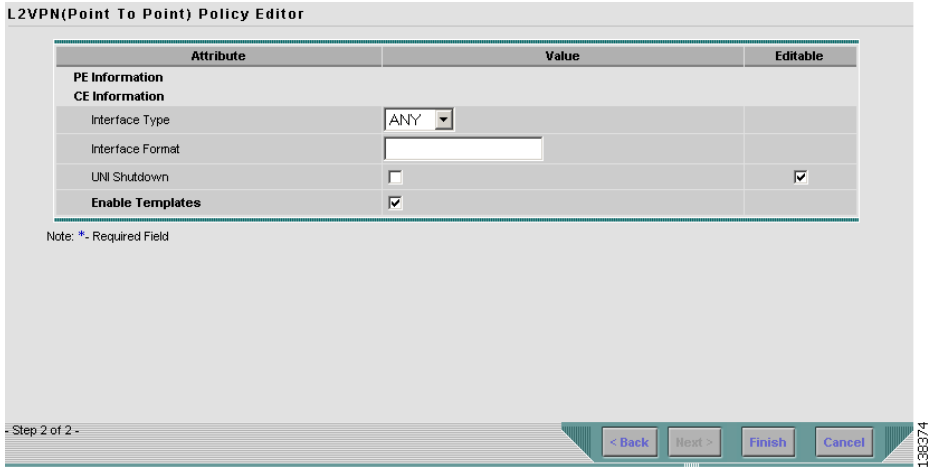


Perform the following steps:

Step 1 Click **Next**. The window in Figure 4-23 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-23 Frame Relay with CE Policy Attributes



Step 2 Choose the **Encapsulation** type for the PE from the drop-down list. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Step 3 Choose the **Interface Type** for the **CE** from the drop-down list. The choices are:

- **ANY**
- **Serial**
- **POS**
- **Hssi**
- **BRI**

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose the CE Encapsulation type. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

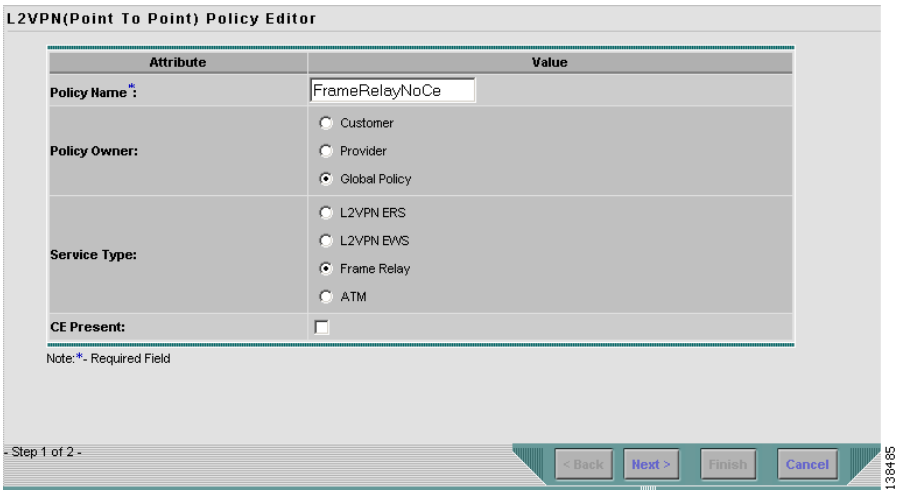
Step 7 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 8 Click **Finish**.

Defining a Frame Relay Policy without a CE

This section describes how to define a Frame Relay policy without a CE present. Figure 4-24 is an example of the first page of this policy.

Figure 4-24 Frame Relay Policy without a CE

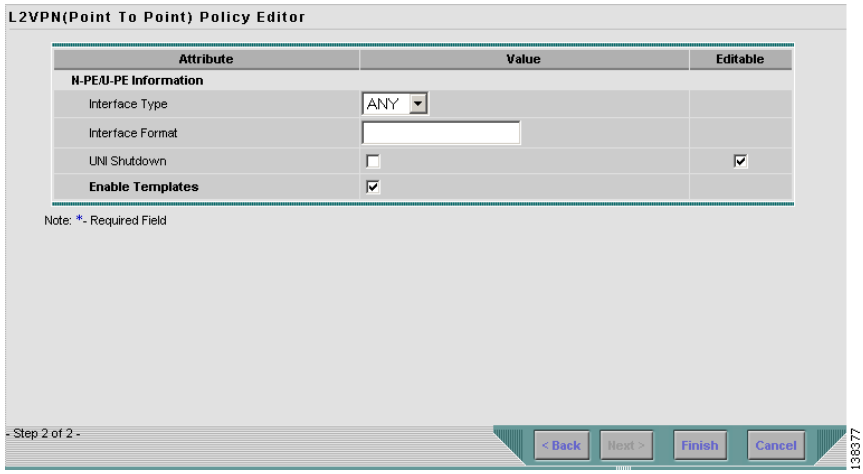


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-25 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-25 Frame Relay without CE Policy Attributes



Step 2 Choose the N-PE/U-PE **Interface Type** for the **CE** from the drop-down list. The choices are:

- **ANY**
- **Serial**
- **POS**
- **Hssi**
- **BRI**

Step 3 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose the N-PE/U-PE **Encapsulation** type. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

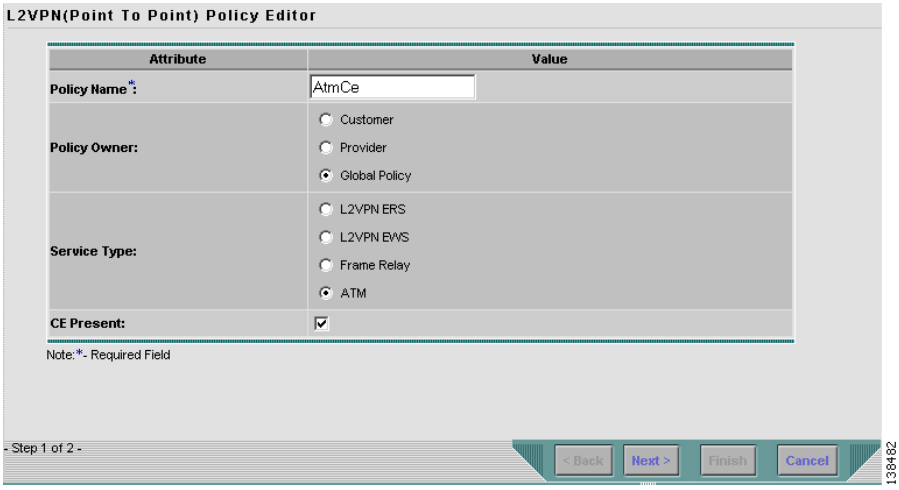
Step 6 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 7 Click **Finish**.

Defining an ATM Policy with a CE

This section describes how to define an AMT policy with CE present. Figure 4-26 is an example of the first page of this policy.

Figure 4-26 ATM Policy with a CE

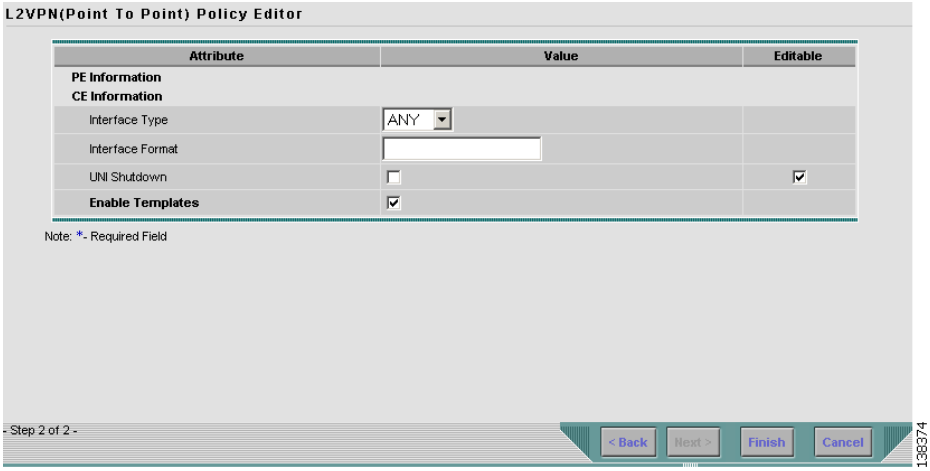


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-27 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-27 ATM with CE Policy Attributes



Step 2 Choose the **PE Encapsulation** type from the drop-down list. The choices are:

- **AAL5**
- **AAL0**

Step 3 Choose the **CE Interface Type** from the drop-down list. The choices are:

- **ANY**
- **ATM**
- **Switch**

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a **CE Encapsulation**. The choices are:

- **AAL5SNAP**
- **AAL5MUX**
- **AAL5NLPID**
- **AAL2**

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

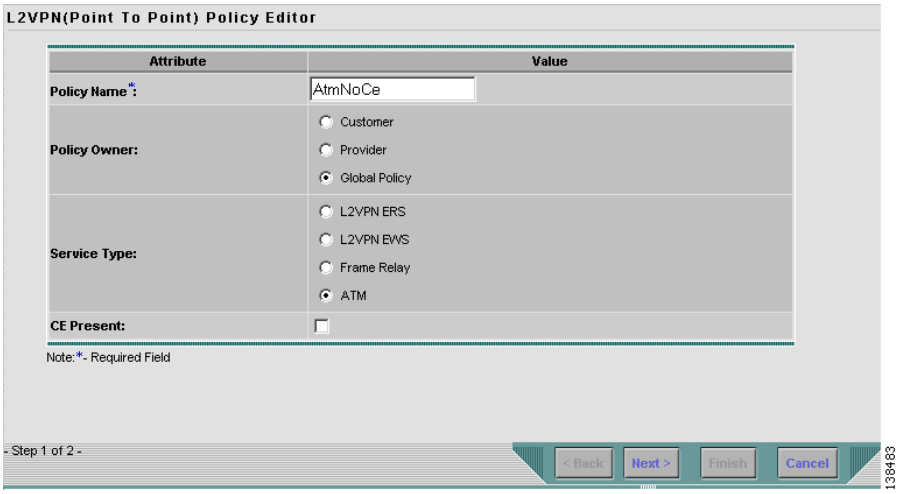
Step 7 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 8 Click **Finish**.

Defining an ATM Policy without a CE

This section describes how to define an AMT policy without a CE present. Figure 4-28 is an example of the first page of this policy.

Figure 4-28 ATM Policy without a CE

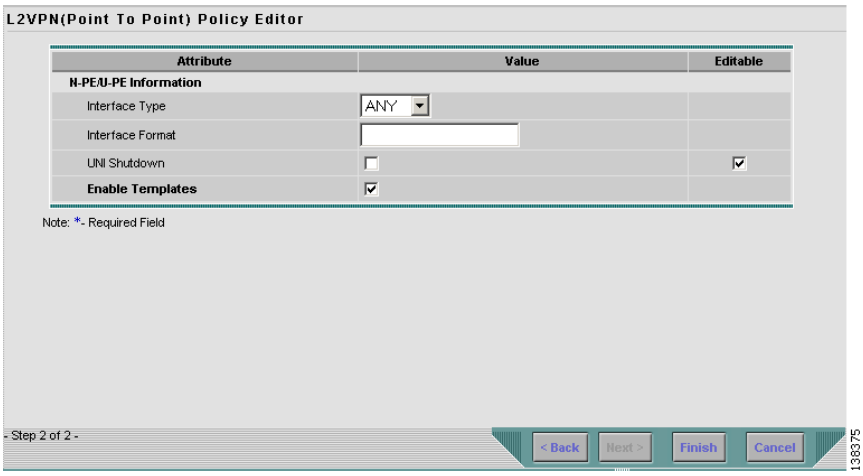


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-29 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 4-29 ATM without CE Policy Attributes



Step 2 Choose the **N-PE/U-PE Interface Type** from the drop-down list. The choices are:

- **ANY**
- **ATM**
- **Switch**

Step 3 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose a **PE Encapsulation**. The choices are:

- **AAL5**
- **AAL0**

Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 7 Click **Finish**.

Managing an L2VPN Service Request

This chapter covers the basic steps to provision an L2VPN service. It contains the following sections:

Introducing L2VPN Service Requests

An L2VPN service request consists of one or more end-to-end wires, connecting various sites in a point-to-point topology. When you create a service request, you enter several parameters, including the specific interfaces on the CE and PE routers.

Note If you are creating an L2TPv3 service request, see Chapter 7, "Introducing L2TPv3 Service Requests."

You can also integrate a Cisco IP Solution Center (ISC) template with a service request. You can associate one or more templates to the CE and the PE.

To create a service request, a Service Policy must already be defined, as described in Chapter 4, "Creating an L2VPN Policy".

Based on the predefined L2VPN policy, an operator creates an L2VPN service request, with or without modifications to the L2VPN policy, and deploys the service. Service creation and deployment are normally performed by regular network technicians for daily operation of network provisioning.

The following steps are involved in creating a service request for Layer 2 connectivity between customer sites:

- Choose a CE Topology for ERS/Frame Relay/ATM services.
- Select the endpoints (CE and PE) that must be connected. For each end-to-end Layer 2 connection, ISC creates an end-to-end wire object in the repository for the service request.
- Choose a CE or PE interface.

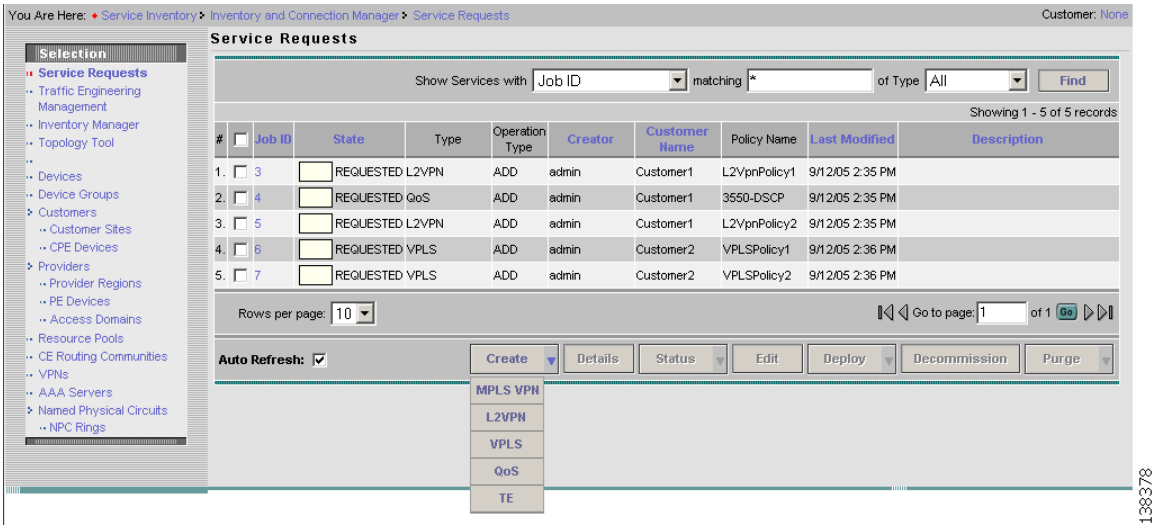
- Choose a Named Physical Circuit (NPC) for the CE or PE.
- Edit the end-to end connection.
- Edit the link attributes.

Creating an L2VPN Service Request

Perform the following steps to create an L2VPN service request.

Step 1 Select **Service Inventory > Inventory and Connection Manage > Service Requests**. The Service Requests window appears as shown in Figure 5-1.

Figure 5-1 L2VPN Service Activation



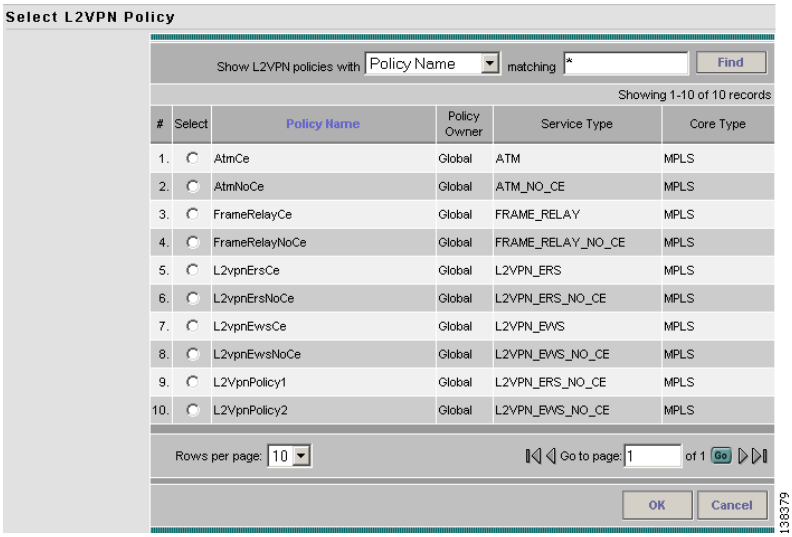
Step 2 Click **Create**.

Step 3 Choose **L2VPN** from the drop-down list.

L2VPN service requests must be associated with an L2VPN policy. You choose an L2VPN policy from the policies previously created (see Chapter 4, "Creating an L2VPN Policy").

Step 4 Select the L2VPN policy of choice. See Figure 5-2. If more than one L2VPN policy exists, a list of L2VPN policies appears.

Figure 5-2 L2VPN Policy Choice



Step 5 When you make the choice, click **OK**.

As soon as you make the choice, the new service request inherits all the properties of that L2VPN policy, such as all the editable and non-editable features and pre-set parameters.

To continue creating an L2VPN service request, go to one of the following sections:

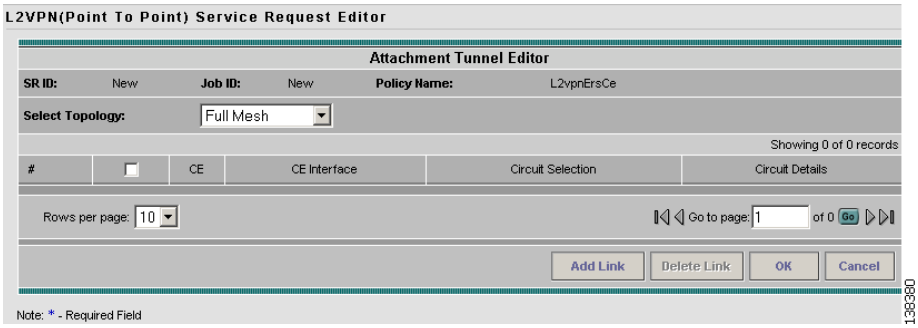
- Creating an L2VPN Service Request with a CE, page 5-3.
- Creating an EWS L2VPN Service Request with a CE, page 5-10.
- Creating an L2VPN Service Request without a CE, page 5-13.
- Creating an EWS L2VPN Service Request without a CE, page 5-17.

Creating an L2VPN Service Request with a CE

This section includes detailed steps for creating an L2VPN service request with a CE present for ERS, ATM, and Frame Relay policies. If you are creating an L2VPN service request for an EWS policy, go to Creating an EWS L2VPN Service Request with a CE, page 5-10.

After you choose an L2VPN policy, the L2VPN Service Request Editor window appears (see Figure 5-3).

Figure 5-3 L2VPN Service Request Editor



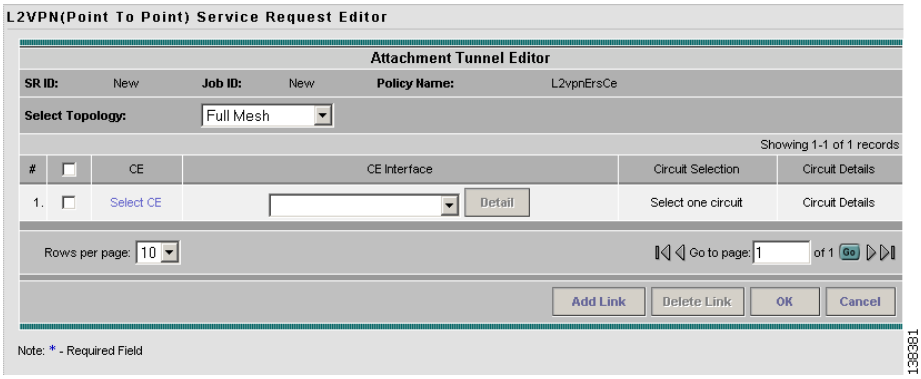
Step 1 Choose a **Topology** from the drop-down list. If you choose **Full Mesh**, each CE will have direct connections to every other CE. If you choose **Hub and Spoke**, then only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other.

Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two end points. For example, with four end points, ISC automatically creates six links with full mesh topology. With hub and spoke topology, however, ISC creates only three links.

Step 2 Click **Add Link**.

You specify the CE end points using the Attachment Tunnel Editor. You can create one or more CEs from a window like the one in Figure 5-4.

Figure 5-4 Select CE



Note All the services that deploy point-to-point connections (ERS, EWS, ATMoMPLS, and FRoMPLS) must have at least two CEs specified.

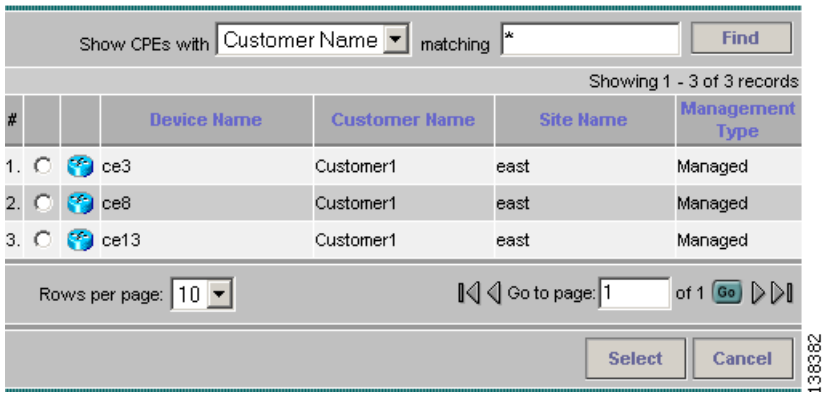
Step 3 Click **Select CE** in the CE column. The CPE for Attachment Circuit window appears (see Figure 5-5). This window displays the list of currently defined CEs.

a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.

b. You can use the **Find** button to either search for a specific CE, or to refresh the display.

c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Figure 5-5 Select CPE Device



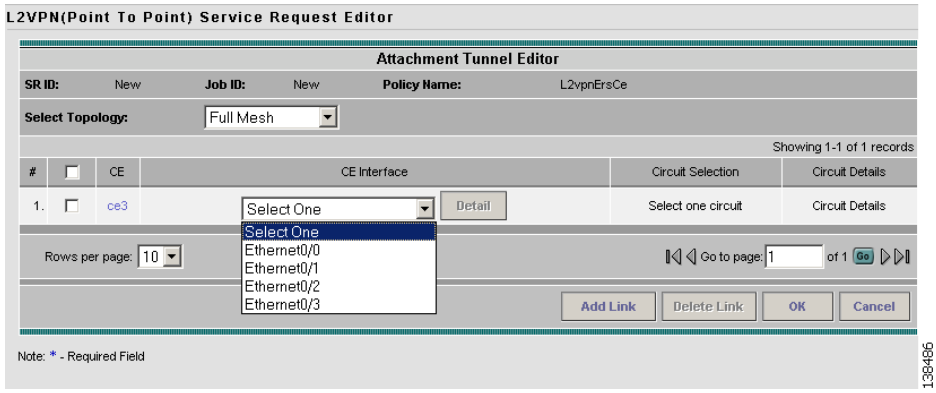
Step 4 In the Select column, choose a CE for the L2VPN link.

Step 5 Click **Select**.

The Service Request Editor window appears displaying the name of the selected CE in the CE column.

Step 6 Select the CE interface from the drop-down list (see Figure 5-6).

Figure 5-6 Select the CE Interface



Note When you provision an L2VPN ERS service, when you select a UNI for a particular device, ISC determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

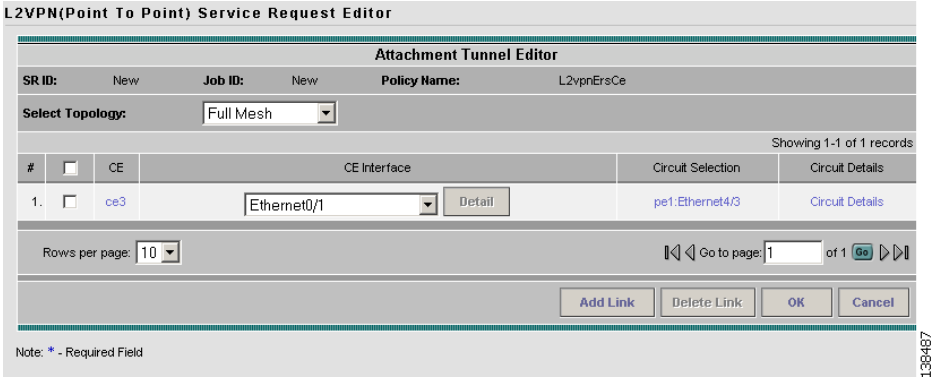
Note ISC only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.

Step 7 If only one NPC exists for the Chosen CE and CE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly. If more then one NPC is available, click **Select one circuit** in the Circuit Selection column. The NPC window appears, enabling you to select the appropriate NPC.

Step 8 Click **OK**.

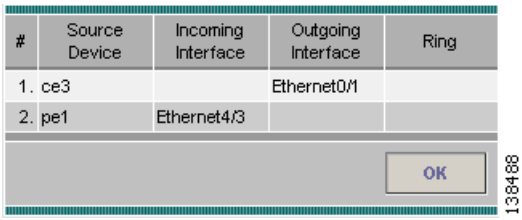
Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection** as in Figure 5-7. This means that you do not have to further specify the PE to complete the link.

Figure 5-7 NPC Created



If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC. In Figure 5-8, the CE and PE and their corresponding interfaces appear.

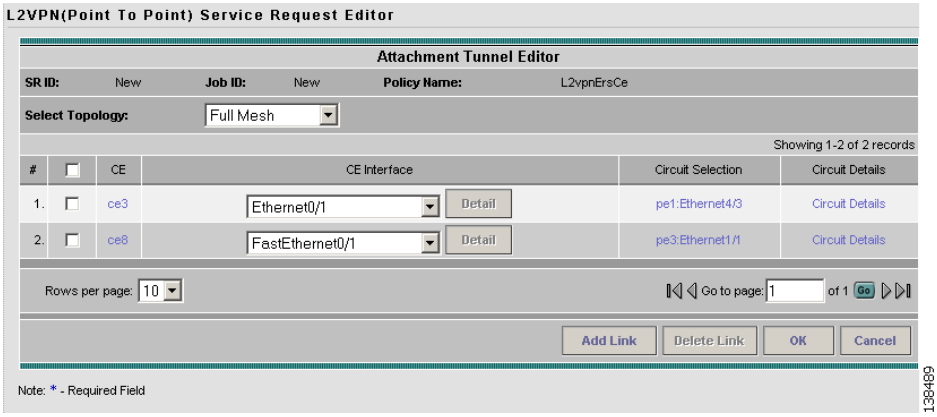
Figure 5-8 NPC Details



Step 9 Continue to specify additional CEs, as in previous steps. ISC creates the links between CEs based on the Topology that you chose.

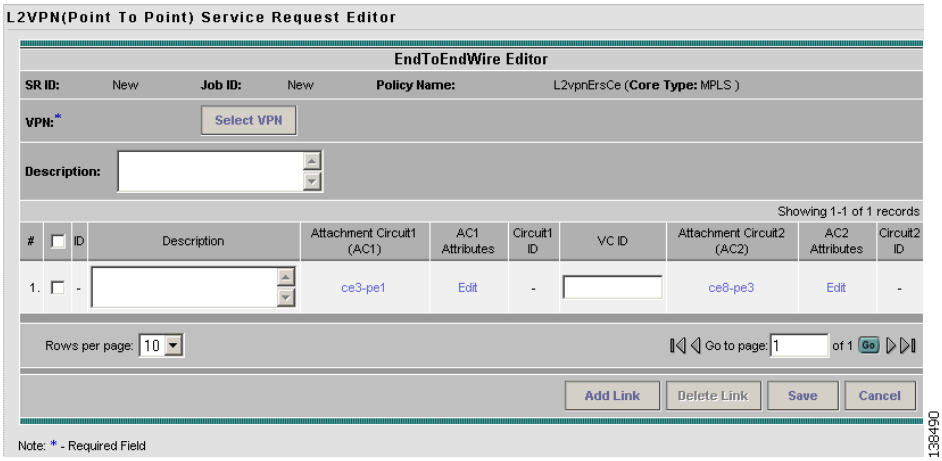
Step 10 Click **OK** in Figure 5-9.

Figure 5-9 NPCs Created



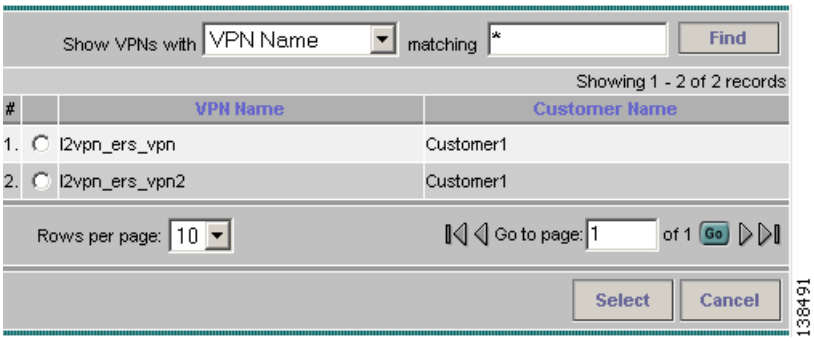
For ERS, ATM, and Frame Relay, the End-to-End Wire Editor window appears as shown in Figure 5-10.

Figure 5-10 End-to-End Wire Editor



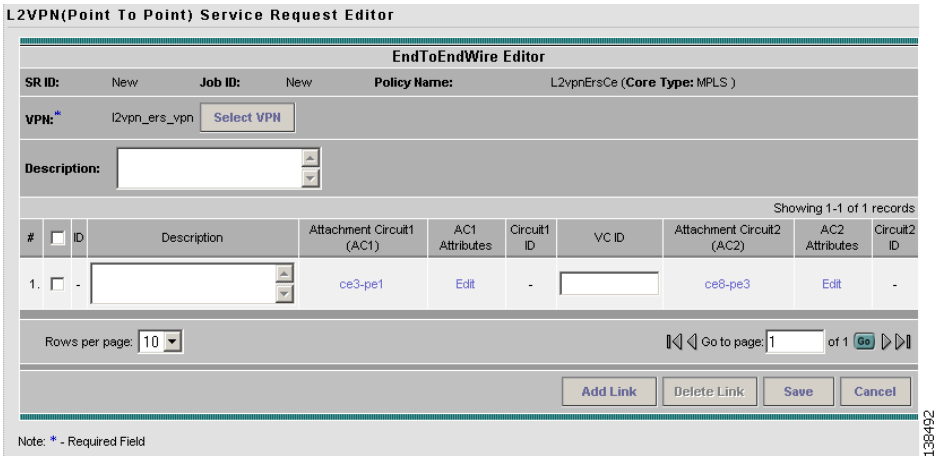
Step 11 The VPN for this service request appears in the **VPN** field. If there is more than one VPN, click **Select VPN** to choose a VPN. The VPN for L2VPN service request window appears as shown in Figure 5-11.

Figure 5-11 Select VPN for L2VPN Service Request



Step 12 Choose a **VPN Name** and click **Select**. The L2VPN Service Request Editor window appears with the VPN name displayed as shown in Figure 5-12.

Figure 5-12 Attachment Circuit Selection

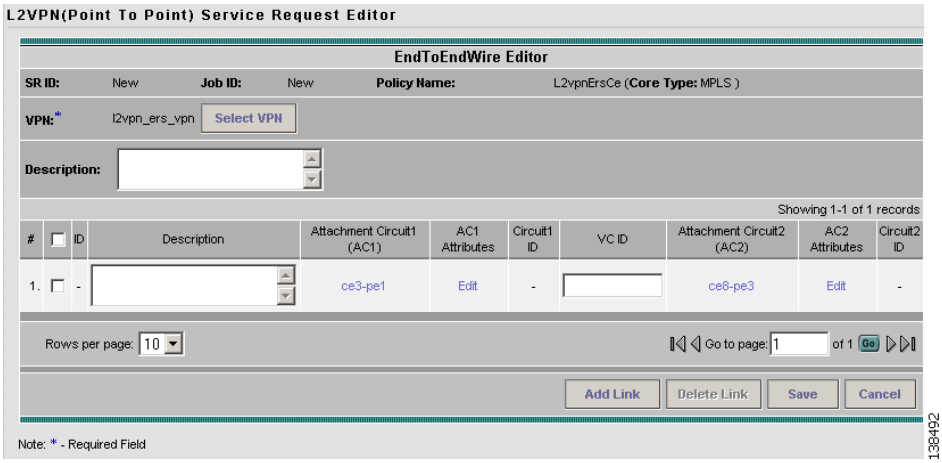


Step 13 Click **Add AC** in the Attachment Circuit AC2 column.

Step 14 Repeat Steps 3 to 10 for AC2.

The End-to-End Wire Editor window displays the complete end-to-end wire as shown in Figure 5-13.

Figure 5-13 End-to-End Wire Created



You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can edit the AC link attributes to change the default policy settings. After you edit these fields, the blue link changes from Default to Changed.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

If the policy was set up for you to define a VC ID manually, enter it into the empty **VC ID** field. If policy was set to “auto pick” the VC ID, ISC will supply a VC ID, and this field will not be editable. In the case where you supply the VC ID manually, if the entered value is in the provider’s range, ISC validates if the entered value is available or allocated. If the entered value has been already allocated, ISC generates an error message saying that the entered value is not available and prompts you to re-enter the value. If the entered value is in the provider’s range, and if it is available, then it is allocated and is removed from the VC ID pool. If the entered value is outside the provider’s range, ISC displays a warning saying that no validation could be performed to verify if it is available or allocated.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

Step 15 When you are finished editing the end-to-end wires, click **Save**.

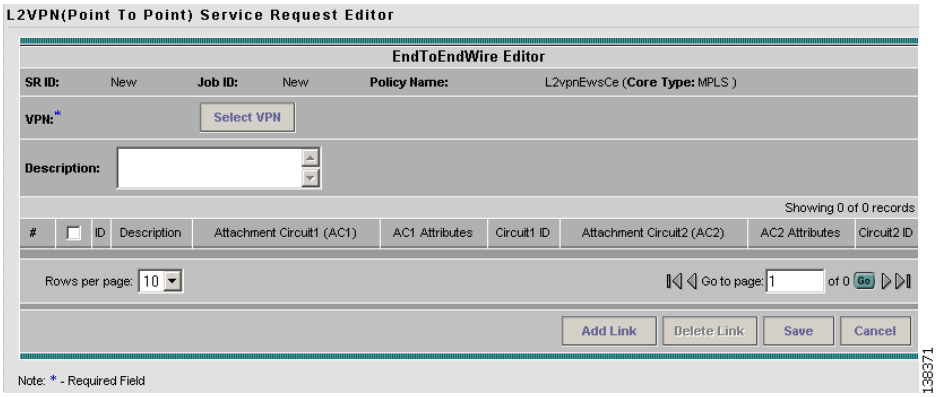
The service request is created and saved into ISC.

Creating an EWS L2VPN Service Request with a CE

This section includes detailed steps for creating an L2VPN service request with a CE present for EWS. If you are creating an L2VPN service request for an ERS, ATM, or Frame Relay policy, go to Creating an L2VPN Service Request with a CE, page 5-3.

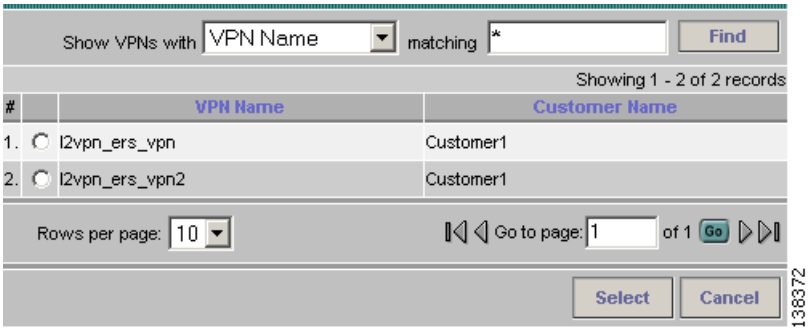
After you choose an L2VPN policy, the L2VPN Service Request Editor window appears (see Figure 5-14).

Figure 5-14 EWS Service Request Editor



Step 1 Click **Select VPN** to select a VPN for use with this CE. The Select VPN window appears with the VPNs defined in the system. See Figure 5-15.

Figure 5-15 Select a VPN

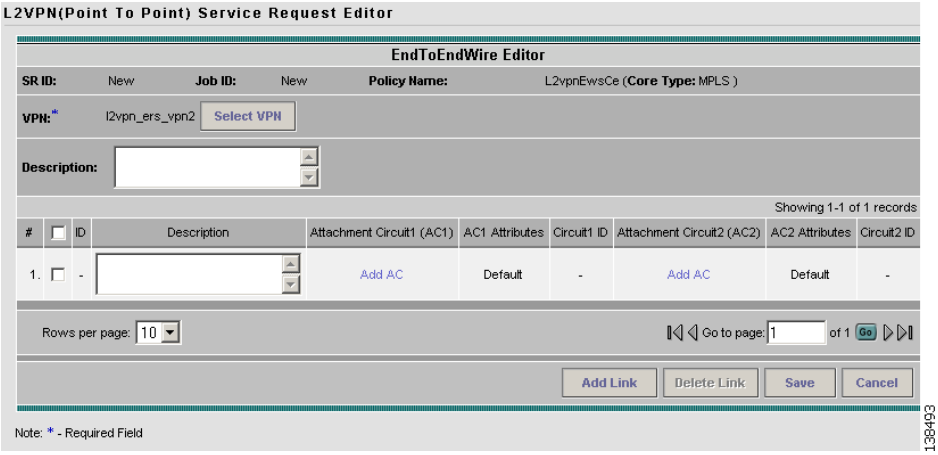


Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**. The L2VPN Service Request Editor window appears with the VPN name displayed.

Step 4 Click **Add Link**. See Figure 5-16.

Figure 5-16 End-To-End Wire Editor



Step 5 Click **Add AC** in the Attachment Circuit (A1) column. The Attachment Tunnel Editor appears as shown in Figure 5-17.

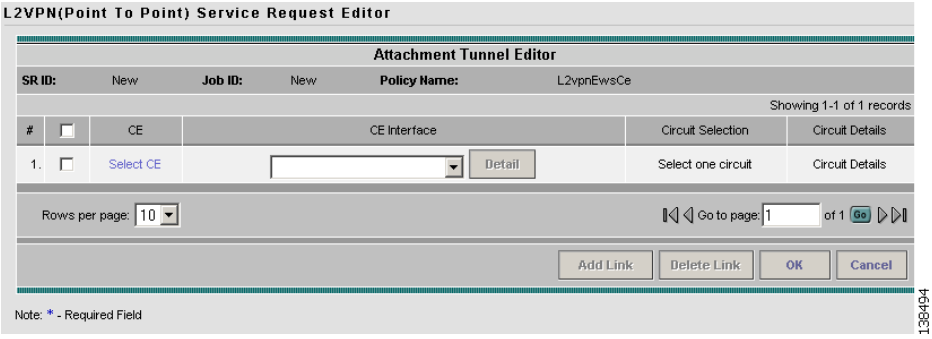
You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Figure 5-17 Select CE for Attachment Circuit



Step 6 Click **Select CE**. The CPE for Attachment Circuit window appears as shown in Figure 5-18.

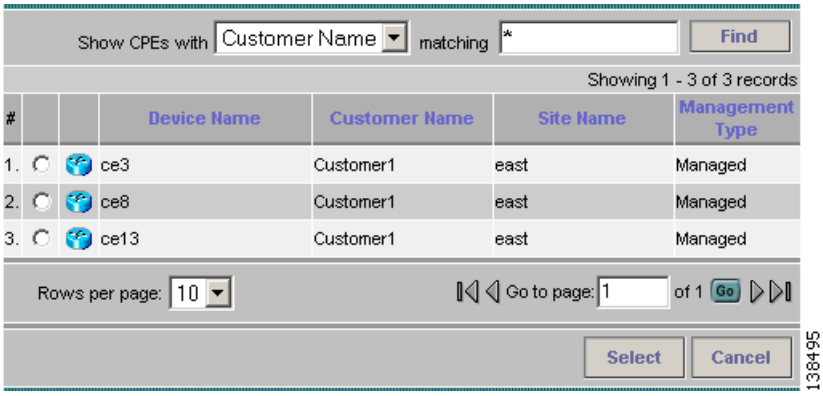
This window displays the list of currently defined CEs.

a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.

b. You can use the **Find** button to either search for a specific CE, or to refresh the display.

c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Figure 5-18 CPE for Attachment Circuit



Step 7 In the Select column, choose a CE for the L2VPN link.

Step 8 Click **Select**.

Step 9 Choose a CE interface from the drop-down list.

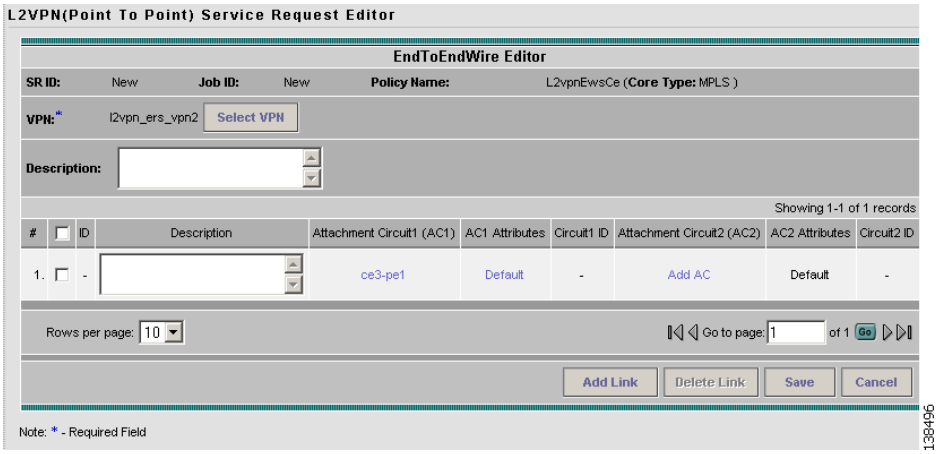
Step 10 If only one NPC exists for the Chosen CE and CE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly. If more then one NPC is available, click **Select one circuit** in the Circuit Selection column. The NPC window appears, enabling you to select the appropriate NPC.

Step 11 Click **OK**.

Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection** as in Figure 5-19. This means that you do not have to further specify the PE to complete the link.

Step 12 Click **OK**.

Figure 5-19 NPC Created



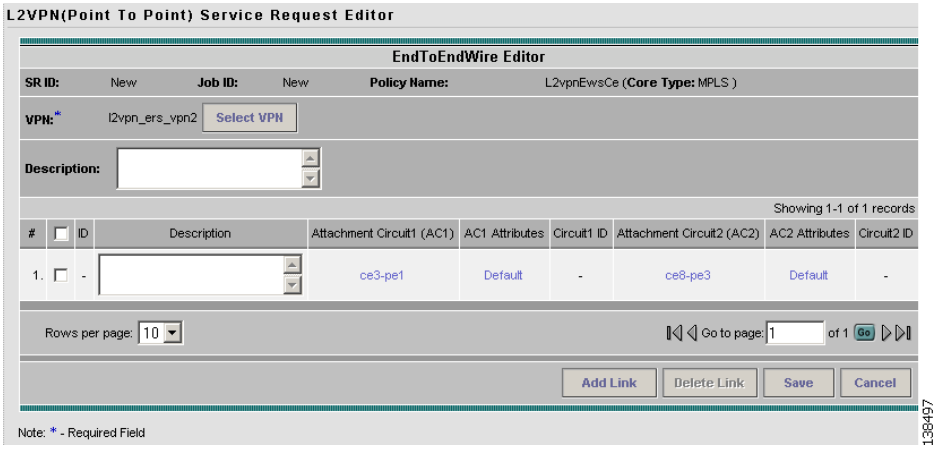
Step 13 The Service Request Editor window appears displaying the name of the selected CE in the AC1 column.

Step 14 Click **AC1** Link Attributes and edit the attributes if desired (see the Modifying the L2VPN Service Request, page 5-22). Click **OK**.

Step 15 Repeat Steps 5 through 14 for **AC2**.

Step 16 Click **OK**. You see a screen like Figure 5-20.

Figure 5-20 Attachment Circuits Selected



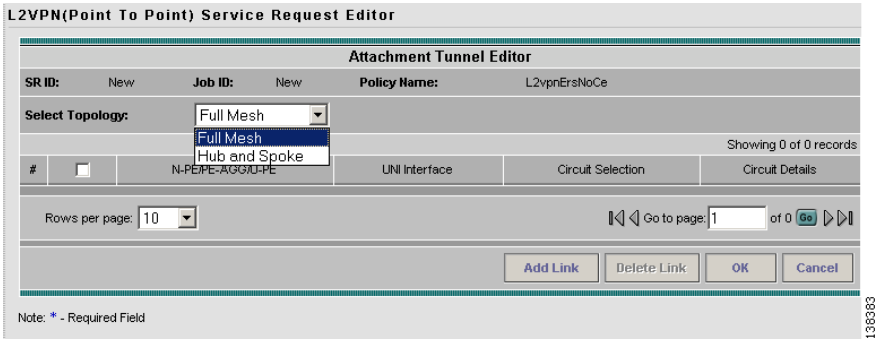
Step 17 Click **Save**. The EWS service request is created and saved in ISC.

Creating an L2VPN Service Request without a CE

This section includes detailed steps for creating an L2VPN service request without a CE present for ERS, ATM, and Frame Relay policies. If you are creating an L2VPN service request for an EWS policy, go to the Creating an EWS L2VPN Service Request without a CE, page 5-17.

After you choose an L2VPN policy, the L2VPN Service Request Editor window appears (see Figure 5-21).

Figure 5-21 L2VPN Service Request Editor



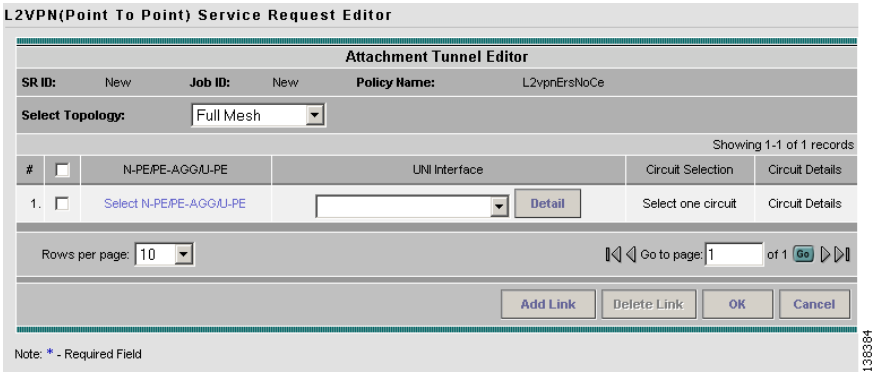
Step 1 Choose a **Topology** from the drop-down list. If you choose **Full Mesh**, each CE will have direct connections to every other CE. If you choose **Hub and Spoke**, then only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other.

Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two endpoints. For example, with four endpoints, ISC automatically creates six links with full mesh topology. With hub and spoke topology, however, ISC creates only three links.

Step 2 Click **Add Link**.

You specify the N-PE/PE-AGG/U-PE endpoints using the Attachment Tunnel Editor. You can create one or more PEs from a window like the one in Figure 5-22.

Figure 5-22 Select U-PE/PE-AGG/N-PE



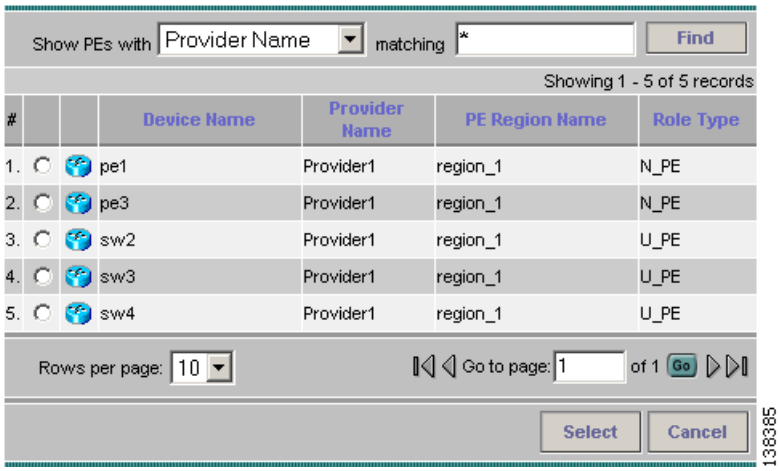
Step 3 Click **Select U-PE/PE-AGG/N-PE** in the U-PE/PE-AGG/N-PE column. The PE for Attachment Circuit window appears (see Figure 5-23). This window displays the list of currently defined PEs.

a. The **Show PEs with** drop-down list shows PEs by customer name, by site, or by device name.

b. The **Find** button allows a search for a specific PE or a refresh of the window.

c. The **Rows per page** drop-down list allows the page to be set to 5, 10, 20, 30, 40, or All.

Figure 5-23 Select PE Device



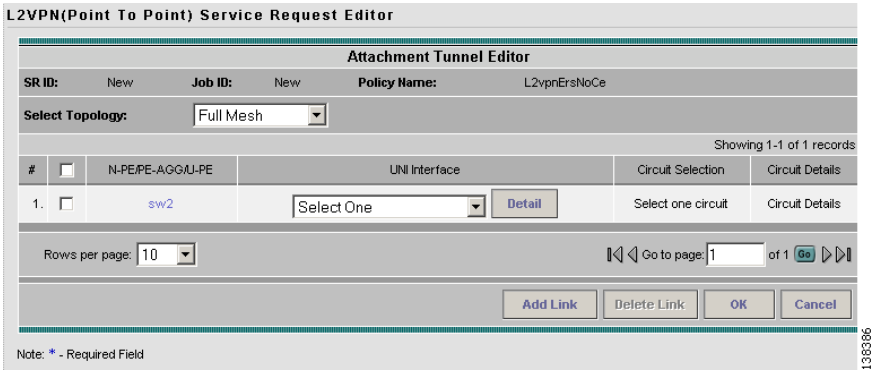
Step 4 In the **Select** column, choose the PE device name for the L2VPN link.

Step 5 Click **Select**.

The Service Request Editor window appears displaying the name of the selected PE in the PE column.

Step 6 Select the UNI interface from the drop-down list (see Figure 5-24).

Figure 5-24 Select the UNI Interface



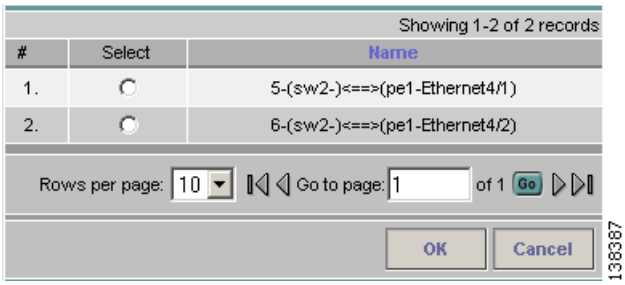
Note When you provision an L2VPN ERS service, when you select a UNI for a particular device, ISC determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

Note ISC only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.

Step 7 If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column. The NPC window appears (see Figure 5-25). If only one NPC exists for the Chosen PE and PE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly.

Note If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

Figure 5-25 Select NPC

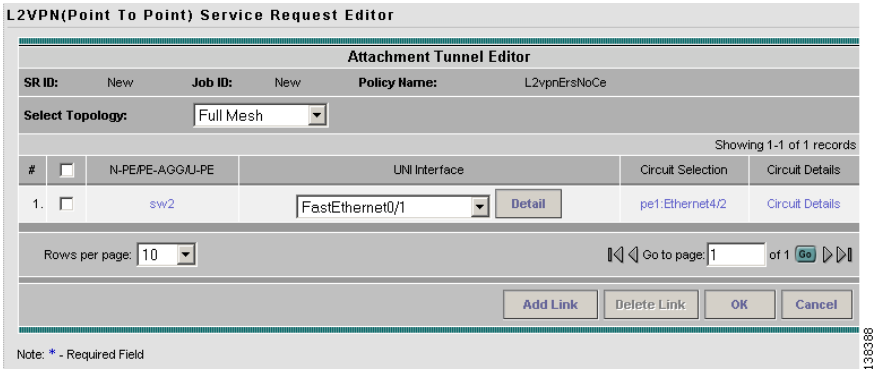


Step 8 Choose the name of the NPC from the **Select** column.

Step 9 Click **OK**.

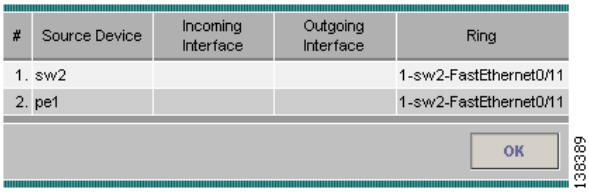
Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection** as in Figure 5-26. This means that you do not have to further specify the PE to complete the link.

Figure 5-26 NPC Created



Step 10 If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC. In Figure 5-27, the CE and PE and their corresponding interfaces appear.

Figure 5-27 NPC Details



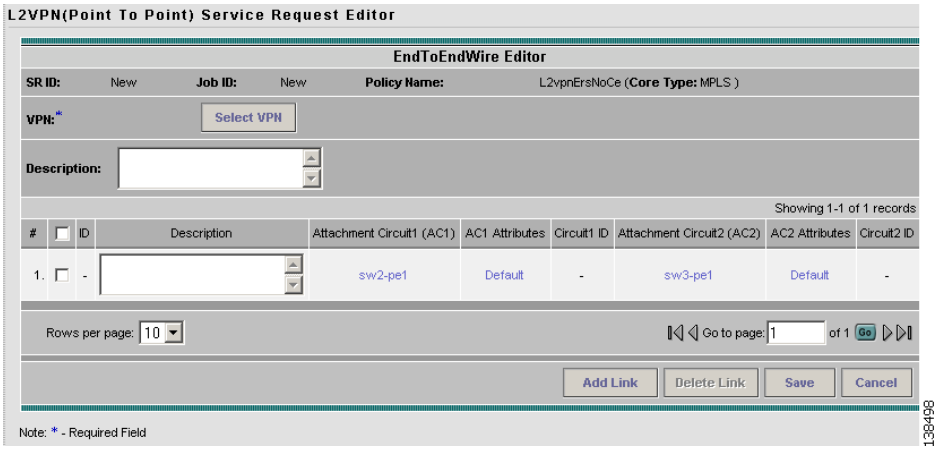
After you specify all the PEs, ISC creates the links between PEs based on the Topology that you chose.

Step 11 Click **OK**. The Attachment Tunnel Editor window appears. See Figure 5-26.

Step 12 Click **OK**.

Step 13 For ERS, ATM, and Frame Relay, the End-to-End-Wire Editor window appears as shown in Figure 5-28.

Figure 5-28 End-to-End Wire Editor



Step 14 The VPN for this service request appears in the Select VPN field. If there is more than one VPN, click **Select VPN** to choose a VPN.

You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can edit the AC link attributes to change the default policy settings. After you edit these fields, the blue link changes from Default to Changed.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 15 When you are finished editing the end-to-end wires, click **Save**.

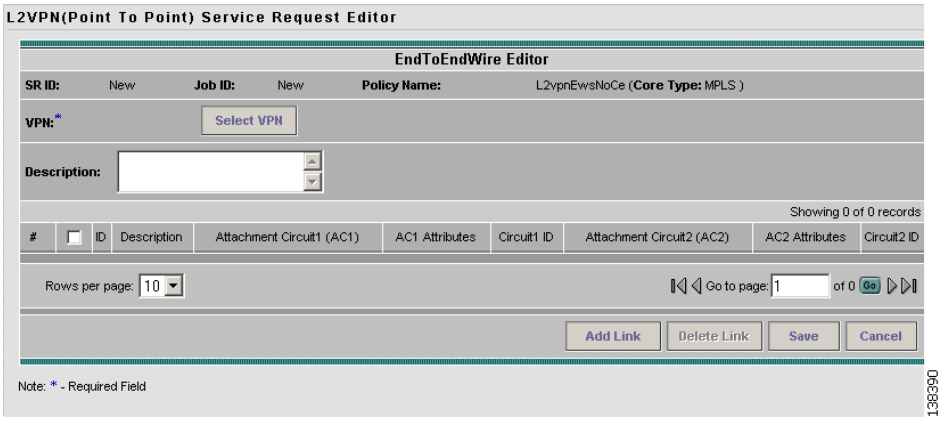
The service request is created and saved into ISC.

Creating an EWS L2VPN Service Request without a CE

This section includes detailed steps for creating an L2VPN service request without a CE present for EWS. If you are creating an L2VPN service request for an ERS, ATM, or Frame Relay policy, see Creating an L2VPN Service Request without a CE, page 5-13.

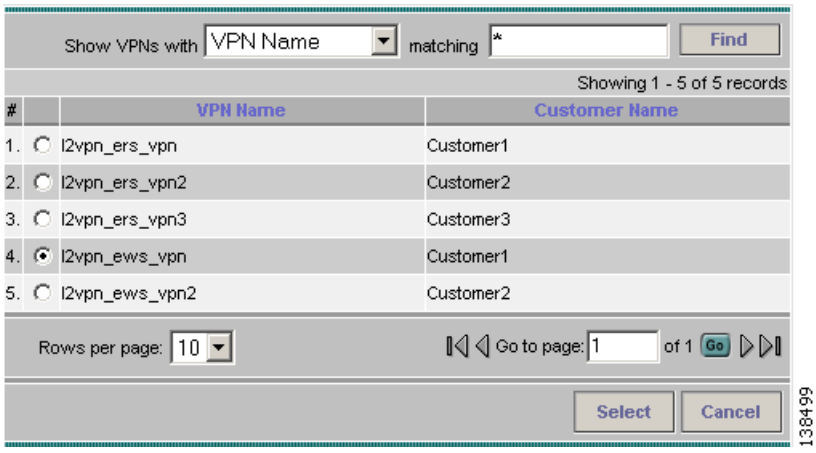
After you choose an L2VPN policy, the L2VPN Service Request Editor window appears (see Figure 5-29).

Figure 5-29 EWS Service Request Editor



Step 1 Click **Select VPN** to select a VPN for use with this PE. The Select a VPN window appears with the VPNs defined in the system. See Figure 5-30.

Figure 5-30 Select a VPN

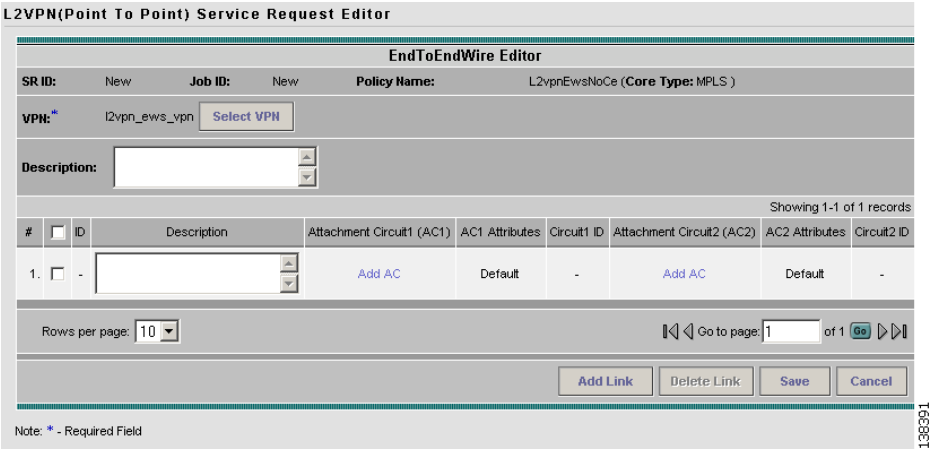


Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**. The L2VPN Service Request Editor window appears with the VPN name displayed.

Step 4 Click **Add Link**. See Figure 5-31.

Figure 5-31 End-To-End Wire Editor



You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

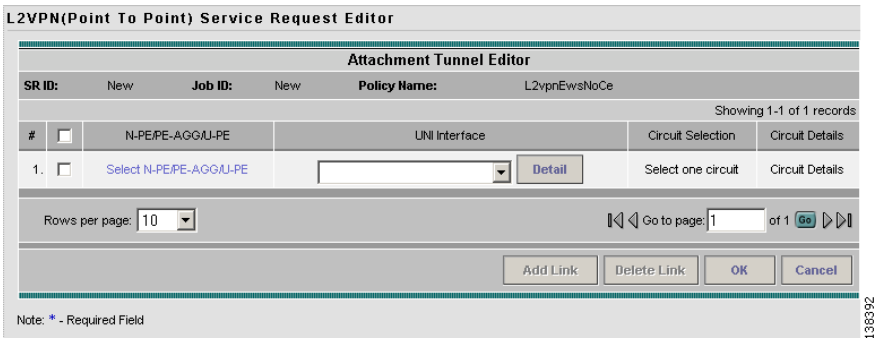
You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 5 Click **Add AC** in the Attachment Circuit (AC1) column. See Figure 5-32.

Figure 5-32 Select the PE for the Attachment Circuit



Step 6 Click **Select N-PE/PE-AGG/U-PE**. The PE for Attachment Circuit window appears as shown in Figure 5-33.

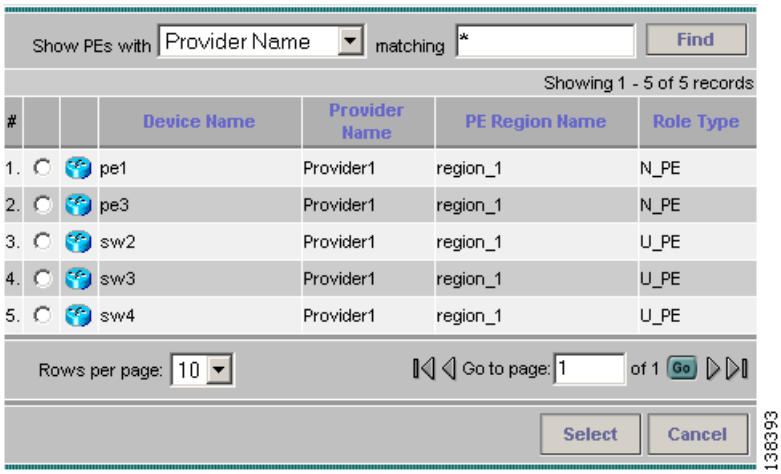
This window displays the list of currently defined PEs.

a. From the **Show PEs with** drop-down list, you can display PEs by Customer Name, by Site, or by Device Name.

b. You can use the **Find** button to either search for a specific PE, or to refresh the display.

c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Figure 5-33 PE for Attachment Circuit

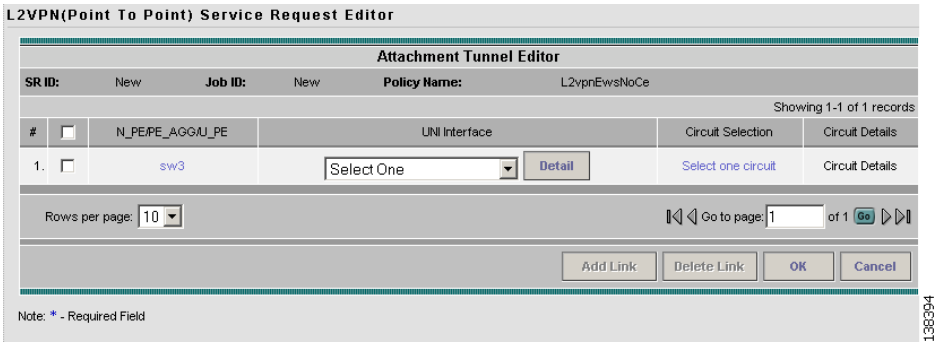


Step 7 In the Select column, choose a PE for the L2VPN link.

Step 8 Click **Select**.

Step 9 Choose a PE interface from the drop-down list as shown in Figure 5-34.

Figure 5-34 PE Interface



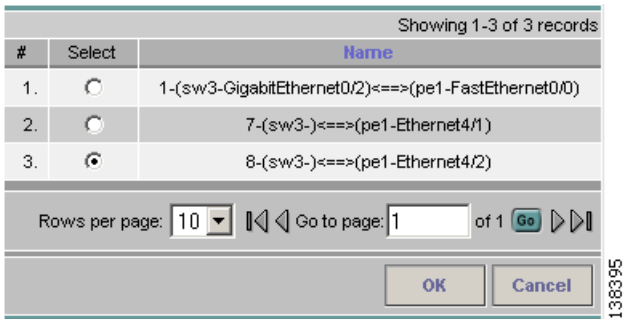
Note ISC only displays the available interfaces for the service, based on the configuration of the underlying interfaces, existing service requests that might be using the interface, and the customer associated with the service request. You can click the **Details** button to display a pop-up window with information on the available interfaces, such as interface name, customer name, VPN name and service request ID, service request type, VLAN translation type, and VLAN ID information.

Step 10 Click **OK** if the PE role type is N-PE.

Step 11 If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column. The NPC window appears (see Figure 5-35). If only one NPC exists for the Chosen PE and PE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly.

Note If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

Figure 5-35 Select NPC

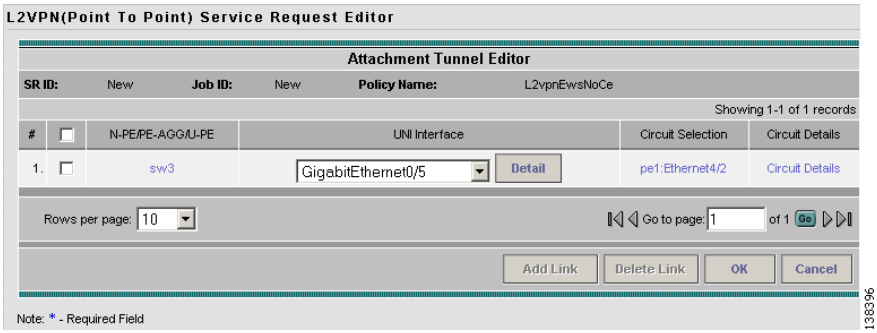


Step 12 Choose the name of the NPC from the Select column.

Step 13 Click **OK**.

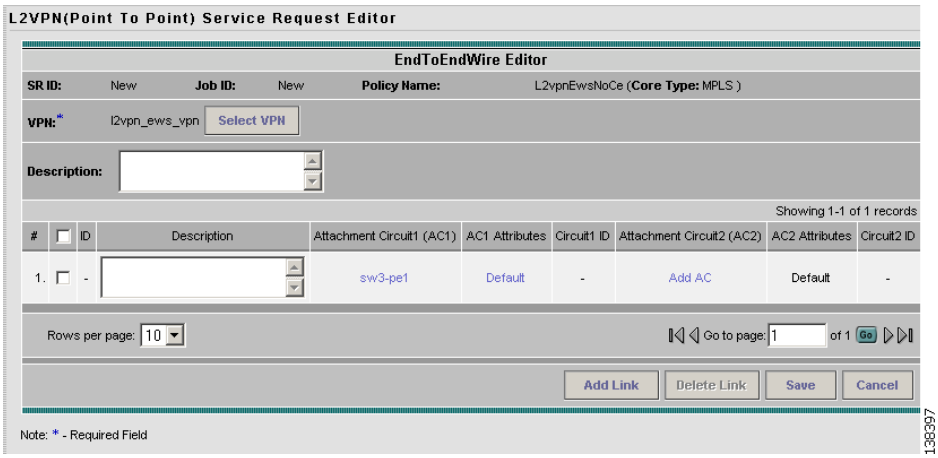
Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection** as in Figure 5-36. This means that you do not have to further specify the PE to complete the link.

Figure 5-36 NPC Created



Step 14 Click **OK**. The Service Request Editor window (Figure 5-37) appears displaying the name of the selected PE in the AC1 column.

Figure 5-37 Attachment Circuit Selected



Step 15 Click **AC1** Link Attributes and edit the attributes if desired (see the Modifying the L2VPN Service Request, page 5-22). Click **OK**.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 16 Repeat Steps 5 through 15 for **AC2**.

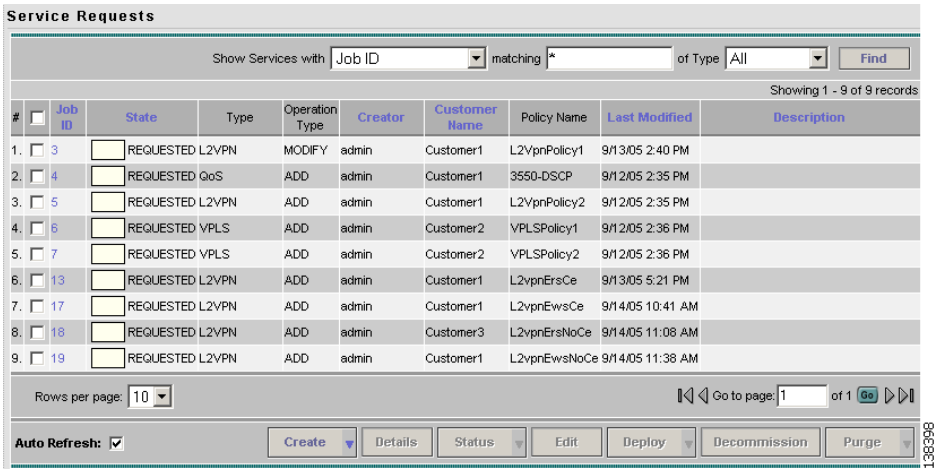
Step 17 Click **Save**. The EWS service request is created and saved in ISC.

Modifying the L2VPN Service Request

After you choose all the CE end points and the NPC from the CE, go to the End-to-End Wire Editor and work on the end-to-end wire—the end-to-end connection that links two CEs. An end-to-end wire is a virtual logical link between a CE-CE pair. Each end-to-end-wire is associated with one end-to-end wire attribute and two attachment circuits (ACs). An AC is a virtual logical link between a CE-PE pair. Each AC is associated with one set of AC attributes and one or more L2VPN logical links.

Step 1 Select **Service Inventory** > **Inventory and Connection Manager** > **Service Requests**. See Figure 5-38.

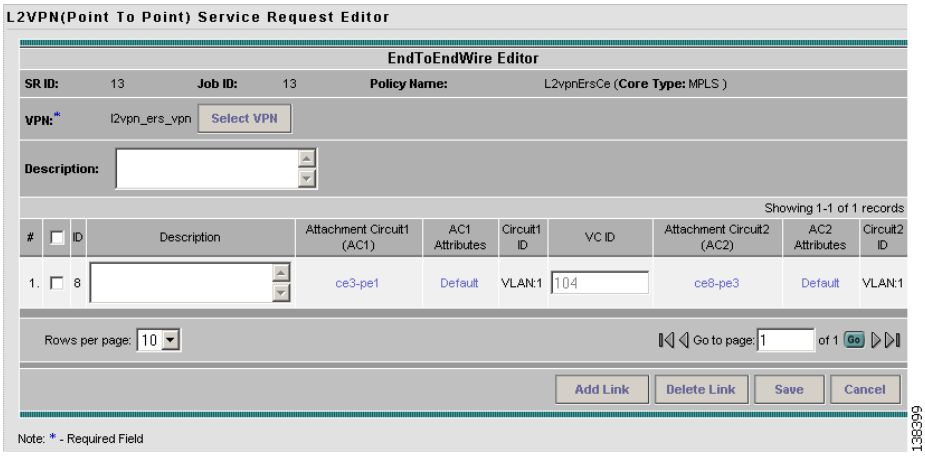
Figure 5-38 L2VPN Service Activation



Step 2 Select a check box for a service request.

Step 3 Click **Edit**. The End-to-End-Wire Editor window appears as shown in Figure 5-39.

Figure 5-39 End-to-End Wire Editor



Step 4 The VPN for this service request appears in the Select VPN field. If this request has more than one VPN, click **Select VPN** to choose a VPN.

You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can edit the AC link attributes to change the default policy settings. After you edit these fields, the blue link changes from Default to Changed.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end wire in the **Description** field provided for each wire. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The Circuit ID is created automatically, based on the VLAN data for the circuit.

If the policy was set up for you to define a VC ID manually, enter it into the empty **VC ID** field. If policy was set to "auto pick" the VC ID, ISC will supply a VC ID, and this field will not be editable. In the case where you supply the VC ID manually, if the entered value is in the provider's range, ISC validates if the entered value is available or allocated. If the entered value has been already allocated, ISC generates an error message saying that the entered value is not available and prompts you to re-enter the value. If the entered value is in the provider's range, and if it is available, then it is allocated and is removed from the VC ID pool. If the entered value is outside the provider's range, ISC displays a warning saying that no validation could be performed to verify if it is available or allocated.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

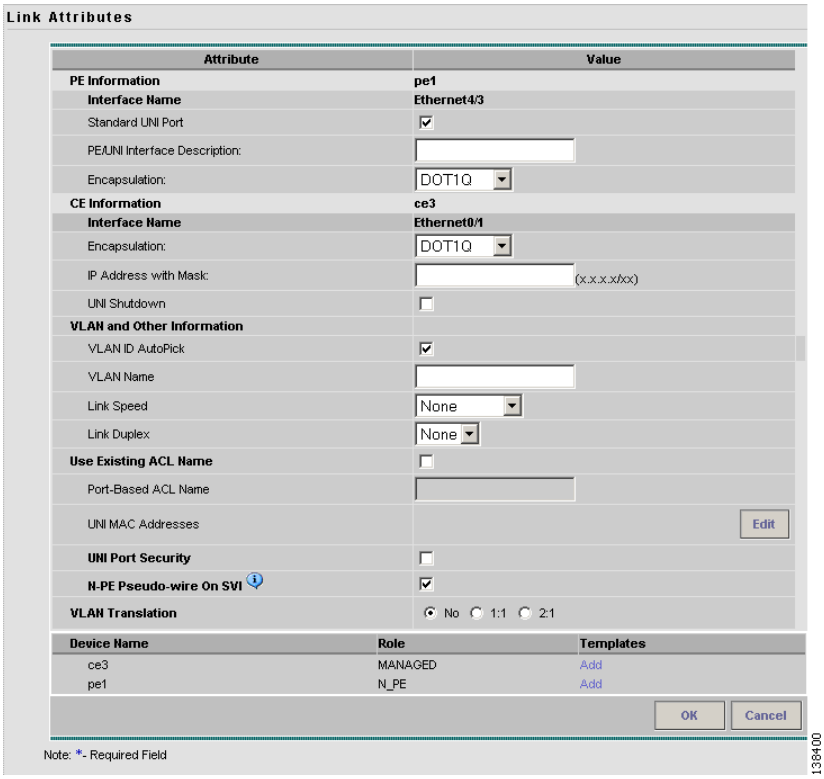
The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 5 To add a template data file to an attachment circuit, click **Default**. The Link Attributes window appears as shown in Figure 5-40.

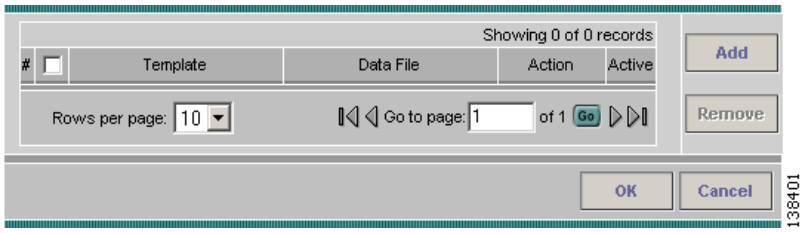
Note To add a template to an attachment circuit, you must have already created the template. For detailed steps to create templates, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Figure 5-40 Link Attributes Window



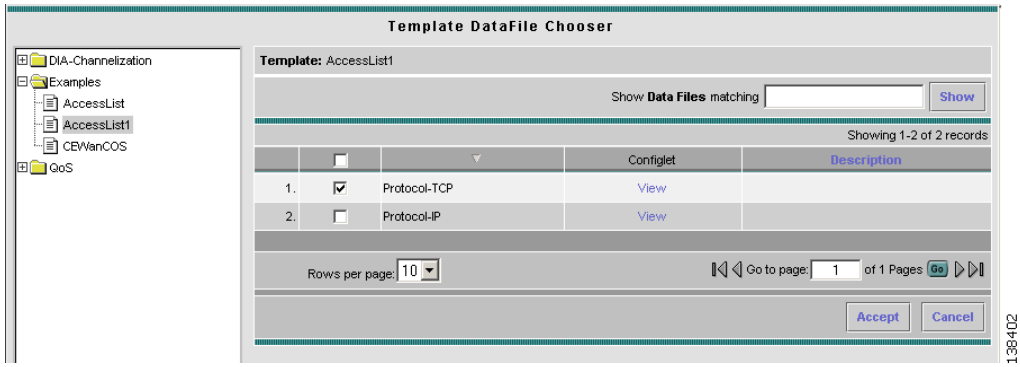
Step 6 Choose a Device Name, and click **Add** under Templates. The Add/Remove Templates window appears as shown in Figure 5-41.

Figure 5-41 Add/Remove Templates



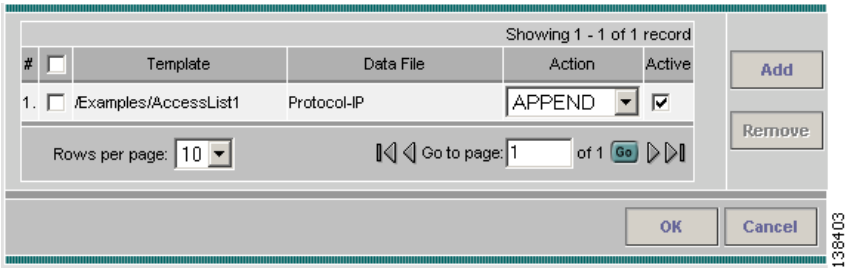
Step 7 Click **Add**. The Template Data File Chooser window appears as shown in Figure 5-42.

Figure 5-42 Template Datafile Chooser



Step 8 Select the template that you want to add and click **Accept**.The Add/Remove Templates window appears with the template displayed as shown in Figure 5-43.

Figure 5-43 Add/Remove Templates with Templates Shown



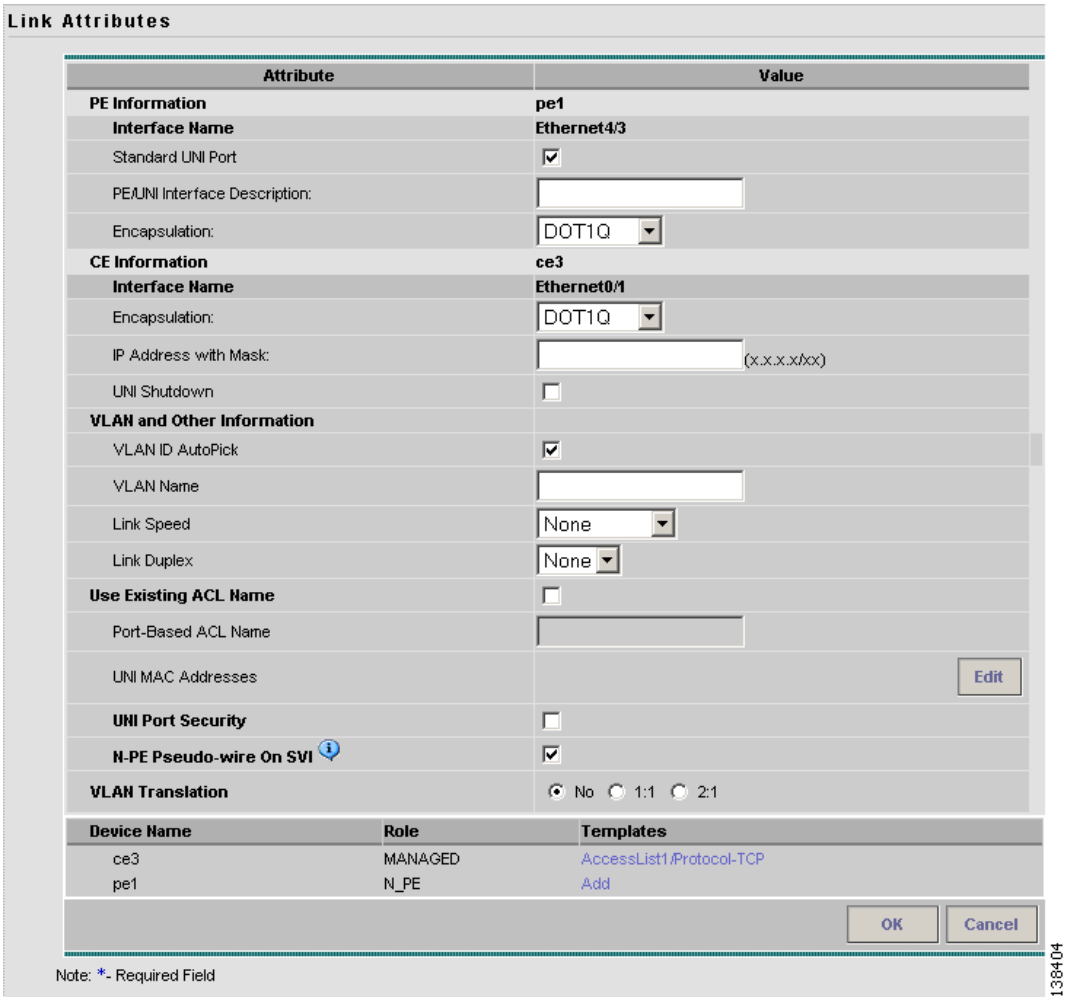
Step 9 Choose a Template name.

Step 10 Under Action, use the drop-down list and select **APPEND** or **PREPEND.** Append tells ISC to append the template generated CLI to the regular ISC (non-template) CLI. Prepend is the reverse and does not append the template to the ISC CLI.

Step 11 Select Active to use this template for this service request. If you do not select Active, the template is not used.

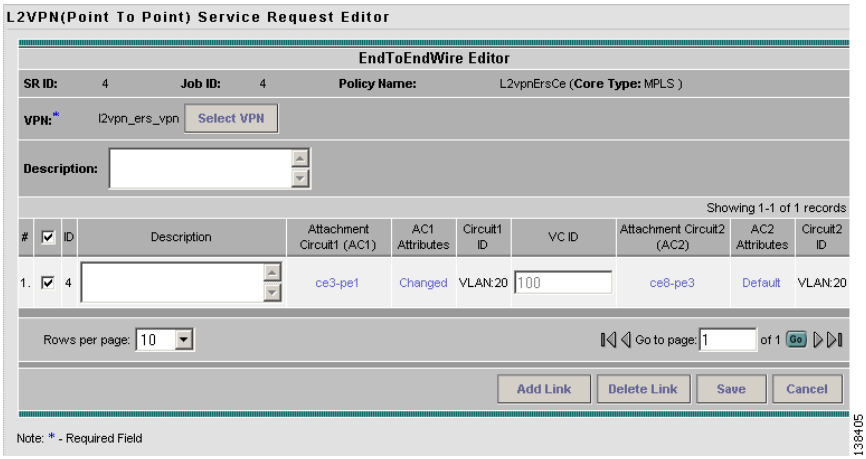
Step 12 Click **OK**. The Link Attributes with the template added appears as shown in Figure 5-44

Figure 5-44 Link Attributes with Template Added



Step 13 Click **OK**. The Service Request Editor window appears showing the default for AC1 changed as shown in Figure 5-45.

Figure 5-45 Service Request Editor with Link Attributes Changed.



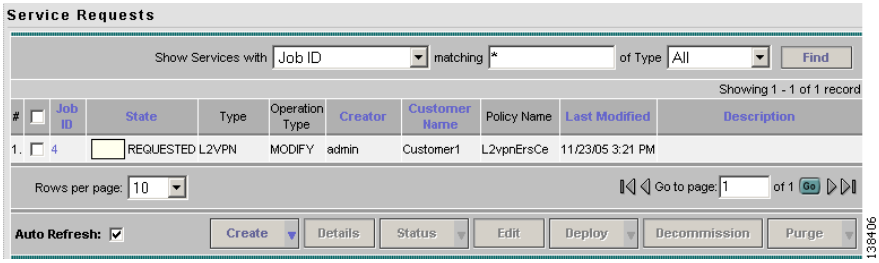
Step 14 When you are finished editing the end-to-end wires, click **Save**.

Saving the L2VPN Service Request

When you are finished with Link Attributes for all the Attachment Circuits, click **Save** to finish the L2VPN service request creation as shown in Figure 5-46.

If the L2VPN service request is successfully created, you will see the service request list window where the newly created L2VPN service request is added with the state of REQUESTED as shown in Figure 5-46. If, however, the L2VPN service request creation failed for some reason (for example, the value chosen is out of bounds), you are warned with an error message. Go back to correct the error and **Save** again.

Figure 5-46 L2VPN Service Request Created



The L2VPN service request is in Requested state. See Deploying Service Requests, page 12-1 for information on deploying L2VPN service requests.

Creating an L2TPv3 Policy

This chapter contains the basic steps to create an L2TPv3 policy. It contains the following sections:

Defining an L2TPv3 Policy

You must define an L2TPv3 policy before you can provision a Cisco IP Solution Center (ISC) L2TPv3-based L2VPN service. An L2TPv3 policy defines the common characteristics shared by the end-to-end wire attributes and Attachment Circuit (AC) attributes.

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is not set to editable, the service request creator cannot change the policy item.

The two major categories of an L2TPv3 policy correspond to the two major services that L2TPv3 provides:

- Frame Relay transport over L2TPv3, both port-based and DLCI-based MFR support.
- ATM transport over L2TPv3, VP mode and VC mode, single cell.

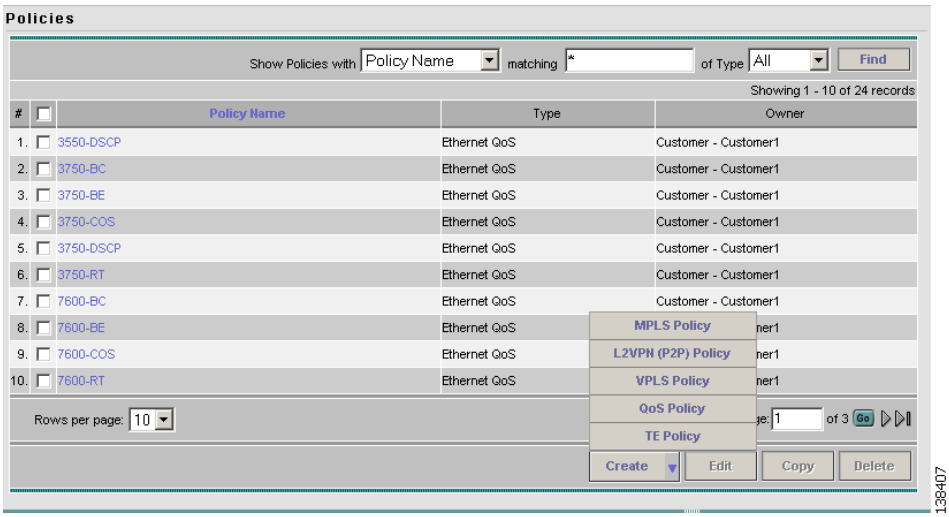
A policy is a template of most of the parameters needed to define an L2TPv3 service request. After you define it, an L2TPv3 policy can be used by all the L2TPv3 service requests that share a common set of characteristics.

You create a new L2TPv3 policy whenever you create a new type of service or a service with different parameters. L2TPv3 policy creation is normally performed by experienced network engineers.

To define an L2TPv3 policy in ISC, perform the following steps.

Step 1 Select **Service Design > Policies**. The Policies window appears as shown in Figure 6-1.

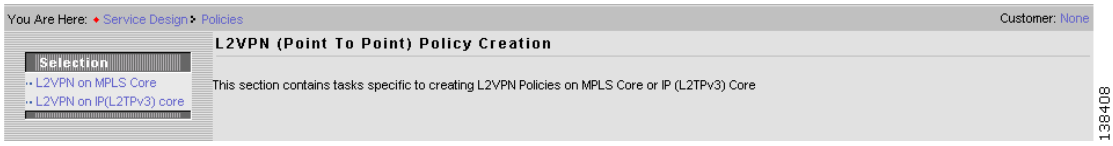
Figure 6-1 Creating an L2TPv3 Policy



Step 2 Click **Create**.

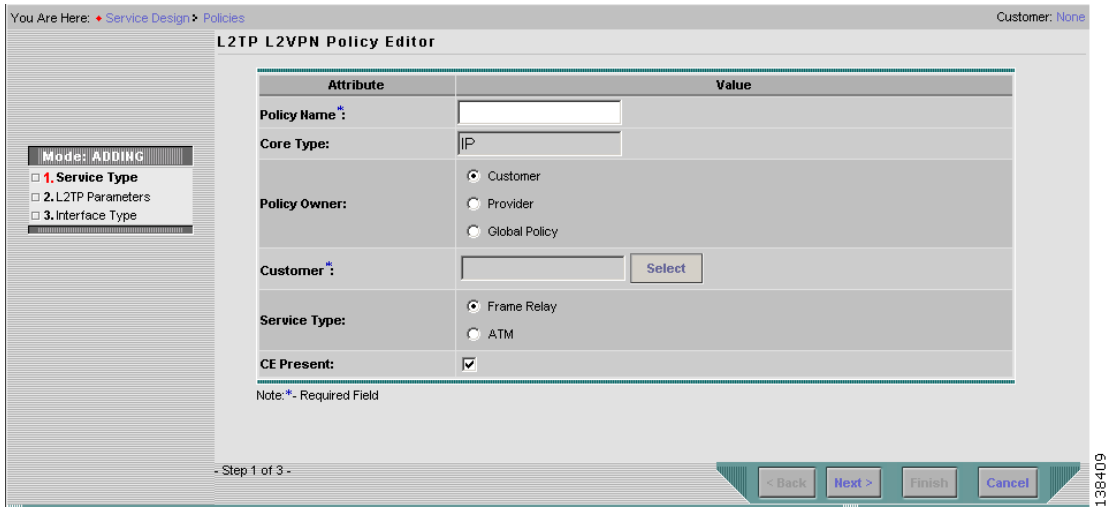
Step 3 Select **L2VPN (P2P) Policy**. When you select L2VPN (P2P) Policy, the window in Figure 6-2 appears.

Figure 6-2 L2VPN Policy Window



Step 4 Select **L2VPN on IP (L2TPv3) core**. The window in Figure 6-3 appears.

Figure 6-3 L2TP L2VPN Policy Editor



Step 5 Enter a **Policy Name** for the L2TPv3 policy.

Step 6 Choose the **Policy Owner** for the L2TPv3 policy.

There are three types of L2TPv3 policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this L2TPv3 policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, an L2TPv3 policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 7 Click **Select** to choose the owner of the L2TPv3 policy. (If you choose Global ownership, the Select function is not available.) The Select Customer window or the Select Provider window appears and you can choose an owner of the policy and click **Select**.

Step 8 Choose the **Service Type** of the L2TPv3 policy.

There are two service types for L2TPv3 policies:

- **Frame Relay**
- **ATM**

Step 9 Select the **CE Present** check box if you want ISC to ask the service operator who uses this L2TPv3 policy to provide a CE router and interface during service activation. The default is CE present in the service.

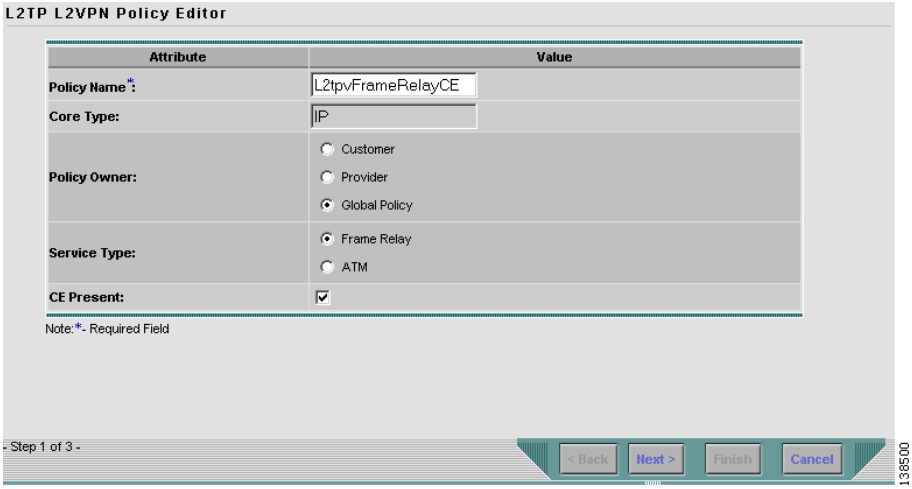
If you do not select the **CE Present** check box, ISC asks the service operator, during service activation, only for the PE router and customer-facing interface.

Step 10 Click **Next**.

Defining a Frame Relay Policy with a CE

This section describes defining a Frame Relay policy with a CE present. Figure 6-4 is an example of the first page of this policy.

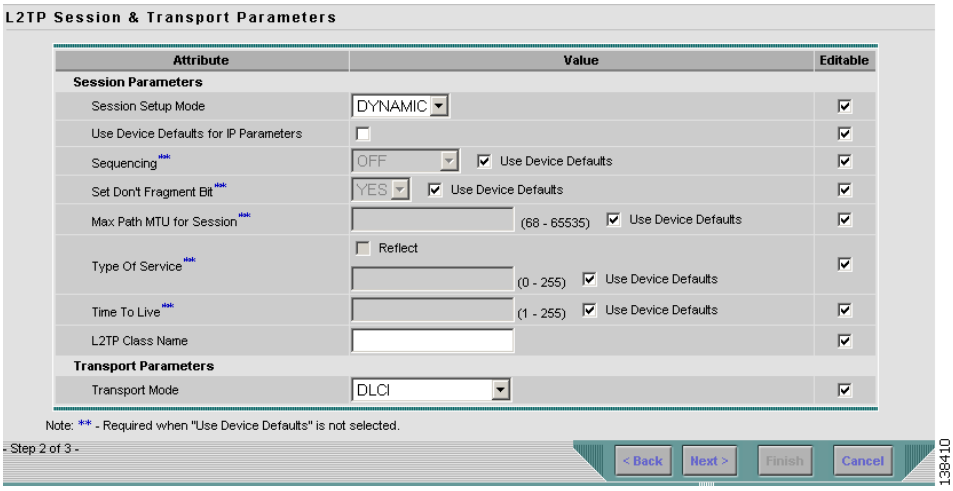
Figure 6-4 Frame Relay Policy with a CE



Step 1 Click **Next**. The window in Figure 6-5 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

Figure 6-5 Frame Relay Policy with a CE Attributes



Step 2 Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

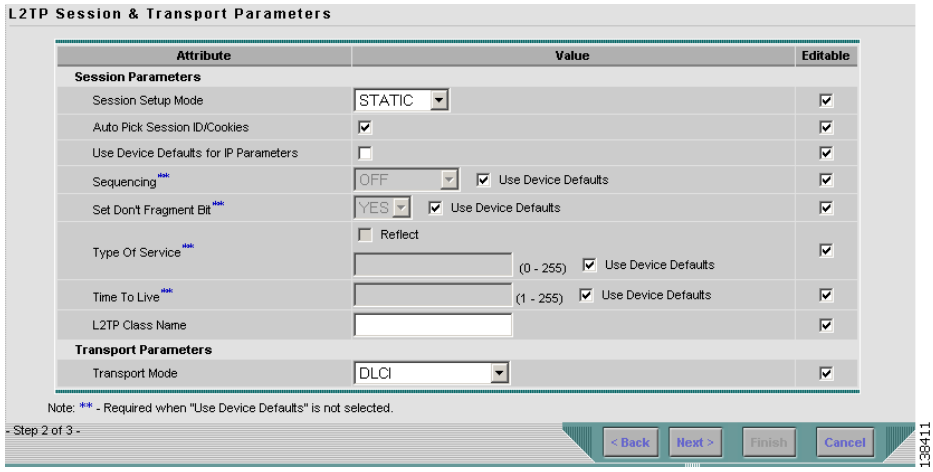
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-6. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

Figure 6-6 Static Session Setup Mode



Step 3 Select the **Use Device Defaults for IP Parameters** check box if you do **not** want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

Step 4 Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default)
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

Step 5 **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

Step 6 **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535.

Step 7 **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

Step 8 **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

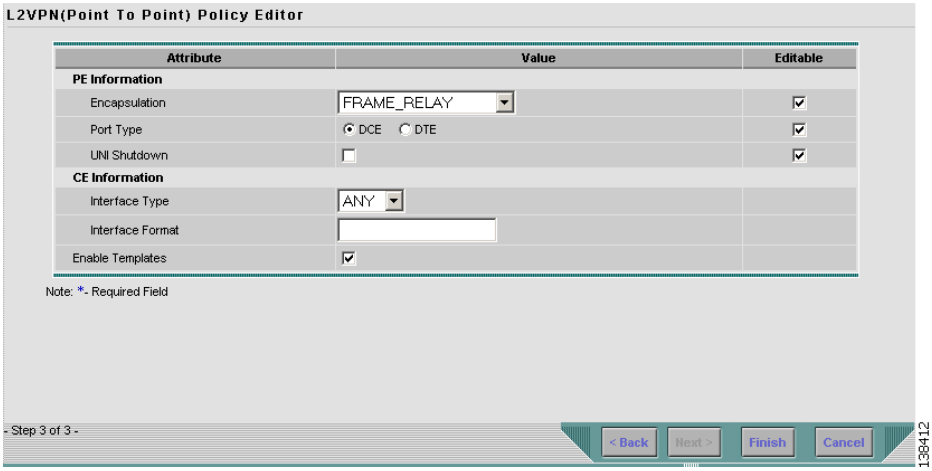
Step 9 **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes. You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel.

Step 10 Select the **Transport Mode** from the drop-down list. The choices are:

- **DLCI** (data-link connection identifier) is the default.
- **PORT_TRUNKING**

Step 11 Click **Next**. The window in Figure 6-7 appears.

Figure 6-7 Frame Relay Interface with a CE Attributes



Step 12 Choose the PE **Encapsulation** type. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Step 13 Choose the PE **Port Type**. The choices are:

- **DCE** (data circuit-terminating equipment)
- **DTE** (data terminal equipment)

For **DCLI** transport mode, set BOTH PEs to DCE or BOTH to DTE. If the PE setting is DCE, then ISC provisions the corresponding CE (if there is one) to be DTE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

For **PORT_TRUNKING** transport mode, set one PE to DTE and the other PE to DCE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

Step 14 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 15 Choose the CE **Interface Type.** The choices are:

- **ANY**

- **Serial**
- **MFR** (Multilink Frame Relay)
- **POS**

Step 16 Enter the CE **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

Step 17 Choose the CE **Encapsulation** type. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Note If the CE Interface Type is ANY, ISC will not ask for an **Encapsulation** type in policy.

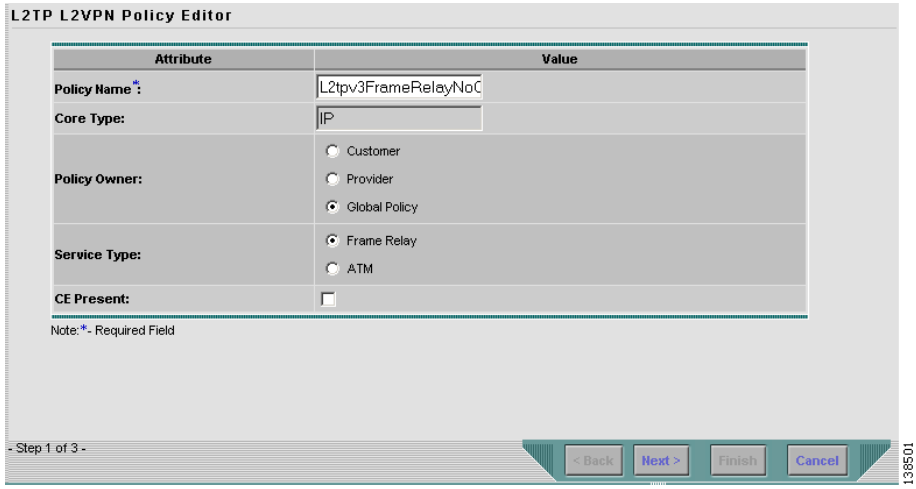
Step 18 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 19 Click **Finish**.

Defining a Frame Relay Policy without a CE

This section describes defining an L2TPv3 Frame Relay policy without a CE present. Figure 6-8 is an example of the first page of this policy.

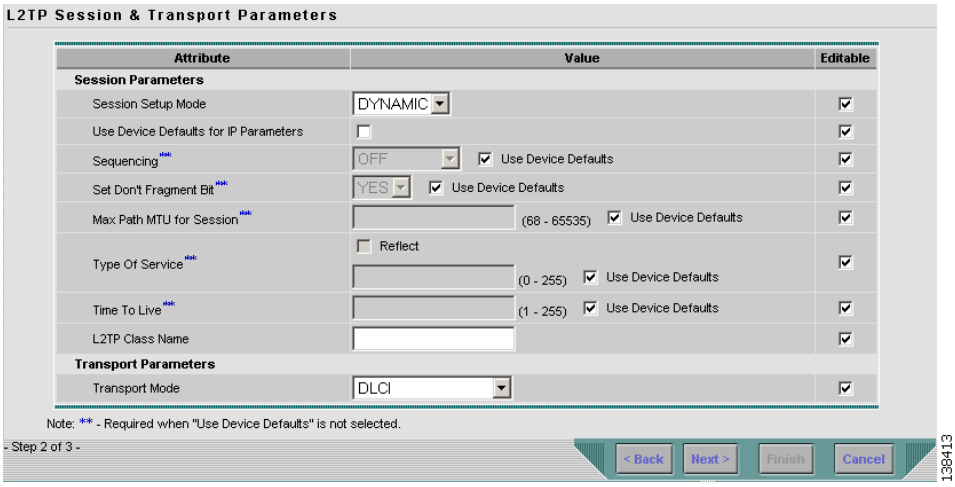
Figure 6-8 Frame Relay Policy without a CE



Step 1 Click **Next**. The window in Figure 6-9 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

Figure 6-9 Frame Relay without CE Policy Attributes



Step 2 Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

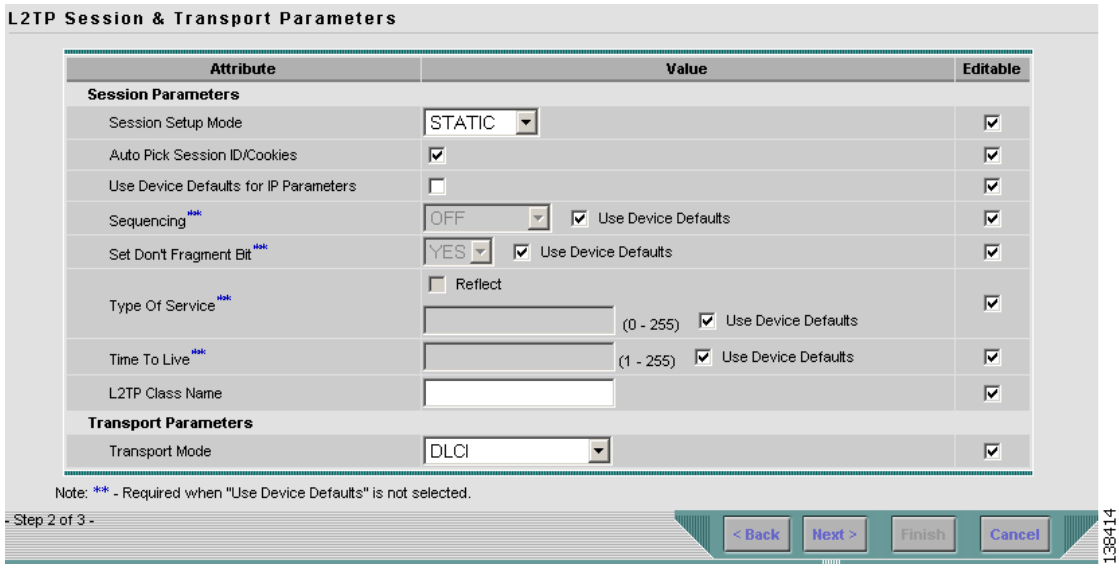
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-10. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

Figure 6-10 Static Session Setup Mode



Step 3 Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

Step 4 Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default)
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

Step 5 **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

Step 6 **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

Step 7 **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

Step 8 **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

Step 9 **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

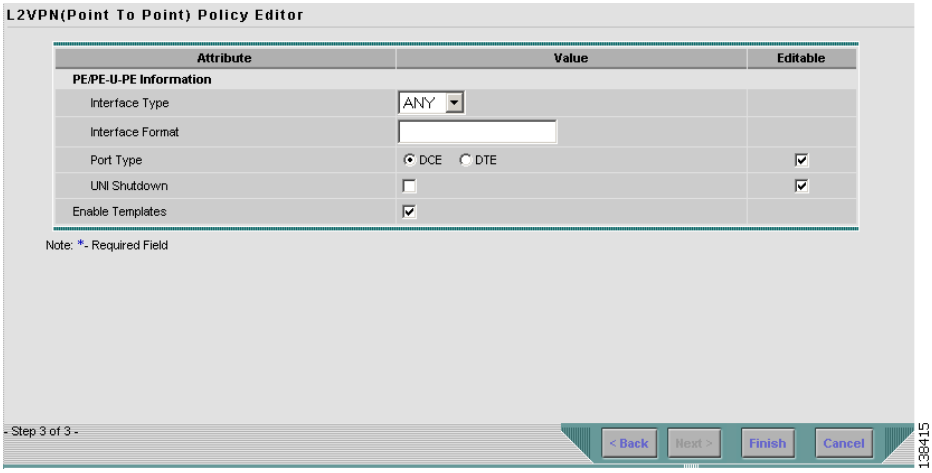
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel.

Step 10 Select the **Transport Mode** from the drop-down list. The choices are:

- **DLCI** (data-link connection identifier) is the default.
- **Port-trunking**

Step 11 Click **Next**. The window in Figure 6-11 appears.

Figure 6-11 PE Frame Relay without a CE



Step 12 Choose the PE **Interface Type**. The choices are:

- **ANY**
- **Serial**
- **MFR** (Multilink Frame Relay)
- **POS**

Step 13 Enter the PE **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

Step 14 Choose the PE **Port Type**. The choices are:

- **DCE** (data circuit-terminating equipment)
- **DTE** (data terminal equipment)

For **DCLI** transport mode, set BOTH PEs to DCE or BOTH to DTE. If the PE setting is DCE, then ISC provisions the corresponding CE (if there is one) to be DTE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

For **PORT_TRUNKING** transport mode, set one PE to DTE and the other PE to DCE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

Step 15 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

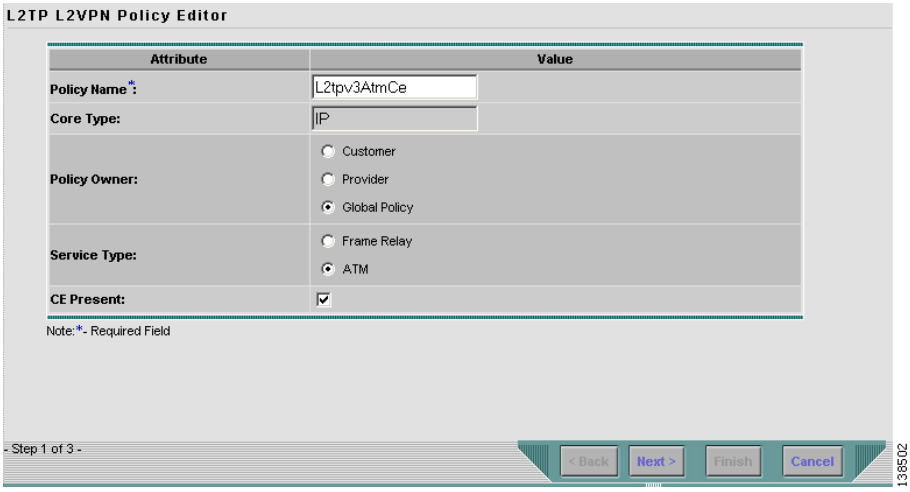
Step 16 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 17 Click **Finish**.

Defining an ATM Policy with aCE

This section describes how to define an L2TPv3 ATM policy with CE present. Figure 6-12 is an example of the first page of this policy.

Figure 6-12 ATM Policy with a CE

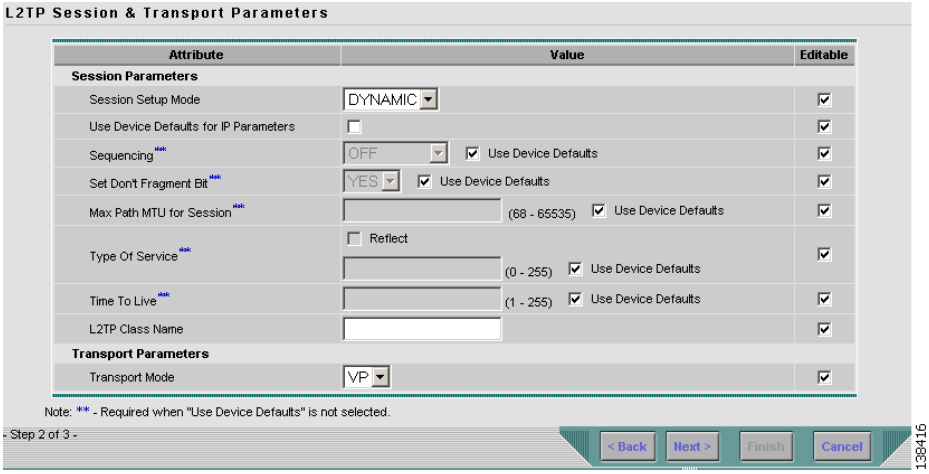


Perform the following steps.

Step 1 Click **Next**. The window in Figure 6-13 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

Figure 6-13 ATM Policy with CE Attributes



Step 2 Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

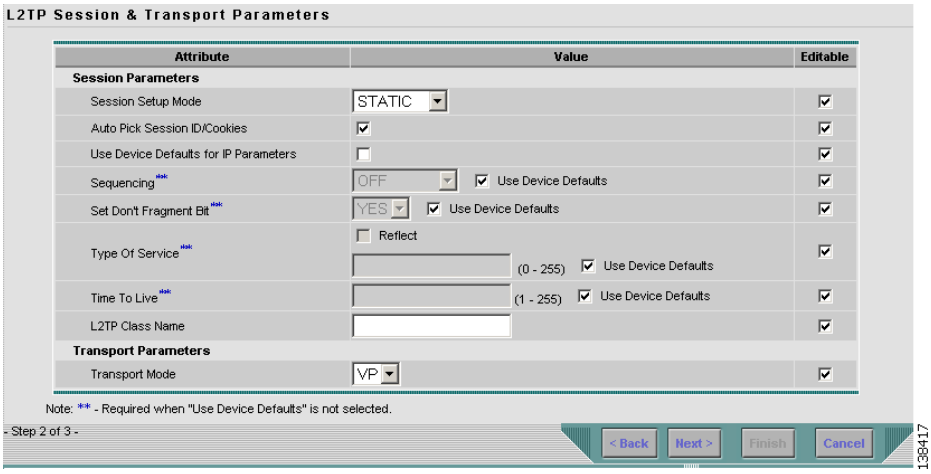
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-14. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

Figure 6-14 Static Session Setup Mode



Step 3 Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

Step 4 Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default)
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

Step 5 **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

Step 6 **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

Step 7 **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

Step 8 **Time To Live.** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

Step 9 **L2TP Class Name.** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

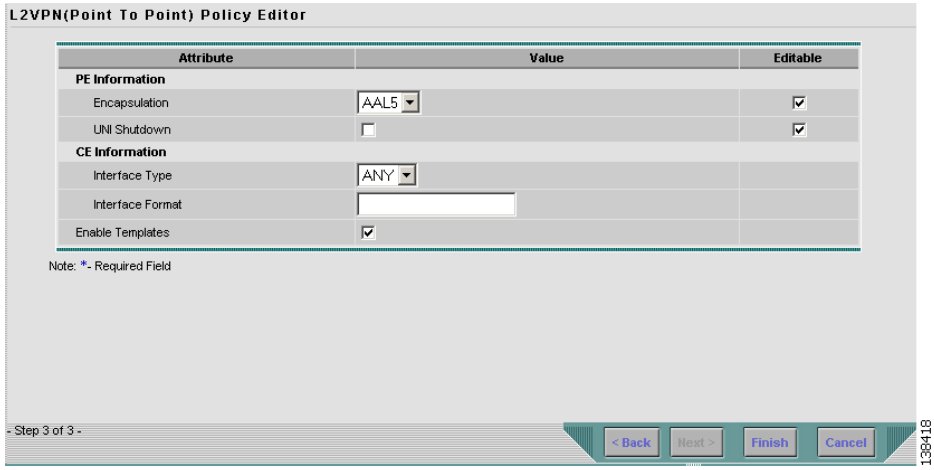
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel. For ATM, the vpi/vci pair for CE must match the vpi/vci pair for PE.

Step 10 Select the **Transport Mode** from the drop-down list. The choices are:

- **VP** (Virtual Path)
- **VC** (Virtual Circuit) This is the default.

Step 11 Click **Next**. The window in Figure 6-15 appears.

Figure 6-15 ATM with a CE Policy Attributes



Step 12 Choose the PE **Encapsulation** type from the drop-down list. The choices are:

- **AAL5**
- **AAL0**

Step 13 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 14 Choose the CE **Interface Type** from the drop-down list. The choices are:

- **ANY**
- **ATM**

Step 15 Enter the CE **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 16 Choose the CE **Encapsulation Type** from the drop-down list. The choices are:

- **AAL5SNAP**
- **AAL5MUX**
- **AAL5NLPID**
- **AAL2**

Note The CE Encapsulation Type only appears if you chose the CE Interface Type as ATM instead of ANY.

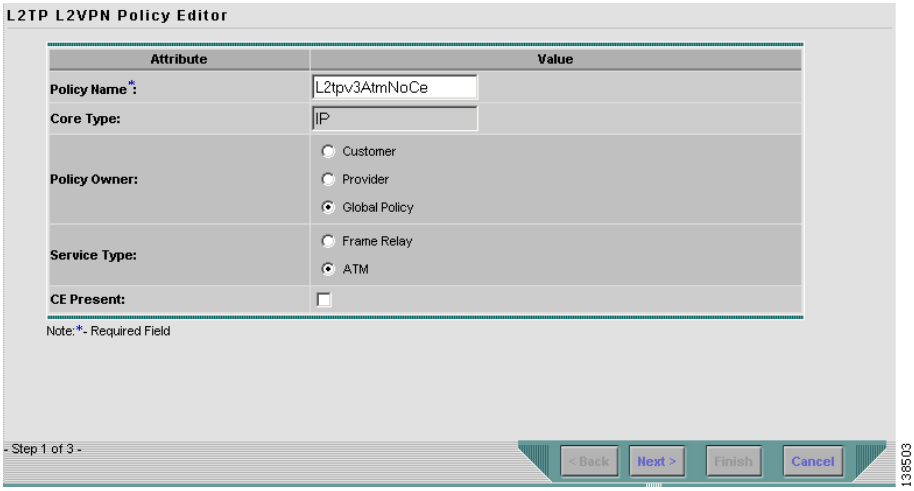
Step 17 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 18 Click **Finish**.

Defining an ATM Policy without a CE

This section describes defining an ATM policy without a CE present. Figure 6-16 is an example of the first page of this policy.

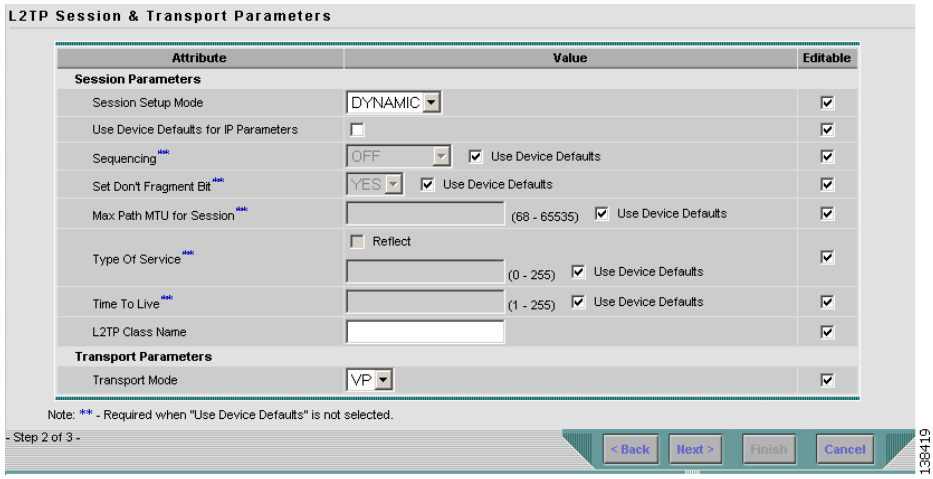
Figure 6-16 ATM Policy without a CE



Step 1 Click **Next**. The window in Figure 6-17 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

Figure 6-17 ATM without a CE Policy Attributes



Step 2 Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

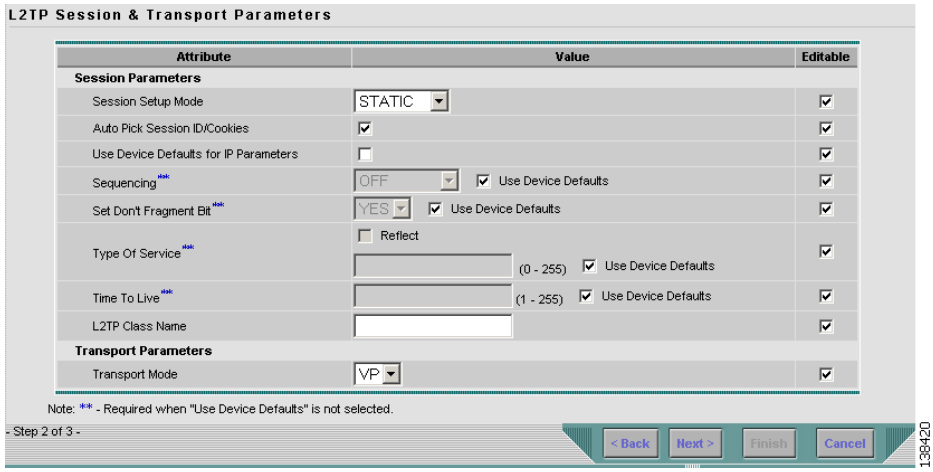
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-18. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

Figure 6-18 Static Session Setup Mode



Step 3 Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

Step 4 Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default)
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

Step 5 **Set Don't Fragment Bit** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudowire.

Step 6 **Max Path MTU for Session** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

Step 7 Type Of Service (ToS)

- Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers.
- Enter the ToS byte value used by all packets sent across the pseudowire. The range is 0 to 255.

Step 8 **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

Step 9 **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

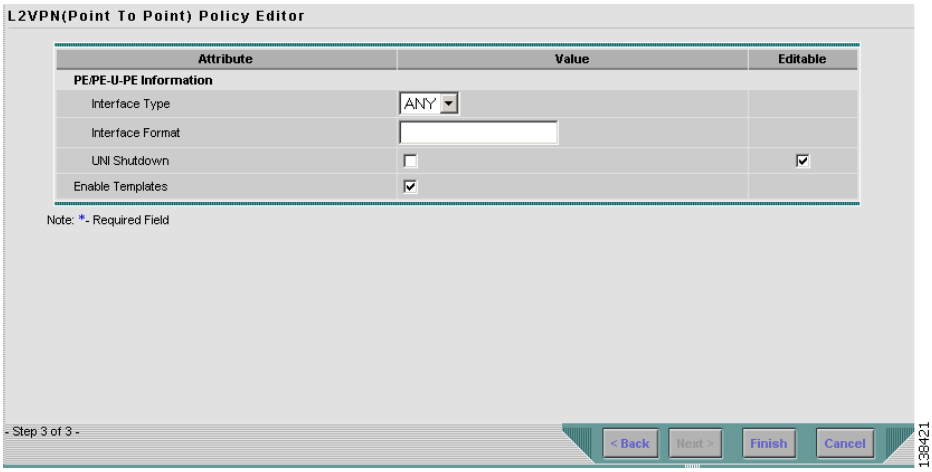
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel. For ATM, the vpi/vci pair for CE must match the vpi/vci pair for PE.

Step 10 Select the **Transport Mode** from the drop-down list. The choices are:

- **VP** (Virtual Path)
- **VC** (Virtual Circuit) This is the default.

Step 11 Click **Next**. The window in Figure 6-19 appears.

Figure 6-19 ATM PE Policy Information



Step 12 Choose the PE **Interface Type** from the drop-down list. The choices are:

- **ANY**
- **ATM**

Step 13 Enter the PE **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 14 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 15 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 16 Click **Finish**.

Managing an L2TPv3 Service Request

This chapter contains the basic steps to provision an L2TPv3 service. It contains the following sections:

Introducing L2TPv3 Service Requests

An L2TPv3 service request consists of one or more end-to-end wires, connecting various sites in a point-to-point topology. When you create a service request, you enter several parameters, including the specific interfaces on the CE and PE routers.

You can also integrate a Cisco IP Solution Center (ISC) template with a service request. You can associate one or more templates to the CE and the PE.

To create a service request, a Service Policy must already be defined, as described in Chapter 6, "Creating an L2TPv3 Policy."

Based on the predefined L2TPv3 policy, an operator creates an L2TPv3 service request, with or without modifications to the L2TPv3 policy, and deploys the service. Service creation and deployment are normally performed by regular network technicians for daily operation of network provisioning.

The following steps are involved in creating a service request for Layer 2 connectivity between customer sites:

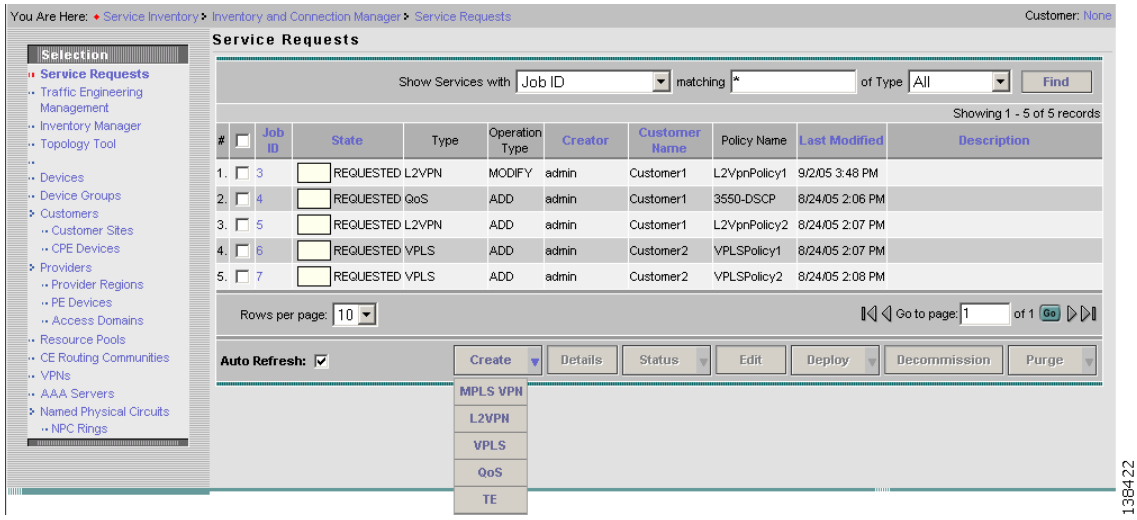
- Select an L2TPv3 policy.
- Select a VPN name.
- Choose a CE Topology for Frame Relay/ATM services.
- Select the endpoints (CE and PE) that must be connected. For each end-to-end Layer 2 connection, ISC creates an end-to-end wire object in the repository for the service request.
- Choose a CE or PE interface.
- Choose a Named Physical Circuit (NPC) for the CE (if there are multiple NPCs between the CE and the PE).
- Edit the end-to-end connection.

- Edit the L2TP parameters.
- Edit the link attributes.
- Save the service request.

Creating an L2TPv3 Service Request

Step 1 Select **Service Inventory > Inventory and Connection Manage > Service Requests**. The Service Requests window appears as shown in Figure 7-1.

Figure 7-1 L2TPv3 Service Activation



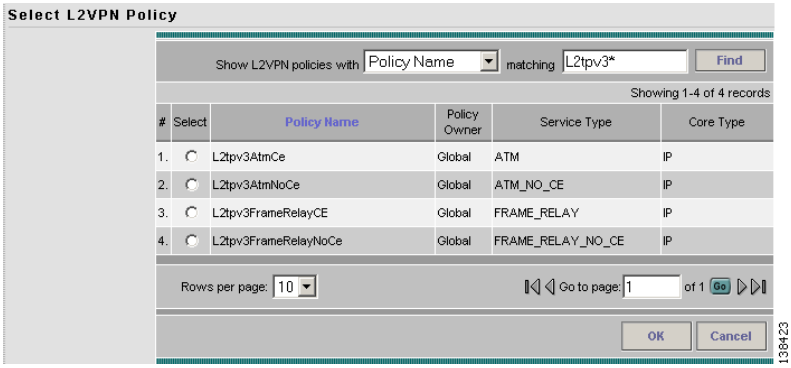
Step 2 Click **Create**.

Step 3 Choose **L2VPN** from the drop-down list.

Step 4 Select the L2TPv3 policy of choice. See Figure 7-2. If more than one L2TPv3 policy exists, a list of L2TPv3 policies appears.

Note L2TPv3 service requests must be associated with an L2TPv3 policy. You choose an L2TPv3 policy from the policies previously created (see Chapter 5, “Creating an L2TPv3 Policy”).

Figure 7-2 L2TPv3 Policy Choice



Step 5 After you make the choice, click **OK**.

As soon as you make the choice, the new service request inherits all the properties of that L2TPv3 policy, such as all the editable and non-editable features and pre-set parameters.

To continue creating an L2TPv3 service request, go to one of the following sections:

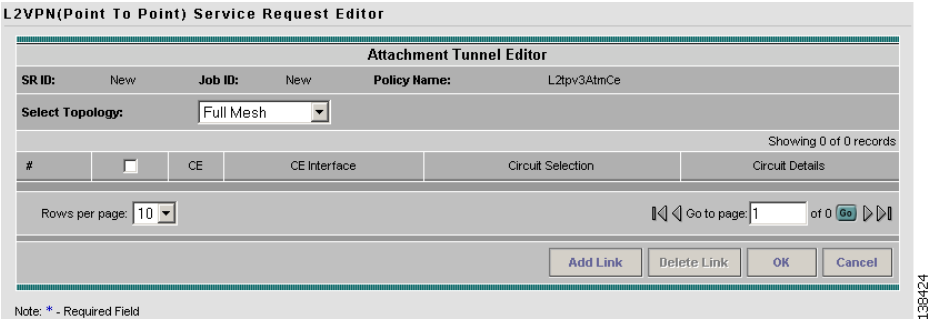
- Creating an L2TPv3 Service Request with a CE, page 7-3.
- Creating an L2TPv3 Service Request without a CE, page 7-8.

Creating an L2TPv3 Service Request with a CE

This section includes detailed steps for creating an L2TPv3 service request with a CE present. If you are creating an L2TPv3 service request with no CE present, see Creating an L2TPv3 Service Request without a CE, page 7-8.

After you choose an L2TPv3 policy, the L2TPv3 Service Request Editor window appears (see Figure 7-3).

Figure 7-3 L2TPv3 Service Request Editor



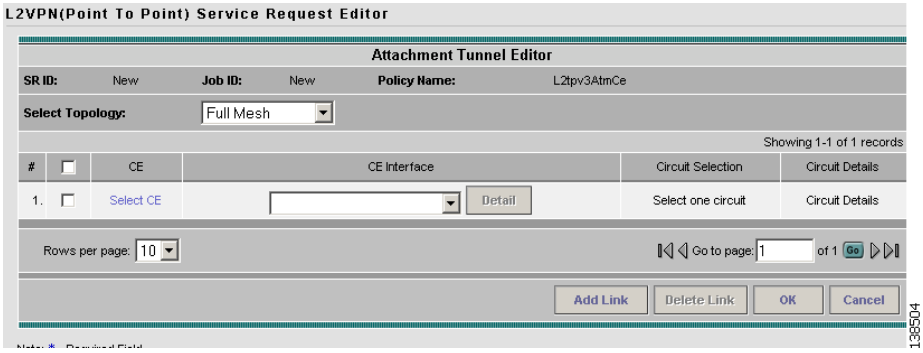
Step 1 Choose a **Topology** from the drop-down list. If you choose **Full Mesh**, each CE will have direct connections to every other CE. If you choose **Hub and Spoke**, then only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other.

Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two end points. For example, with four end points, ISC automatically creates six links with full mesh topology. With hub and spoke topology, however, ISC creates only three links.

Step 2 Click **Add Link**.

You specify the CE end points using the Attachment Tunnel Editor. You can create one or more CEs from a window like the one in Figure 7-4.

Figure 7-4 Select CE



Note All the services that deploy point-to-point connections must have at least two CEs specified.

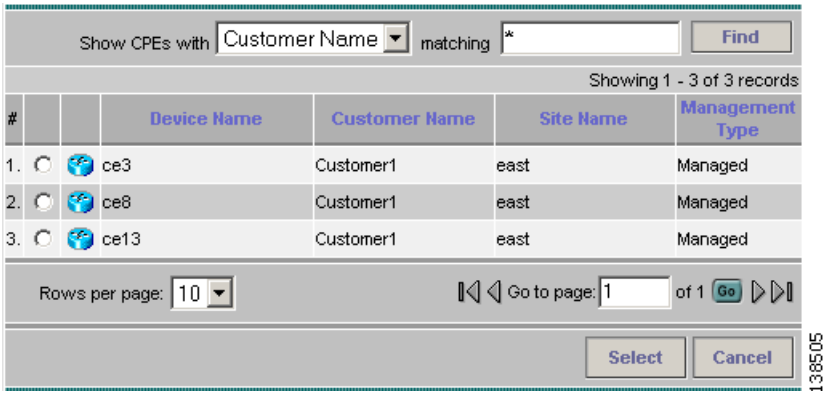
Step 3 Click **Select CE** in the CE column. The CPE for Attachment Circuit window appears (see Figure 7-5). This window displays the list of currently defined CEs.

a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.

b. You can use the **Find** button to either search for a specific CE, or to refresh the display.

c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Figure 7-5 Select CPE Device



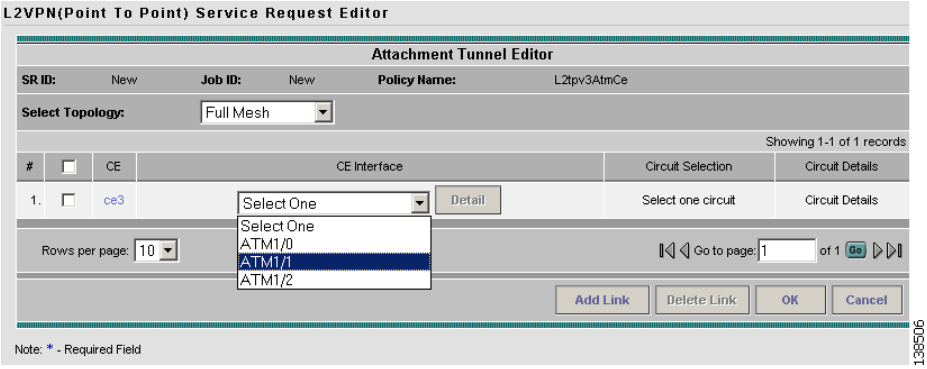
Step 4 In the Select column, choose a CE for the L2TPv3 link.

Step 5 Click **Select**.

The Service Request Editor window appears displaying the name of the selected CE in the CE column.

Step 6 Select the CE interface from the drop-down list (see Figure 7-6).

Figure 7-6 Select the CE Interface

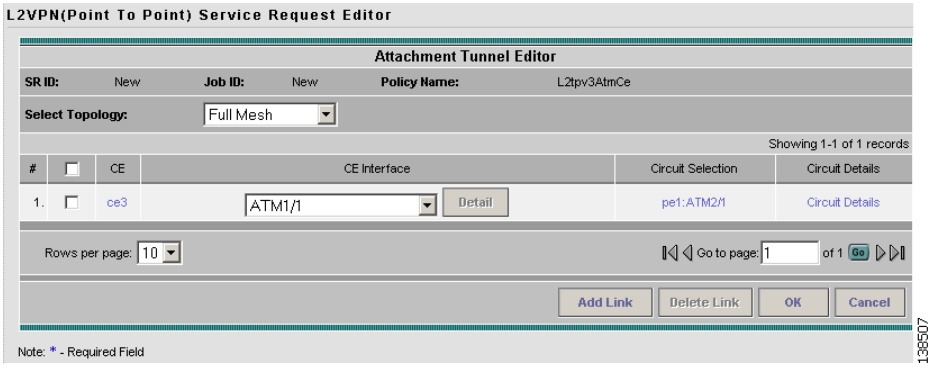


Step 7 If only one NPC exists for the Chosen CE and CE interface, that NPC is auto populated in the Circuit Selection column and you need not choose it explicitly. If more then one NPC is available, click **Select one circuit** in the Circuit Selection column. The NPC window appears, enabling you to select the appropriate NPC.

Step 8 Click **OK**.

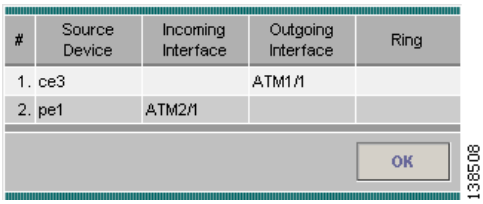
Each time you choose a CE and its interface, the NPC that was pre-created from this CE and interface is automatically displayed under **Circuit Selection** as in Figure 7-7. This means that you do not have to further specify the PE to complete the link.

Figure 7-7 NPC Created



If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC. In Figure 7-8, the CE and PE and their corresponding interfaces appear.

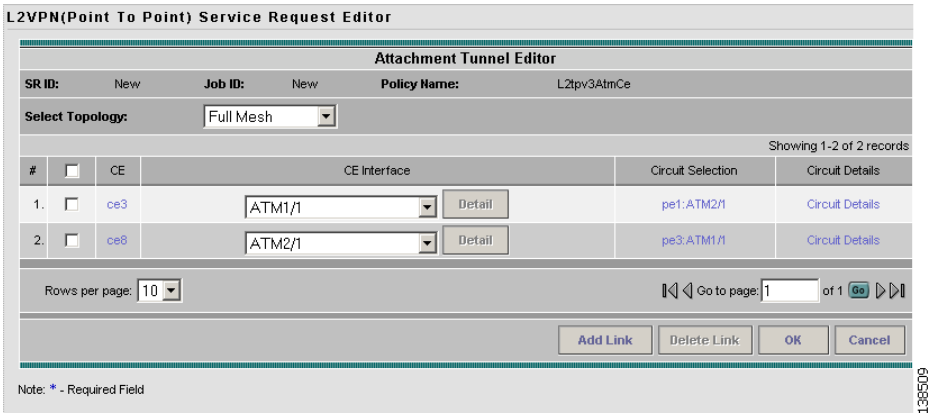
Figure 7-8 NPC Details



After you specify all the CEs, ISC creates the links between CEs based on the Topology that you chose.

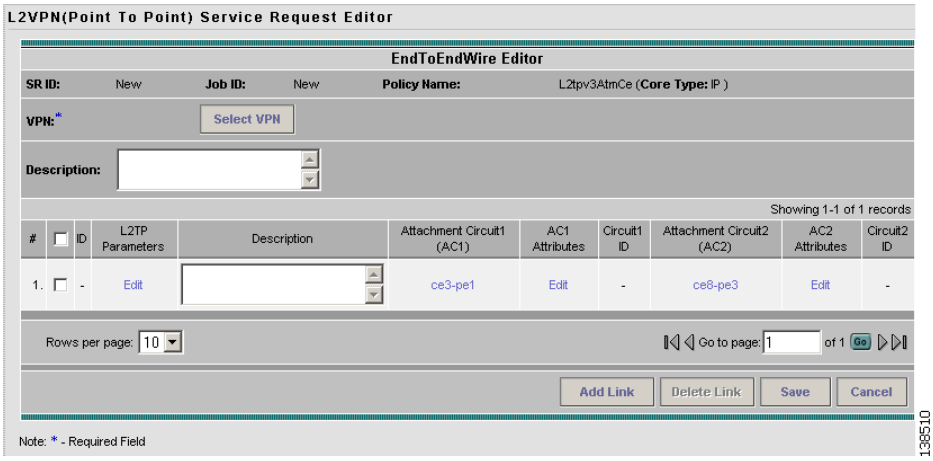
Step 9 Click **OK** in Figure 7-9.

Figure 7-9 Attachment Tunnel Editor



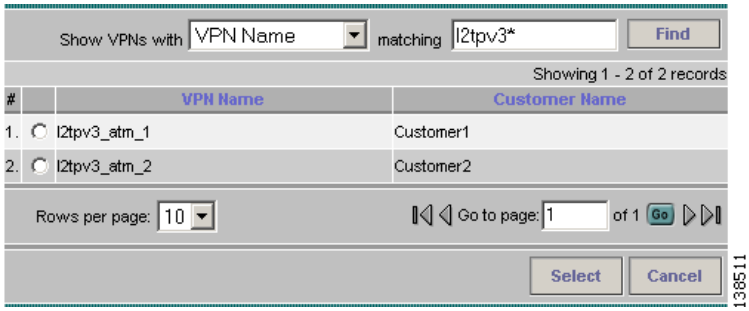
The End-to-End Wire Editor window appears as shown in Figure 7-10.

Figure 7-10 End-to-End Wire Editor



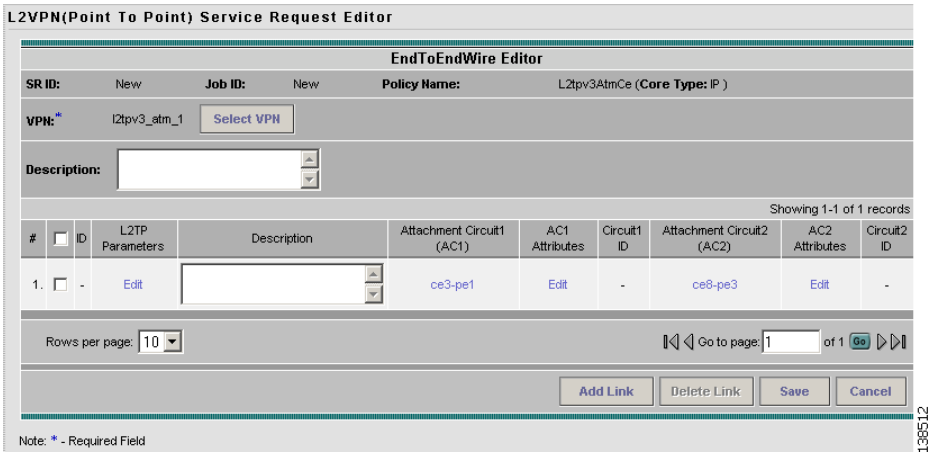
Step 10 The VPN for this service request appears in the Select VPN field. If there is more than one VPN, click **Select VPN** to choose a VPN. The VPN for L2TPv3 service request window appears as shown in Figure 7-11.

Figure 7-11 Select VPN for L2TPv3 Service Request



Step 11 Chose a **VPN Name** and click **Select**. The L2TPv3 Service Request Editor window appears with the VPN name displayed as shown in Figure 7-12.

Figure 7-12 Attachment Circuit Selection



You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end link in the **Description** field provided for each link. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 12 When you are finished editing the end-to-end wires, click **Save**.

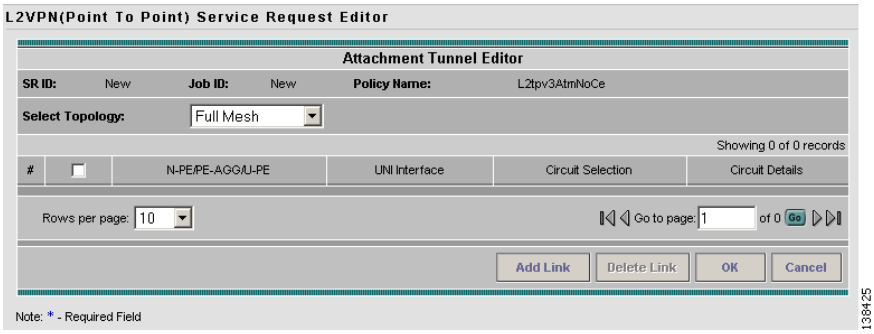
The service request is created and saved into ISC.

Creating an L2TPv3 Service Request without a CE

This section includes detailed steps for creating an L2TPv3 service request without a CE present for ATM and Frame Relay policies. If you are creating an L2TPv3 service request for an L2TPv3 policy with a CE present, see Creating an L2TPv3 Service Request with a CE, page 7-3.

After you choose an L2TPv3 policy, the L2TPv3 Service Request Editor window appears (see Figure 7-13).

Figure 7-13 L2TPv3 Service Request Editor



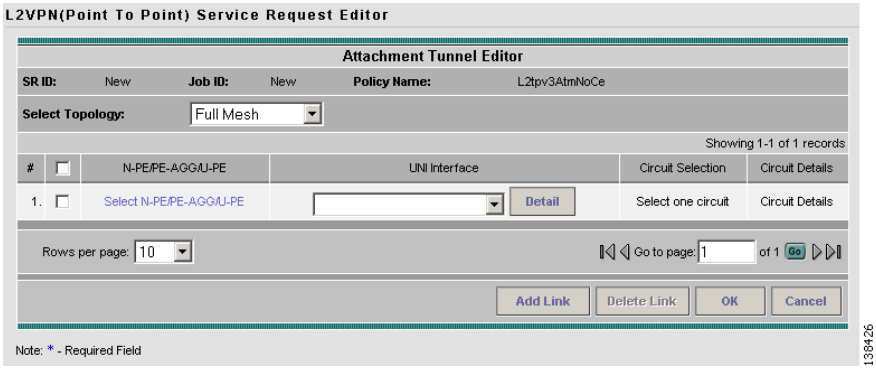
Step 1 Choose a **Topology** from the drop-down list. If you choose **Full Mesh**, each PE will have direct connections to every other PE. If you choose **Hub and Spoke**, then only the Hub PE has connection to each Spoke PE and the Spoke PEs do not have direct connection to each other.

Note The full mesh and the hub and spoke topologies make a difference only when you choose more than two endpoints. For example, with four endpoints, ISC automatically creates six links with full mesh topology. With hub and spoke topology, however, ISC creates only three links.

Step 2 Click **Add Link**.

You specify the PE endpoints using the Attachment Tunnel Editor. You can create one or more PEs from a window like the one in Figure 7-14.

Figure 7-14 Select N-PE/PE-AGG/U-PE



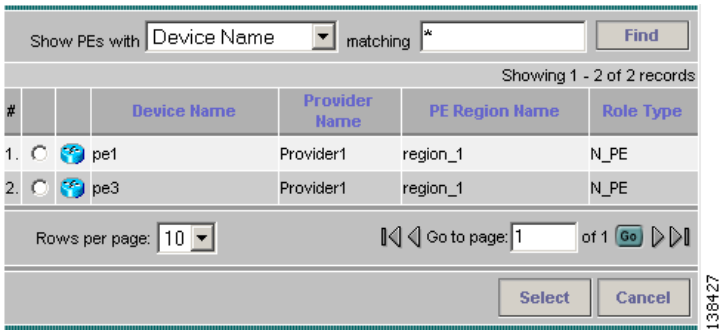
Step 3 Click **Select N-PE/PE-AGG/U-PE** in the N-PE/PE-AGG/U-PE column. The PE for Attachment Circuit window appears (see Figure 7-15). This window displays the list of currently defined PEs.

a. The **Show PEs with** drop-down list shows PEs by customer name, by site, or by device name.

b. The **Find** button allows a search for a specific PE or a refresh of the window.

c. The **Rows per page** drop-down list allows the page to be set to 5, 10, 20, 30, 40, or All.

Figure 7-15 Select PE Device



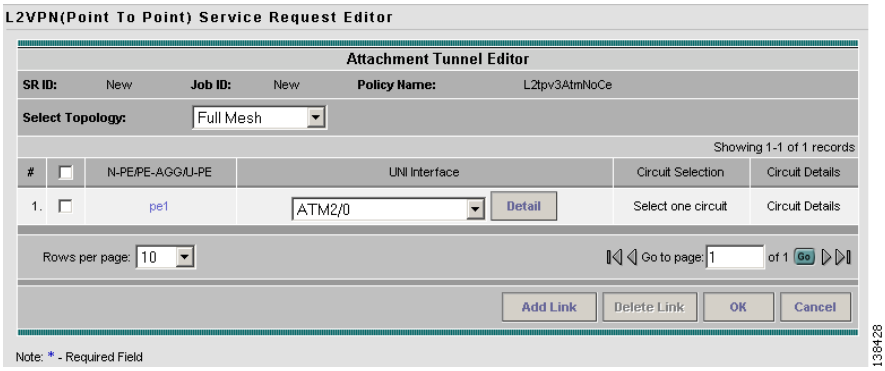
Step 4 In the **Select** column, choose the PE device name for the L2TPv3 link.

Step 5 Click **Select**.

The Service Request Editor window appears displaying the name of the selected PE in the PE column.

Step 6 Select the UNI interface from the drop-down list (see Figure 7-16).

Figure 7-16 Select the UNI Interface

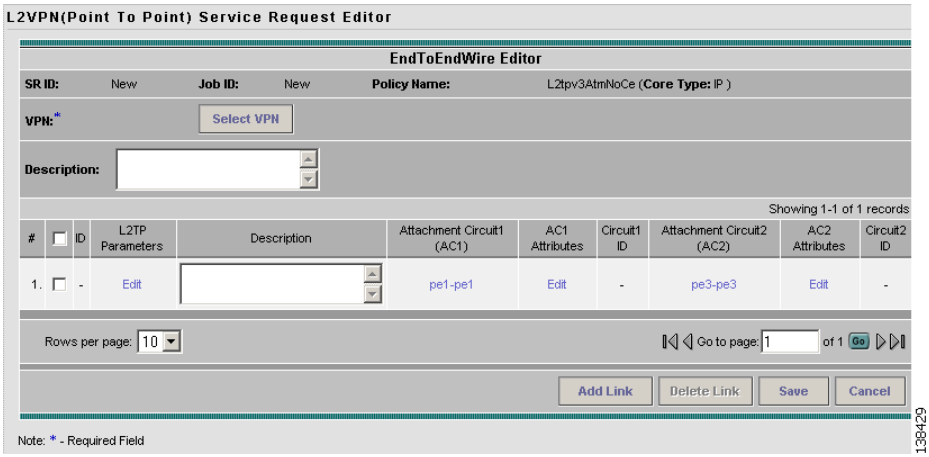


Note Because the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

Step 7 Click **OK**.

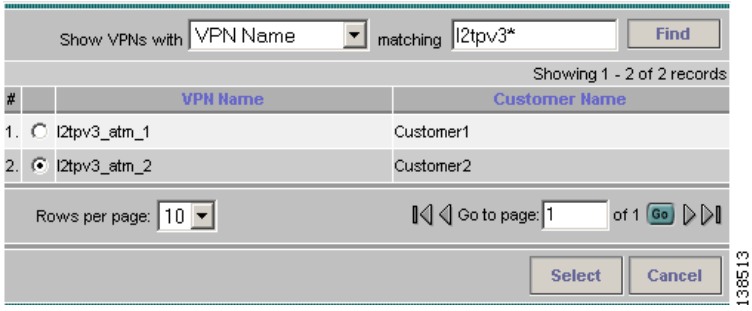
Step 8 The End-to-End-Wire Editor window appears as shown in Figure 7-17.

Figure 7-17 End-to-End Wire Editor



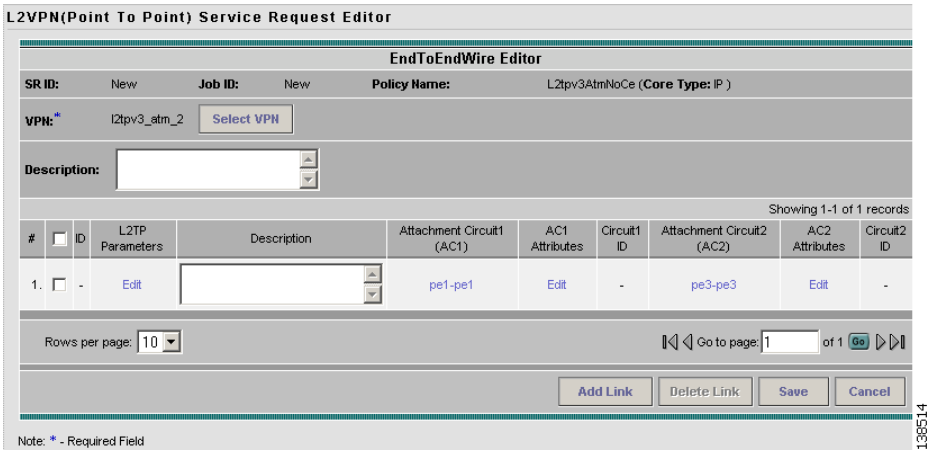
Step 9 The VPN for this service request appears in the Select VPN field. If there is more than one VPN, click **Select VPN** to choose a VPN. The Select VPN for L2TPv3 service request window appears as shown in Figure 7-18.

Figure 7-18 Select VPN for L2TPv3 Service Request



Step 10 Chose a **VPN Name** and click **Select**. The L2TPv3 Service Request Editor window appears with the VPN name displayed as shown in Figure 7-19.

Figure 7-19 Attachment Circuit Selection



You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end link in the **Description** field provided for each link. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

Step 11 When you are finished editing the end-to-end wires, click **Save**.

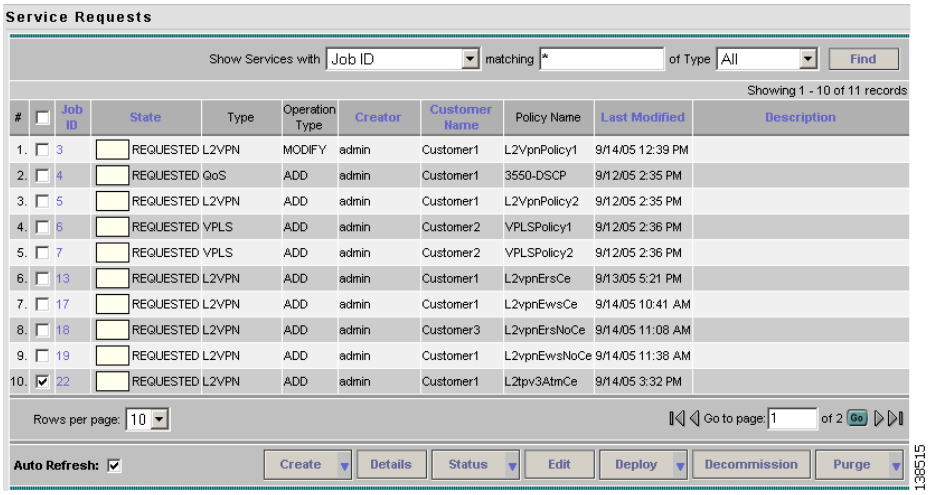
The service request is created and saved into ISC.

Modifying the L2TPv3 Service Request

After you choose all the CE end points and the NPC from the CE, go to the End-to-End Wire Editor and work on the end-to-end wire—the end-to-end connection that links two CEs. An end-to-end wire is a virtual logical link between a CE-CE pair. Each end-to-end-wire is associated with one end-to-end wire attribute and two attachment circuits (ACs). An AC is a virtual logical link between a CE-PE pair. Each AC is associated with one set of AC attributes and one or more L2TPv3 logical links.

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**. See Figure 7-20.

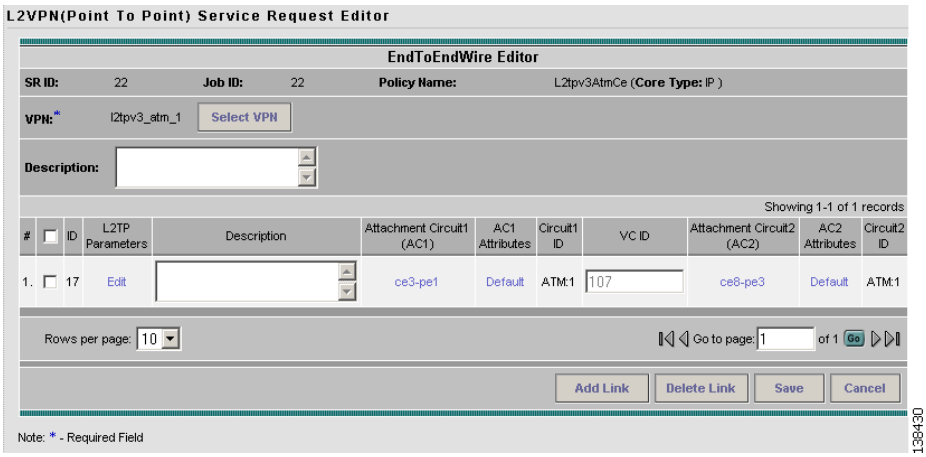
Figure 7-20 L2TPv3 Service Activation



Step 2 Select a check box for a service request.

Step 3 Click **Edit**. The End-to-End-Wire Editor window appears as shown in Figure 7-21.

Figure 7-21 End-to-End Wire Editor



Step 4 The VPN for this service request appears in the Select VPN field. If this request has more than one service request, click **Select** to choose a VPN.

You can choose any of the blue highlighted values to edit the End-to-End Wire.

You can also click **Add Link** to add an end-to-end wire.

You can click **Delete Link** to delete an end-to-end wire.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

You can enter a description for each end-to-end link in the **Description** field provided for each link. The description shows up only in this window. The data in this field is not pushed to the device(s). The maximum length for this field is 256 characters.

The ID number is system-generated identification number for the circuit.

The Circuit ID is created automatically, based on the service. For example, for Ethernet, it is based on the VLAN number; for Frame Relay, it is based on the DLCI; for ATM, it is based on the VPI/VCI.

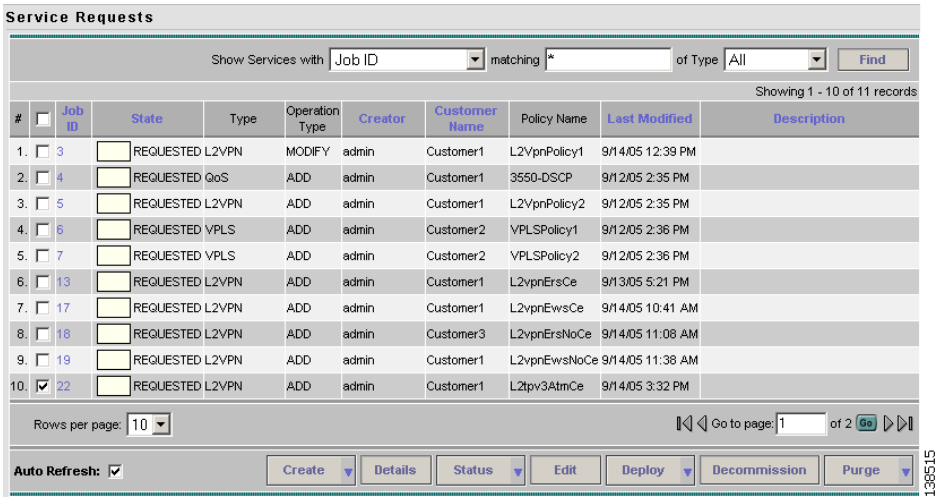
Step 5 When you are finished editing the end-to-end wires, click **Save**.

Saving the L2TPv3 Service Request

When you are finished with Link Attributes for all the Attachment Circuits, click **Save** to finish the L2TPv3 service request creation as shown in Figure 7-22.

If the L2TPv3 service request is successfully created, you will see the service request list window where the newly created L2TPv3 service request is added with the state of REQUESTED as shown in Figure 7-22. If, however, the L2TPv3 service request creation failed for some reason (for example, the value chosen is out of bounds), you are warned with an error message. Go back to correct the error and **Save** again.

Figure 7-22 L2TPv3 Service Request Created



#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	3	REQUESTED	L2VPN	MODIFY	admin	Customer1	L2VpnPolicy1	9/14/05 12:39 PM	
2.	4	REQUESTED	QoS	ADD	admin	Customer1	3550-DSCP	9/12/05 2:35 PM	
3.	5	REQUESTED	L2VPN	ADD	admin	Customer1	L2VpnPolicy2	9/12/05 2:35 PM	
4.	6	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy1	9/12/05 2:36 PM	
5.	7	REQUESTED	VPLS	ADD	admin	Customer2	VPLSPolicy2	9/12/05 2:36 PM	
6.	13	REQUESTED	L2VPN	ADD	admin	Customer1	L2vpnErsCe	9/13/05 5:21 PM	
7.	17	REQUESTED	L2VPN	ADD	admin	Customer1	L2vpnEwsCe	9/14/05 10:41 AM	
8.	18	REQUESTED	L2VPN	ADD	admin	Customer3	L2vpnErsNoCe	9/14/05 11:08 AM	
9.	19	REQUESTED	L2VPN	ADD	admin	Customer1	L2vpnEwsNoCe	9/14/05 11:38 AM	
10.	22	REQUESTED	L2VPN	ADD	admin	Customer1	L2tpv3AtmCe	9/14/05 3:32 PM	

The L2TPv3 service request is in Requested state. See Deploying Service Requests, page 12-1 for information on deploying L2TPv3 service requests.

Creating a VPLS Policy

This chapter contains the basic steps to create a VPLS policy. It contains the following sections:

Defining a VPLS Policy

You must define a VPLS policy before you can provision a service. A VPLS policy defines the common characteristics shared by the Attachment Circuit (AC) attributes.

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is *not* set to editable, the service request creator cannot change the policy item.

VPLS policies correspond to the one of the core types that VPLS provides:

- MPLS core type—provider core network is MPLS enabled
- Ethernet core type—provider core network uses Ethernet switches

and to one of the service types that VPLS provides:

- Multi-point Ethernet Relay Service (ERS)
- Multi-point Ethernet Wire Service (EWS)

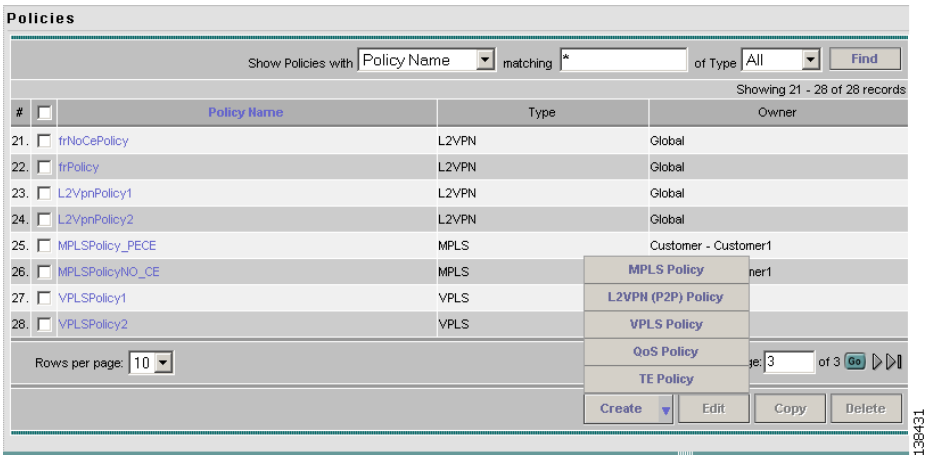
A policy is a template of most of the parameters needed to define a VPLS service request. After you define it, a VPLS policy can be used by all the VPLS service requests that share a common set of characteristics.

You create a new VPLS policy whenever you create a new type of service or a service with different parameters. VPLS policy creation is normally performed by experienced network engineers.

To define a VPLS policy in the Cisco IP Solution Center (ISC), use the following steps. See Figure 8-1.

Step 1 Select **Service Design** > **Policies**. The Policies window appears as show in Figure 8-1.

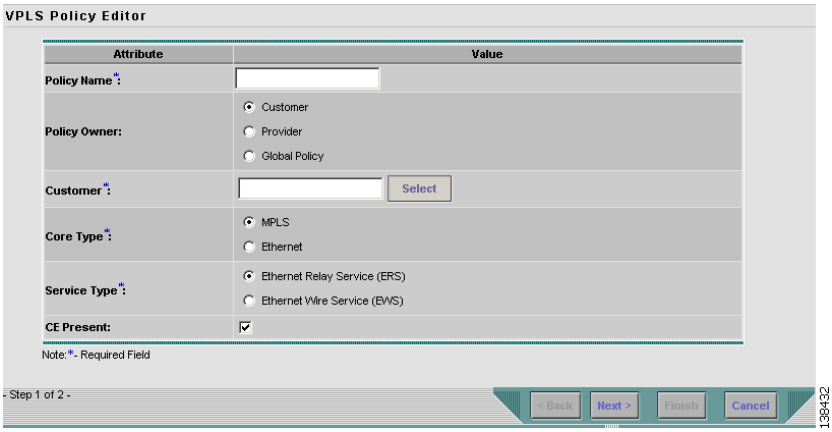
Figure 8-1 Creating a Policy



Step 2 Click **Create**.

Step 3 Select **VPLS Policy**. The VPLS Policy Editor window in Figure 8-2 appears:

Figure 8-2 Creating a VPLS Policy



Step 4 Enter a **Policy Name** for the VPLS policy.

Step 5 Choose the **Policy Owner** for the VPLS policy.

There are three types of VPLS policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this VPLS policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, a VPLS policy that is customer owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 6 Click **Select** to choose the owner of the VPLS policy. The policy owner was established when you created customers or providers during ISC setup. If the ownership is global, the Select function does not appear.

Step 7 Choose the **Core Type** of the VPLS policy.

There are two core types for VPLS policies:

- MPLS—running on an IP network
- Ethernet—all PEs are on an Ethernet provider network

Step 8 Choose the **Service Type** of the VPLS policy.

There are two service types for VPLS policies:

- Multi-point Ethernet Relay Service (ERS)
- Multi-point Ethernet Wire Service (EWS)

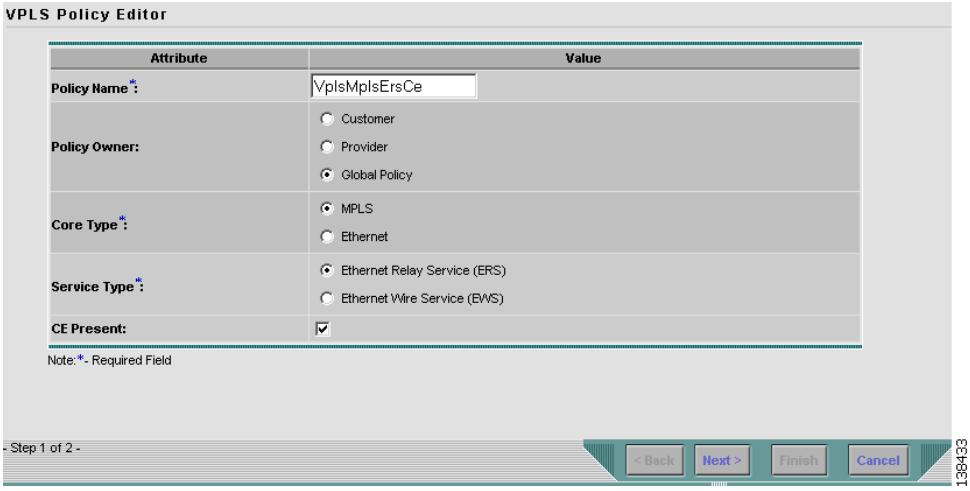
Step 9 Select the **CE Present** check box if you want ISC to ask the service operator who uses this VPLS policy to provide a CE router and interface during service activation. The default is CE present in the service.

If you do not select the **CE Present** check box, ISC asks the service operator, during service activation, only for the PE router and customer-facing interface.

Defining an MPLS/ERS Policy with a CE

This section describes how to define a VPLS policy with an MPLS core type and an ERS service type with CE present. Figure 8-3 is an example of the first page of this policy.

Figure 8-3 MPLS/ERS Policy with a CE

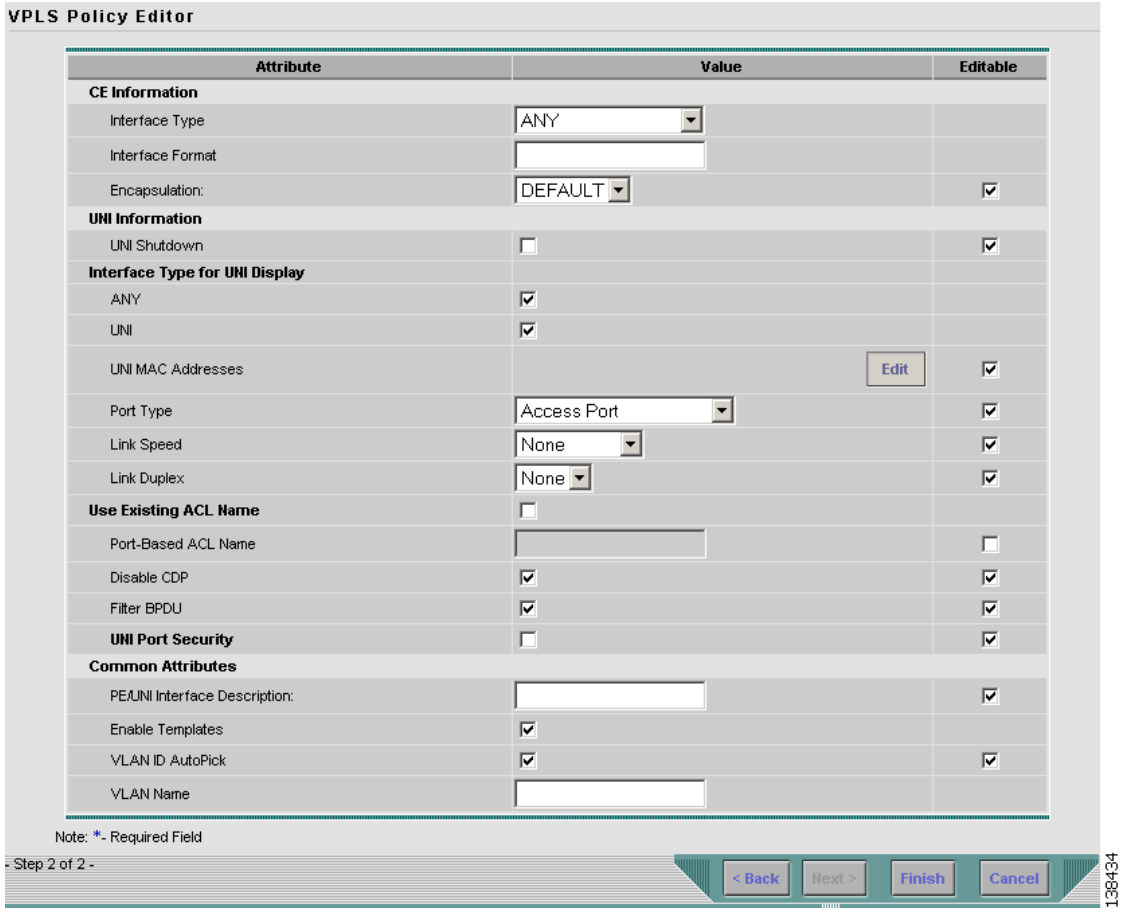


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-4 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-4 MPLS/ERS with a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, PE-AGG, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 7 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Choose a **Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 9 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 10 Enter a **Line Duplex** of none, full, half, or auto.

Step 11 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 12 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 13 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 14 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 15 Select the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 16 Select the **UNI Port Security** check box (see Figure 8-5) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

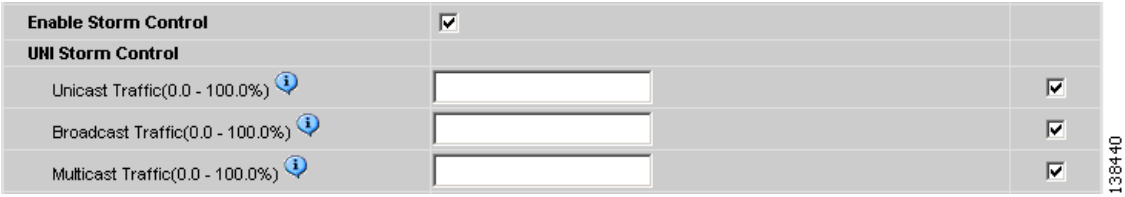
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses. Click the **Edit** button to enter the addresses.

Figure 8-5 UNI Port Security

Step 17 Select the **Enable Storm Control** check box (see Figure 8-6) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-6 Enable Storm Control



Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERS Service*.

Step 19 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 20 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 21 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

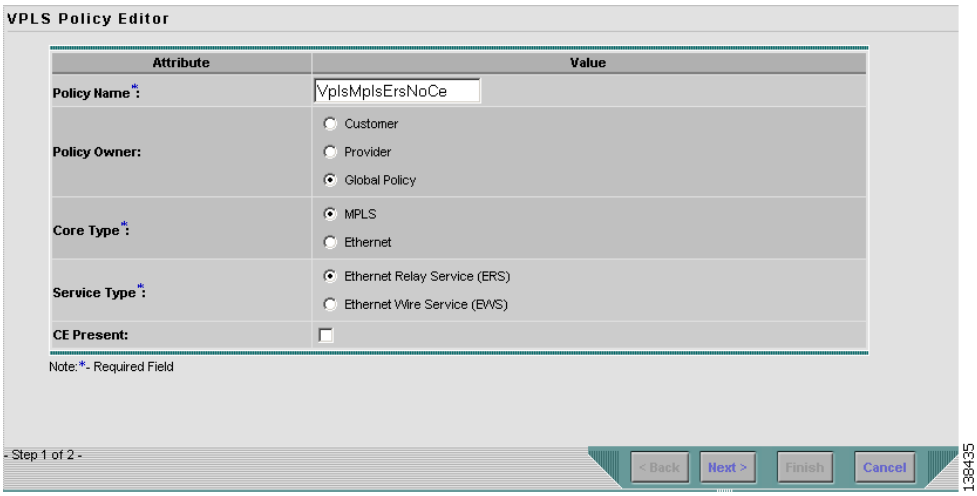
Step 22 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an MPLS/ERS Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an ERS service type without a CE present. Figure 8-7 is an example of the first page of this policy.

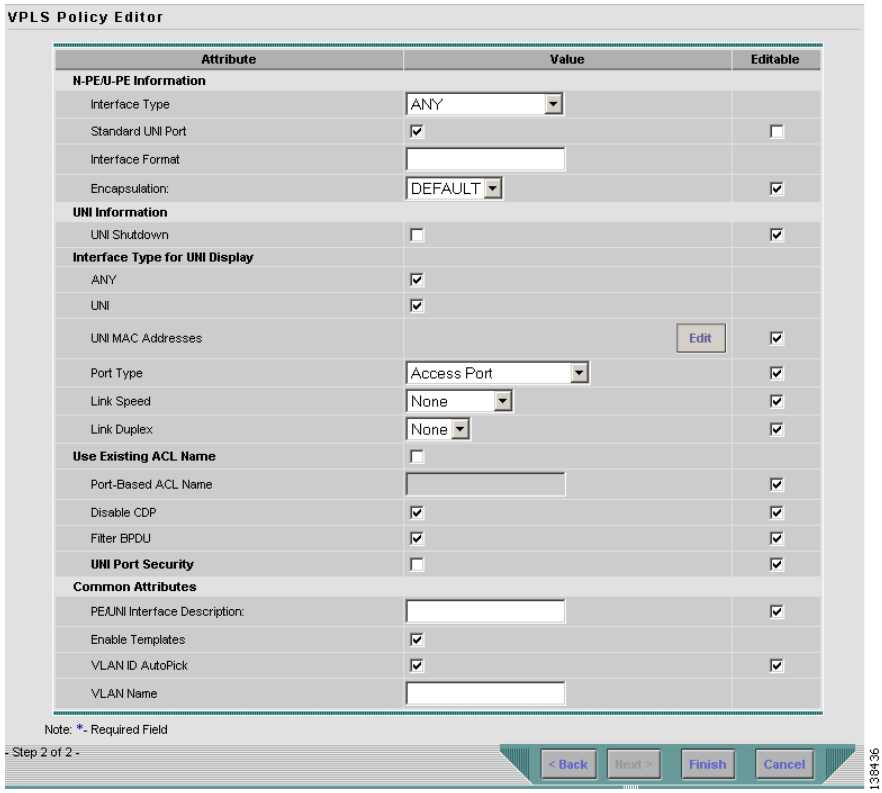
Figure 8-7 MPLS/ERS Policy without a CE



Step 1 Click **Next**. The window in Figure 8-8 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-8 MPLS/ERS without a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Step 6 Check **UNI Shutdown** box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 9 Choose a **Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 10 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 11 Enter a **Line Duplex** of none, full, half, or auto.

Step 12 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 13 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 16 Select the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 17 Select the **UNI Port Security** check box (see Figure 8-9) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

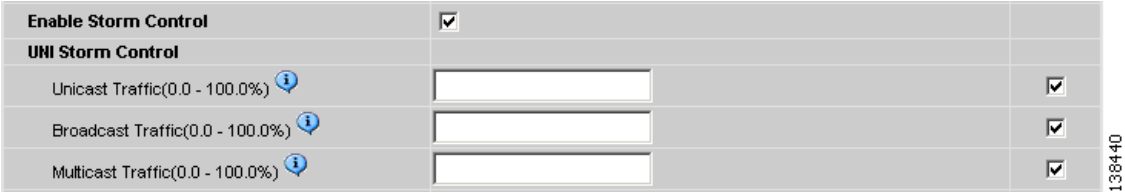
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-9 UNI Port Security

Step 18 Select the **Enable Storm Control** check box (see Figure 8-10) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-10 Enable Storm Control



Step 19 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERS Service*.

Step 20 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 21 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 22 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

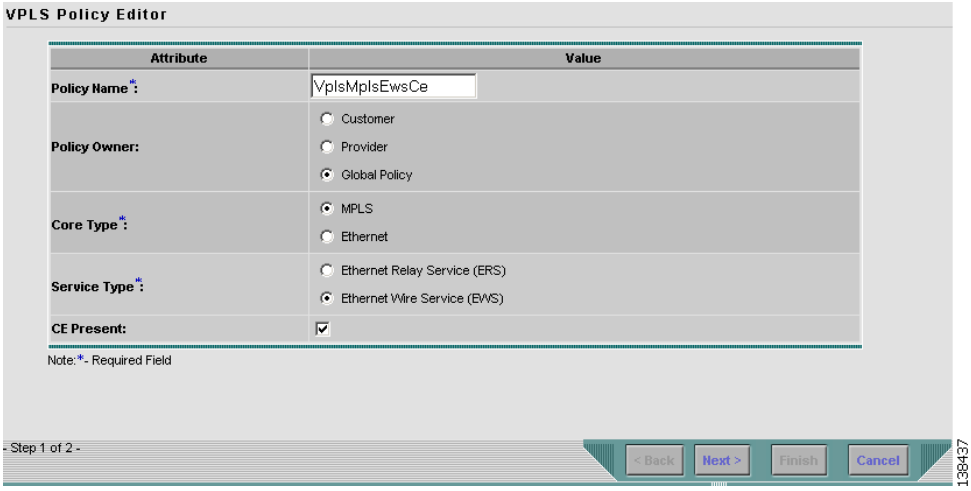
Step 23 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an MPLS/EWS Policy with a CE

This section describes defining a VPLS policy with an MPLS core type and an EWS service type with CE present. Figure 8-11 is an example of the first page of this policy.

Figure 8-11 MPLS/EWS Policy with a CE

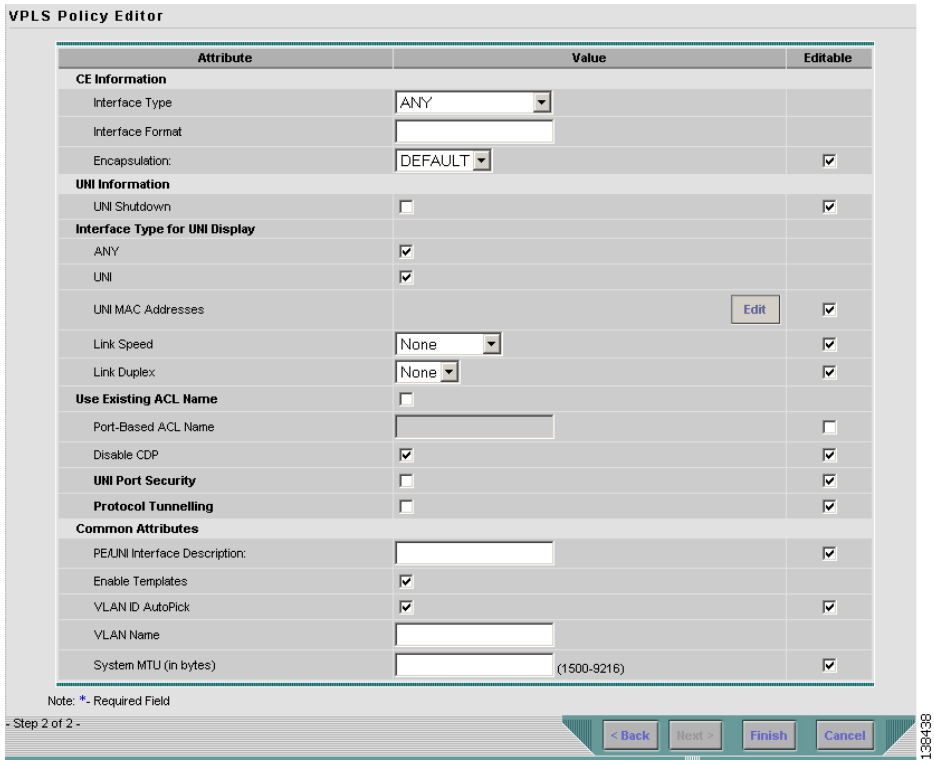


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-12 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-12 MPLS/EWS with a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 7 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 9 Enter a **Line Duplex** of none, full, half, or auto.

Step 10 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 11 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 12 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 13 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 14 Select the **UNI Port Security** check box (see Figure 8-13) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

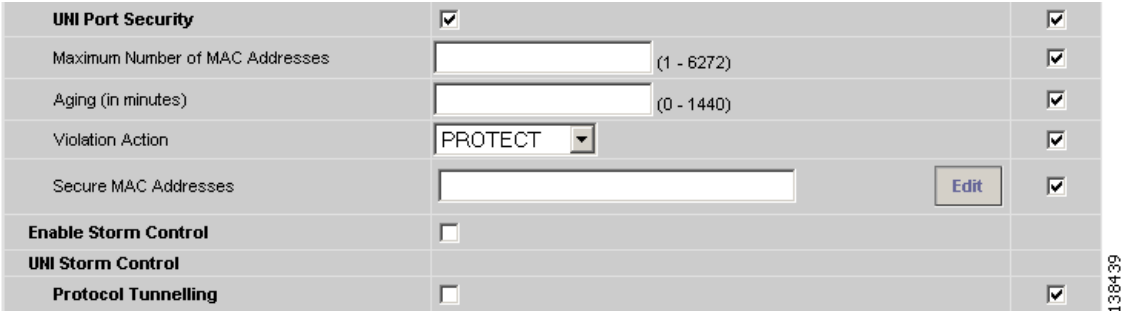
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

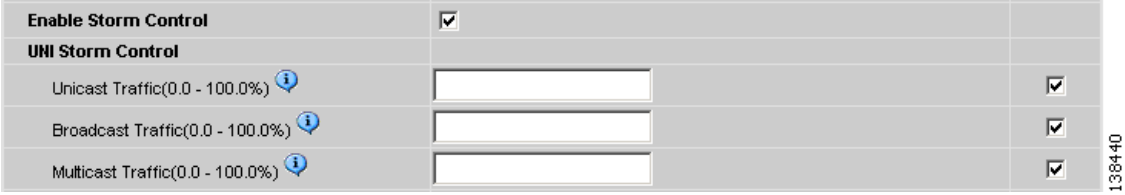
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-13 UNI Port Security



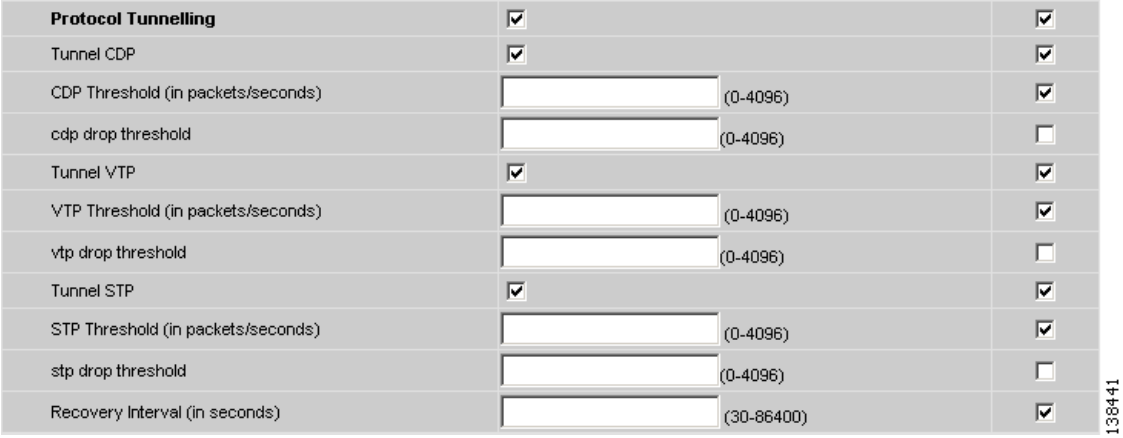
Step 15 Select the **Enable Storm Control** check box (see Figure 8-14) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-14 Enable Storm Control



Step 16 Select the **Protocol Tunnelling** check box (see Figure 8-15) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 8-15 Protocol Tunnelling



For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

a. **Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **CDP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Tunnel STP—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **STP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 17 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EWS Service*.

Step 18 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 19 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Enter the **System MTU** in bytes.

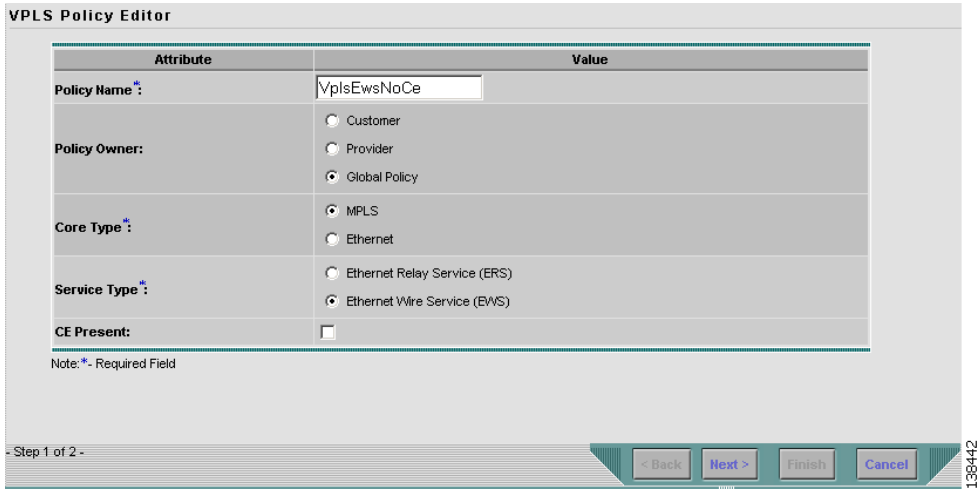
Step 22 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an MPLS/EWS Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an EWS service type without a CE present. Figure 8-16 is an example of the first page of this policy.

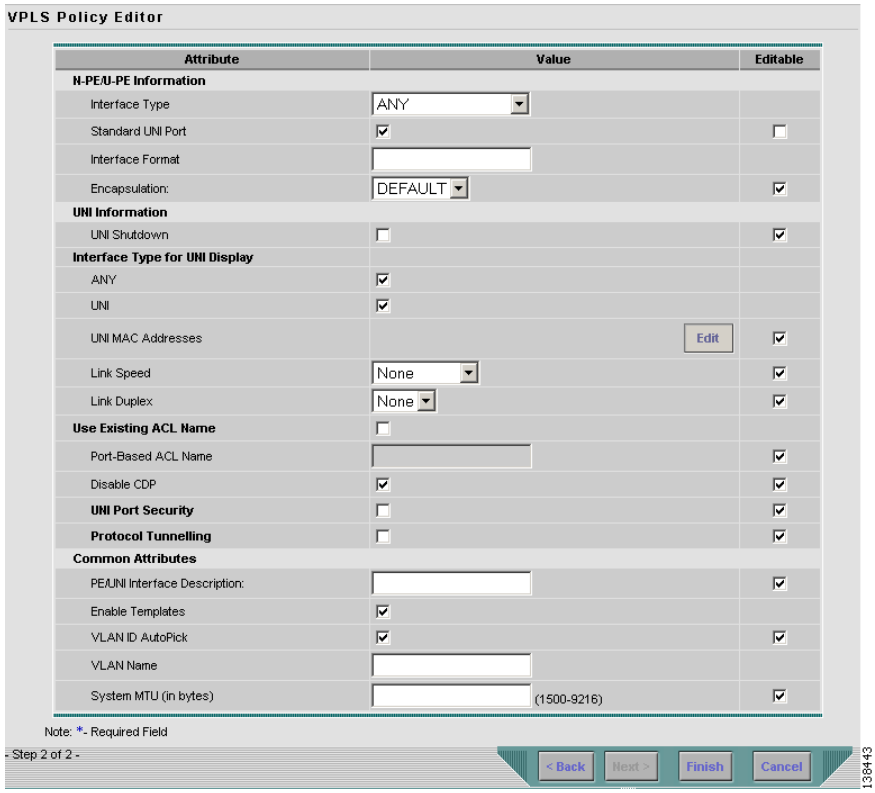
Figure 8-16 MPLS/EWS Policy without a CE



Step 1 Click **Next**. The window in Figure 8-17 appears.

The **Editable** check box gives you the option of making a field editable. If you select **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-17 MPLS/EWS without a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an N-PE/U-PE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 9 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 10 Enter a **Line Duplex** of none, full, half, or auto.

Step 11 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 12 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 13 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 14 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 15 Select the **UNI Port Security** check box (see Figure 8-18) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

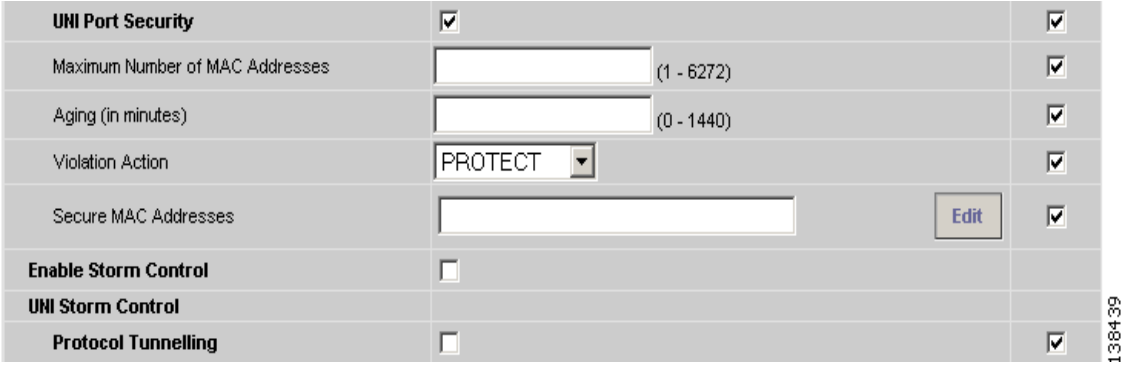
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

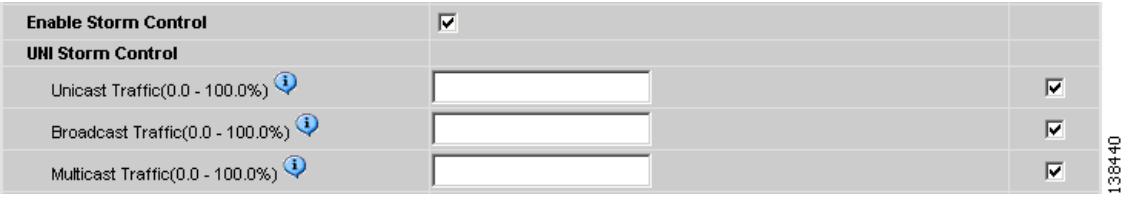
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-18 UNI Port Security



Step 16 Select the **Enable Storm Control** check box (see Figure 8-19) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-19 Enable Storm Control



Step 17 Select the **Protocol Tunnelling** check box (see Figure 8-20) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 8-20 Protocol Tunnelling

Protocol Tunnelling	☑		☑
Tunnel CDP	☑		☑
CDP Threshold (in packets/seconds)		(0-4096)	☑
cdp drop threshold		(0-4096)	☐
Tunnel VTP	☑		☑
VTP Threshold (in packets/seconds)		(0-4096)	☑
vtp drop threshold		(0-4096)	☐
Tunnel STP	☑		☑
STP Threshold (in packets/seconds)		(0-4096)	☑
stp drop threshold		(0-4096)	☐
Recovery Interval (in seconds)		(30-86400)	☑

138441

For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

a. **Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **CDP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Tunnel STP—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **STP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EWS Service*.

Step 19 Check the **Enable Templates** box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 20 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 21 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 22 Enter the **System MTU** in bytes.

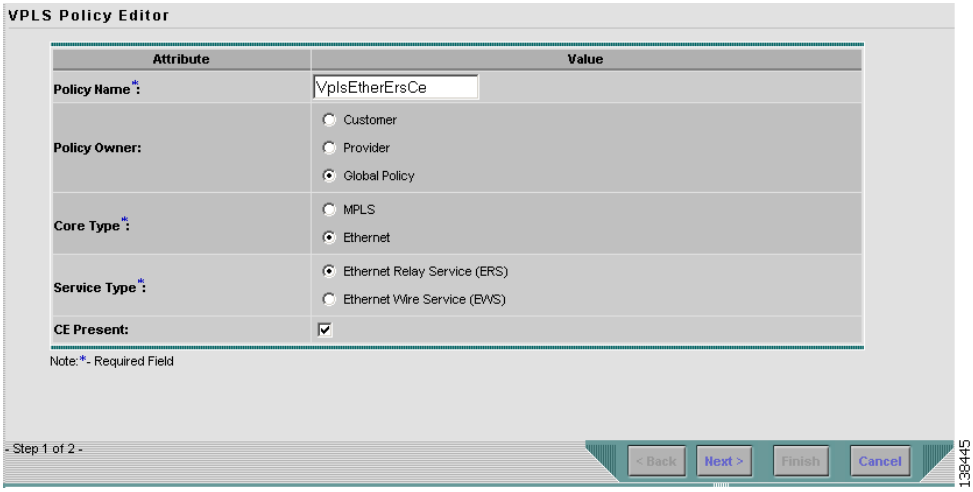
Step 23 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an Ethernet/ERS Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERS service type with CE present. Figure 8-21 is an example of the first page of this policy.

Figure 8-21 Ethernet/ERS Policy with a CE

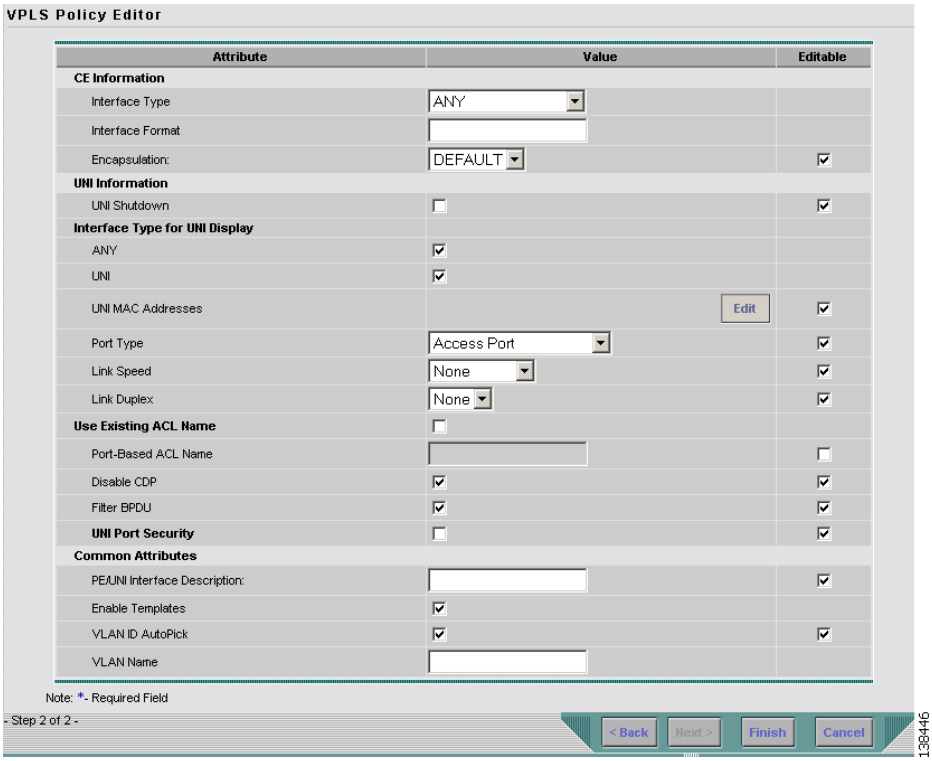


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-22 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-22 Ethernet ERS with a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 7 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Choose a **Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 9 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 10 Enter a **Line Duplex** of none, full, half, or auto.

Step 11 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 12 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 13 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 14 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 15 Select the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 16 Select the **UNI Port Security** check box (see Figure 8-23) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

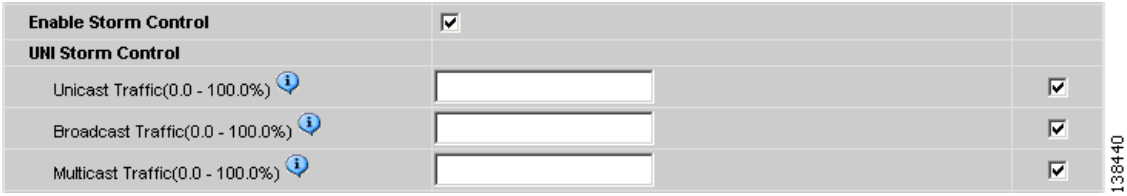
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-23 UNI Port Security

Step 17 Select the **Enable Storm Control** check box (see Figure 8-23) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-24 Enable Storm Control



Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERS Service*.

Step 19 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 20 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 21 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

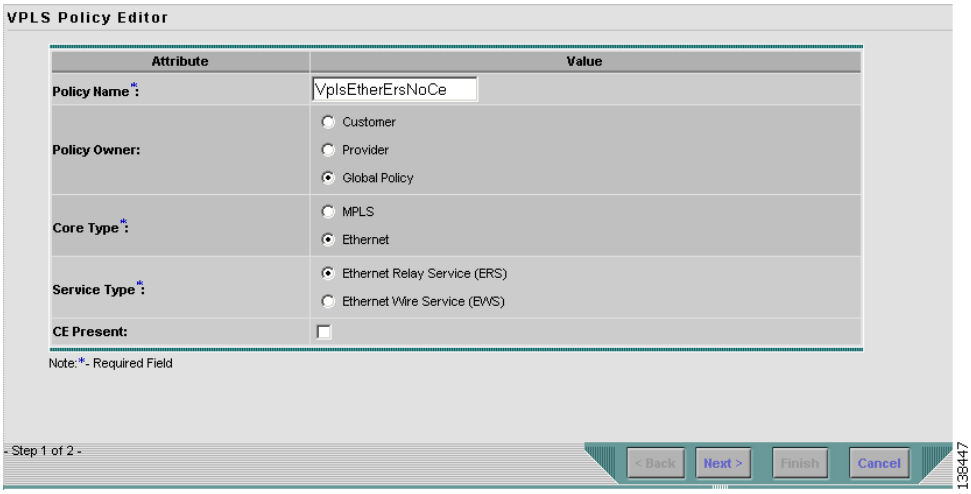
Step 22 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an Ethernet/ERS Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERS service type without a CE present. Figure 8-25 is an example of the first page of this policy.

Figure 8-25 Ethernet/ERS Policy without a CE

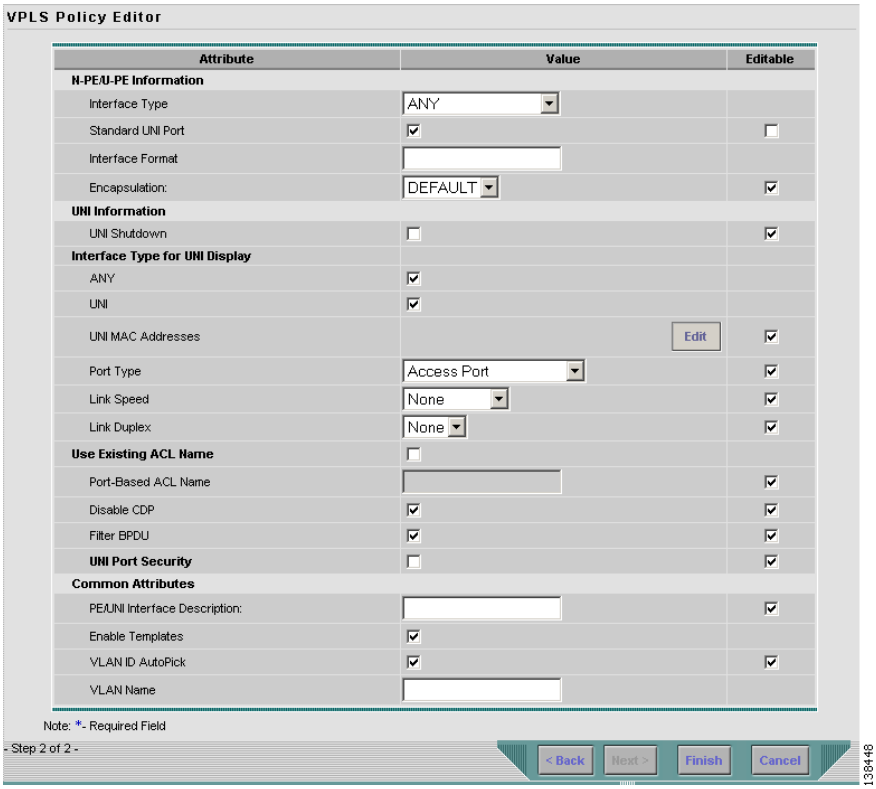


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-26 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-26 Ethernet/ERS without a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 9 Choose a **Port Type**. The choices are:

- **Access Port**
- **Trunk with Native VLAN**

Step 10 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 11 Enter a **Line Duplex** of none, full, half, or auto.

Step 12 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 13 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 14 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 15 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 16 Select the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

Step 17 Select the **UNI Port Security** check box (see Figure 8-27) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

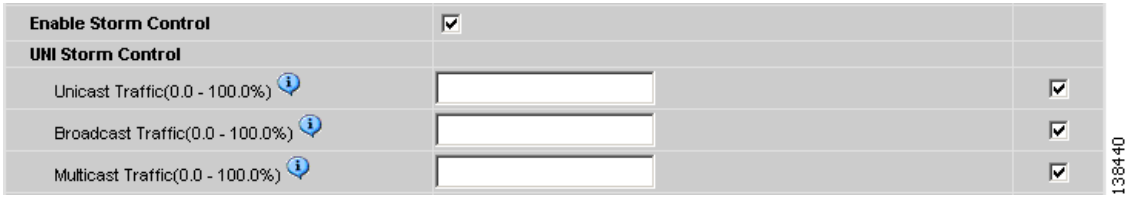
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-27 UNI Port Security

Step 18 Select the **Enable Storm Control** check box (see Figure 8-28) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-28 Enable Storm Control



Step 19 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERS Service*.

Step 20 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 21 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 22 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

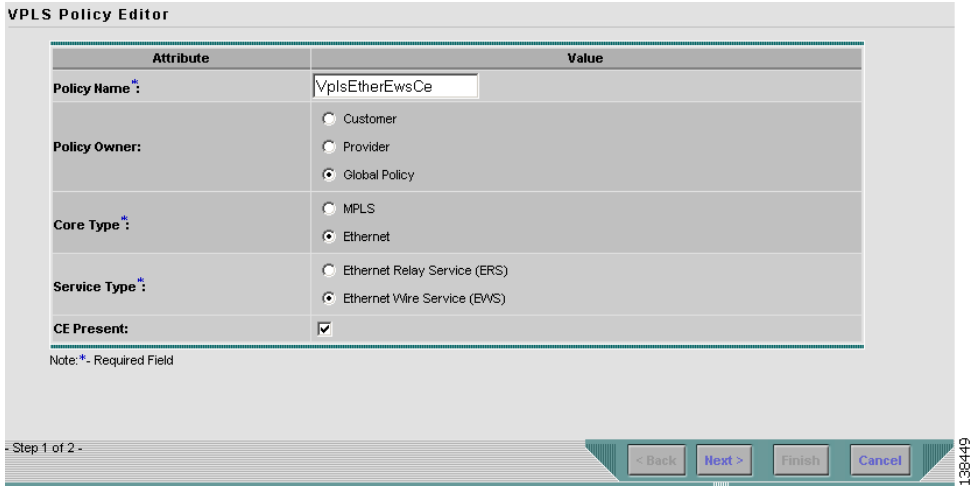
Step 23 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an Ethernet/EWS Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERS service type with a CE present. Figure 8-29 is an example of the first page of this policy.

Figure 8-29 Ethernet/EWS Policy with CE Present

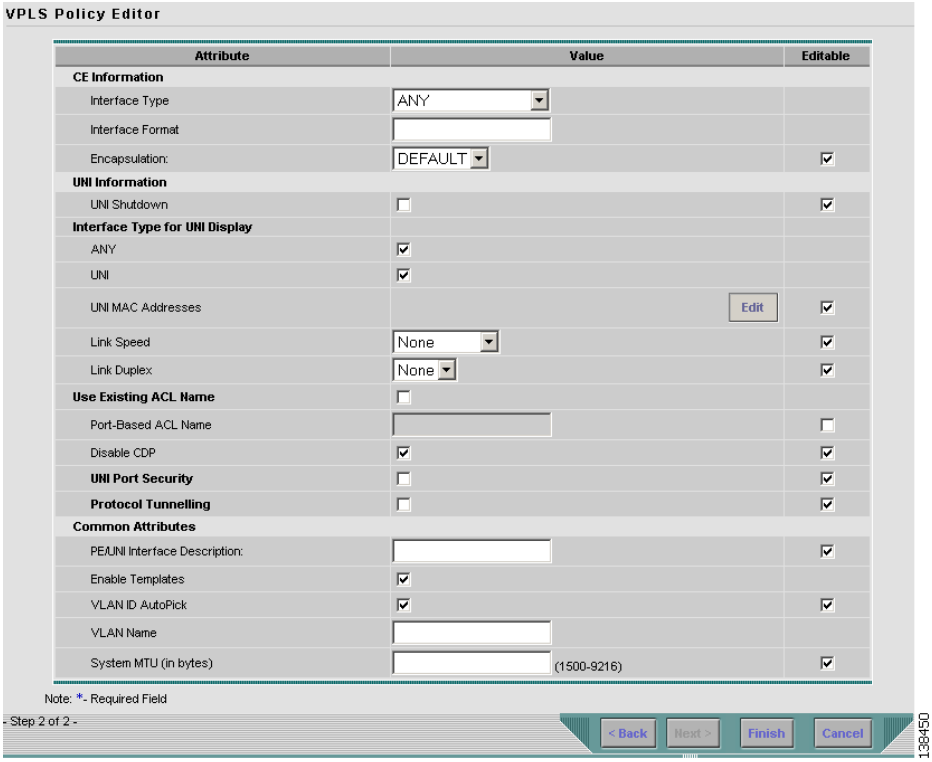


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-30 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-30 Ethernet/EWS with a CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

Step 5 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 7 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 9 Enter a **Line Duplex** of none, full, half, or auto.

Step 10 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 11 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 12 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 13 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 14 Select the **UNI Port Security** check box (see Figure 8-31) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

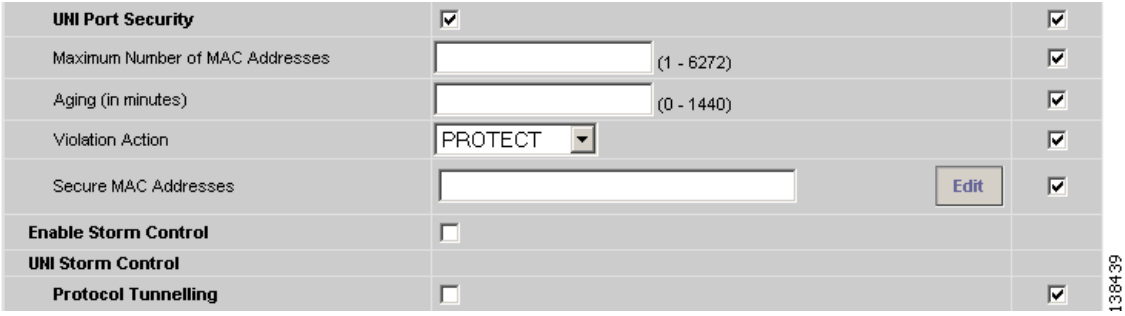
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

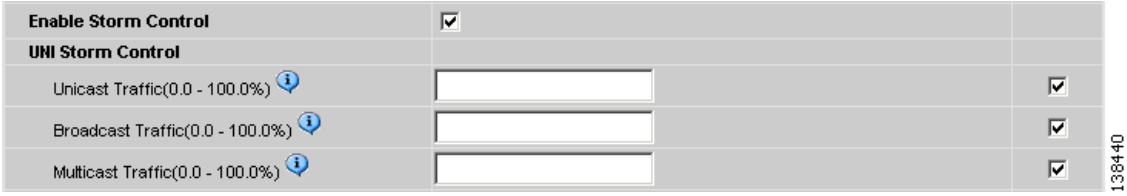
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-31 UNI Port Security



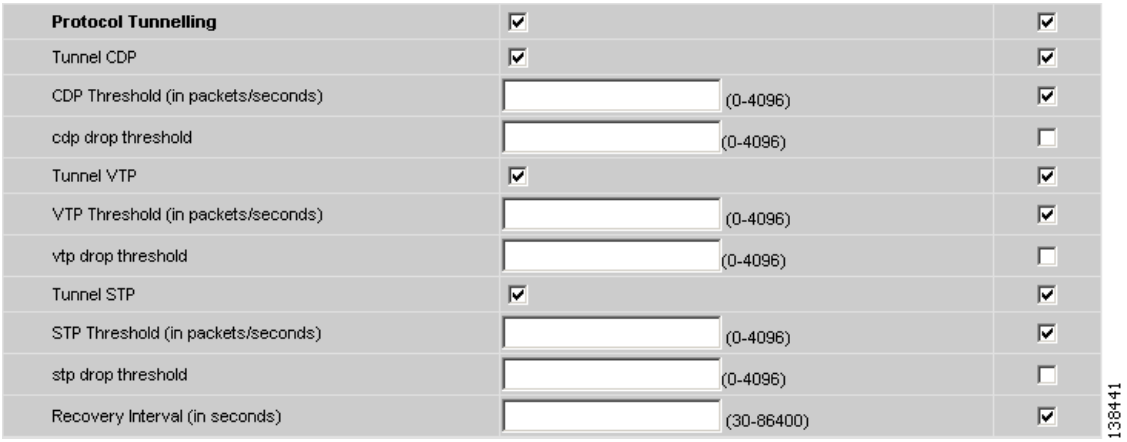
Step 15 Select the **Enable Storm Control** check box (see Figure 8-32) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-32 Enable Storm Control



Step 16 Select the **Protocol Tunnelling** check box (see Figure 8-33) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 8-33 Protocol Tunnelling



For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

a. **Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **CDP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Tunnel STP—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **STP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 17 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EWS Service*.

Step 18 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 19 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 20 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 21 Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 4.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

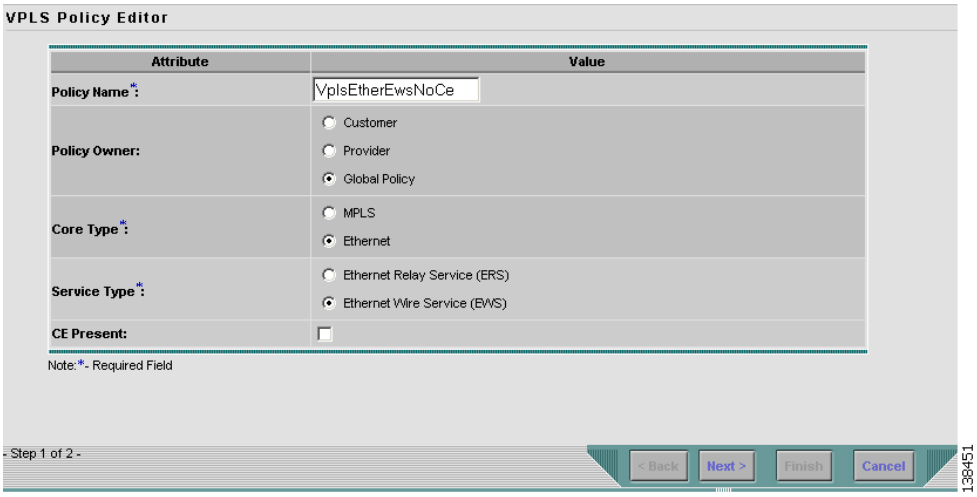
Step 22 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Defining an Ethernet/EWS Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an EWS service type without a CE present. Figure 8-34 is an example of the first page of this policy.

Figure 8-34 Ethernet/EWS Policy without a CE

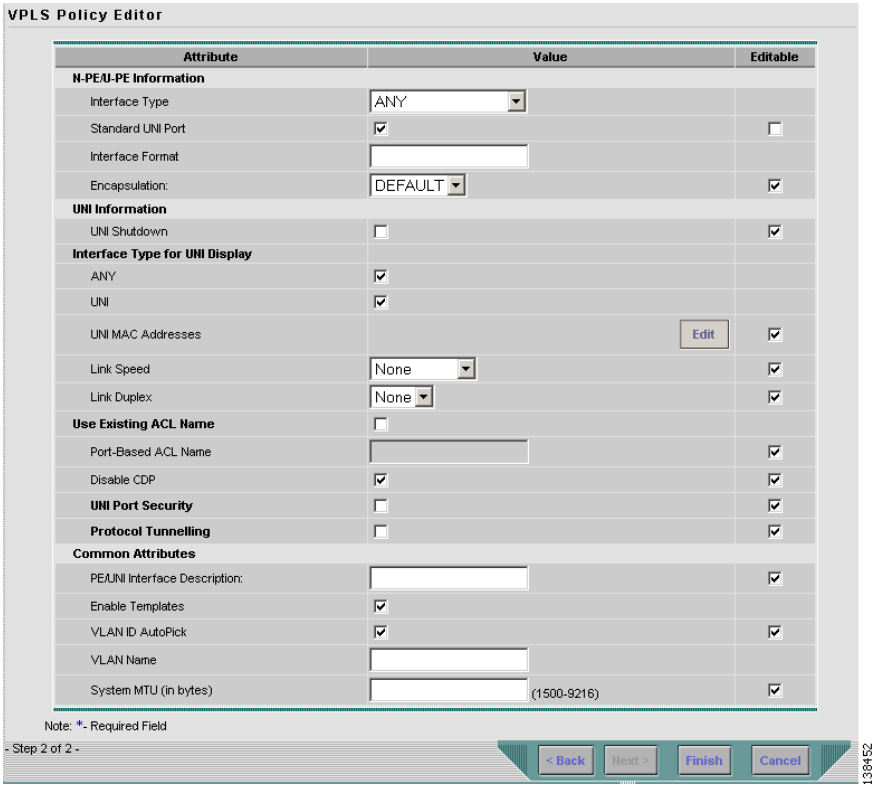


Perform the following steps.

Step 1 Click **Next**. The window in Figure 8-35 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 8-35 Ethernet/EWS without CE Policy Attributes



Step 2 Choose an **Interface Type** from the drop-down list.

You can choose to select a particular interface on a CE, N-PE, U-PE, or PE-AGG interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**

The value defined here functions as a filter to restrict the interface types an operator can see during VPLS service request creation. If defined as ANY, the operator can see all interface types.

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a CE **Encapsulation** type. The choices are:

- **DOT1Q**
- **DEFAULT**

Step 6 Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Select the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 8 Select the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy). This check box is checked by default.

Step 9 Enter a **Link Speed** of none, 10, 100, 1000, or auto.

Step 10 Enter a **Line Duplex** of none, full, half, or auto.

Step 11 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not selected and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 12 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 13 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 14 Select the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

Step 15 Select the **UNI Port Security** check box (see Figure 8-36) if you to want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.

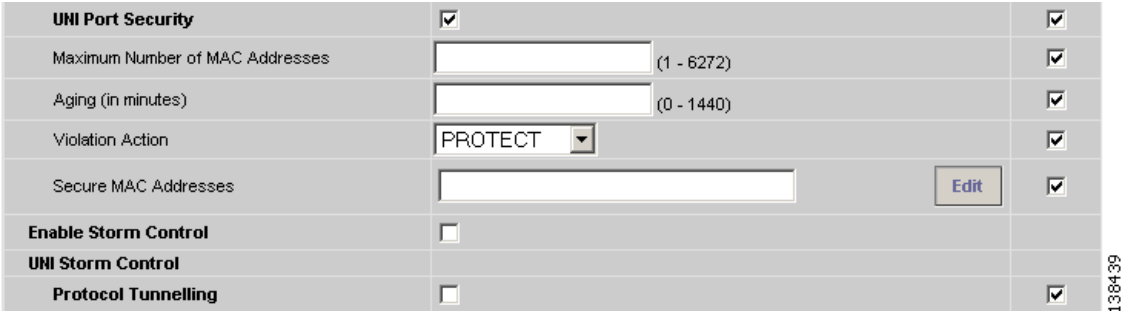
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

c. For **Violation Action**, choose what action will occur when a port security violation is detected:

- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
- **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 8-36 UNI Port Security

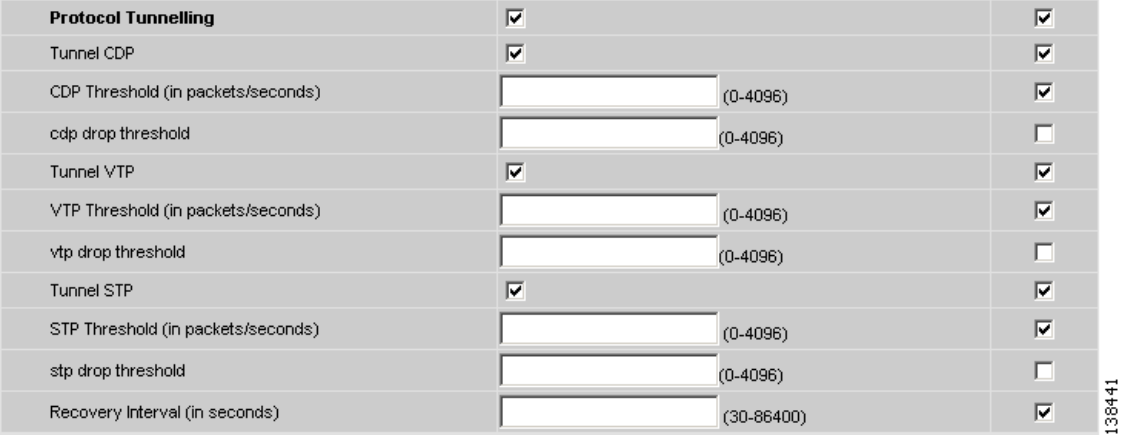


Step 16 Select the **Enable Storm Control** check box (see Figure 8-37) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 8-37 Enable Storm Control

Step 17 Select the **Protocol Tunnelling** check box (see Figure 8-38) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 8-38 Protocol Tunnelling



For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

a. **Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **CDP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **VTP threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Tunnel STP—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **STP Threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 18 In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EWS Service*.

Step 19 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the routers commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 20 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 21 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN. The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique. Two VLANs cannot share the same name.

Step 22 Enter the **System MTU** in bytes.

Step 23 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 4.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 24 Click **Finish**.

Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Managing a VPLS Service Request

This chapter contains the basic steps to provision a VPLS service. It contains the following sections:

Introducing VPLS Service Requests

A VPLS service request consists of one or more attachment circuits, connecting various sites in a multi-point topology. When you create a service request, you enter several parameters, including the specific interfaces on the CE and PE routers and UNI parameters.

You can also integrate a Cisco IP Solution Center (ISC) template with a service request. You can associate one or more templates to the CE, PE, or any U-PE in the middle.

To create a service request, a service policy must already be defined, as described in Chapter 8, "Creating a VPLS Policy."

Based on the predefined VPLS policy, an operator creates a VPLS service request, with or without modifications to the VPLS policy, and deploys the service. The service request must be the same service type (ERS or EWS) as the policy selected.

Service creation and deployment are normally performed by regular network technicians for daily operation of network provisioning.

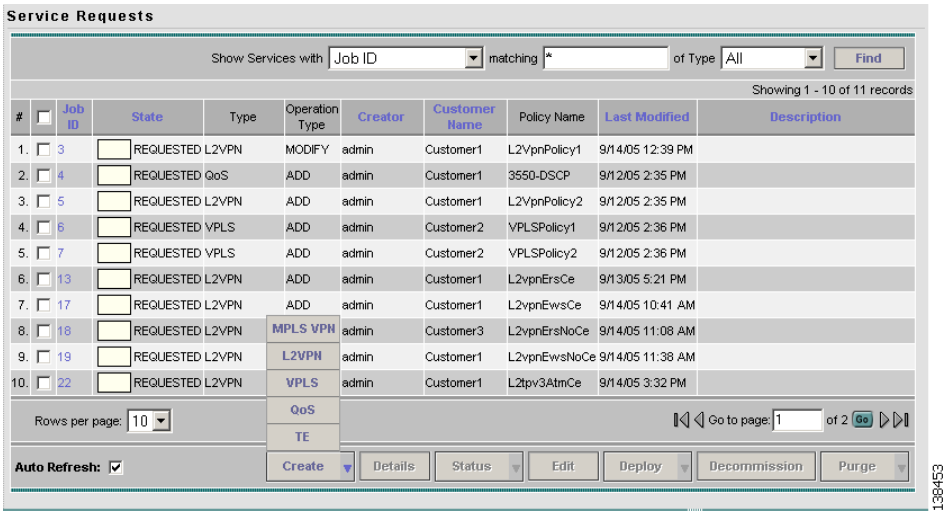
The following steps are involved in creating a service request for Layer 2 connectivity between customer sites:

- Choose a VPLS policy.
- Choose a VPN. See the Defining VPNs, page 3-4, for further information.
- Choose a CE or UNI interface.
- Choose a Named Physical Circuit (NPC) if more than one NPC exists from the CE or the UNI interface.
- Edit the link attributes.

Choosing a VPLS Policy

Step 1 Select **Service Inventory > Inventory and Connection Manager > Service Requests**. The Service Requests window appears as show in Figure 9-1.

Figure 9-1 VPLS Service Activation



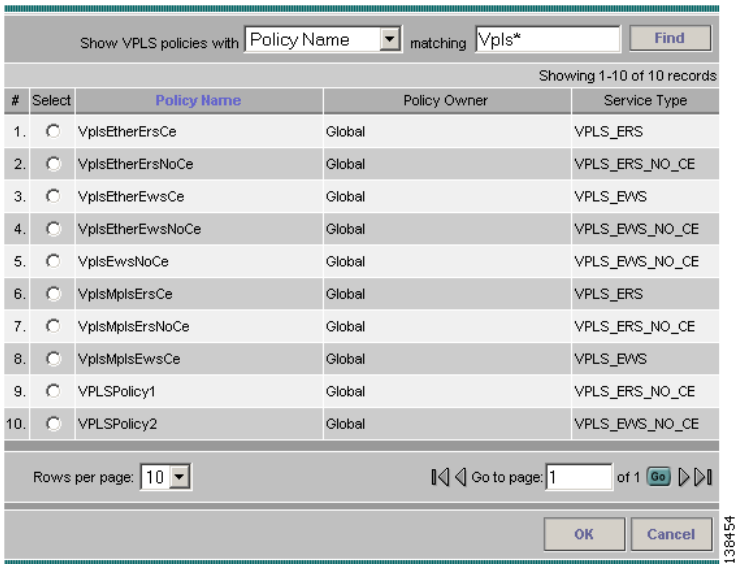
Step 2 Click **Create**.

Step 3 Choose **VPLS** from the drop-down list.

VPLS service requests must be associated with a VPLS policy. You choose a VPLS policy from the policies previously created (see Chapter 8, "Creating a VPLS Policy").

Step 4 Select the button for the VPLS policy of choice. See Figure 9-2. If more than one VPLS policy exists, a list of VPLS policies appears.

Figure 9-2 VPLS Policy Choice



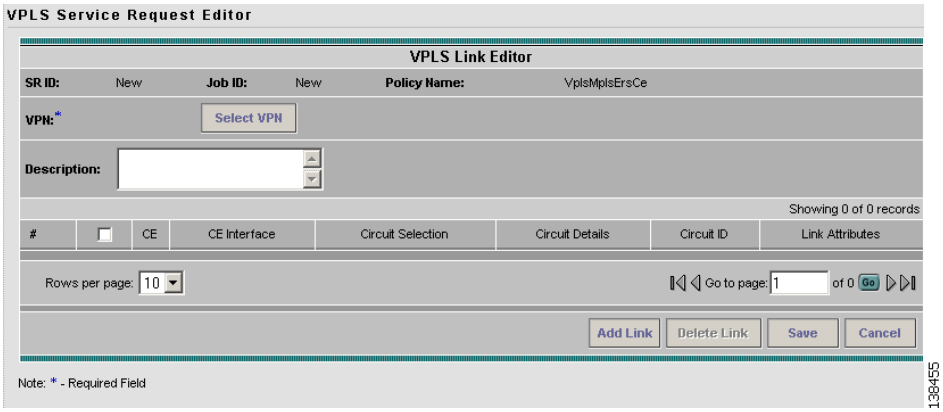
Step 5 After you make the choice, click **OK**.

As soon as you make the choice, the new service request inherits all the properties of that VPLS policy, such as all the editable and non-editable features and pre-set parameters.

Creating a VPLS Service Request with a CE

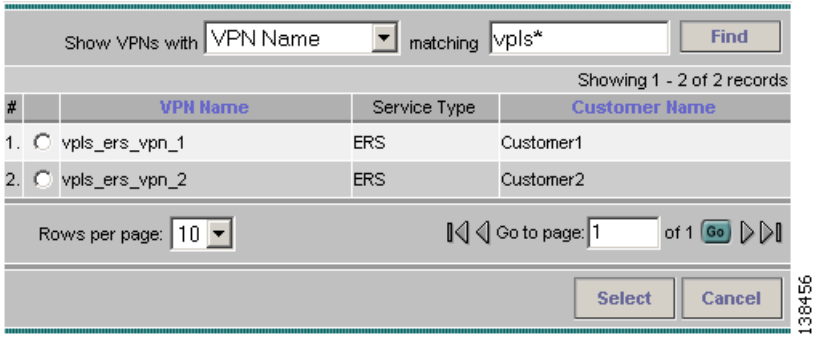
This section includes detailed steps for creating a VPLS service request with a CE present. After you choose a VPLS policy, the VPLS Service Request Editor window appears (see Figure 9-3).

Figure 9-3 VPLS Service Request Editor



Step 1 Click **Select VPN** to select a VPN for use with this CE. The Select VPN window appears with the VPNs defined in the system. Only VPNs with the same service type (ERS or EWS) as the policy you chose appear. See Figure 9-4.

Figure 9-4 Select a VPN



Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you select this check box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

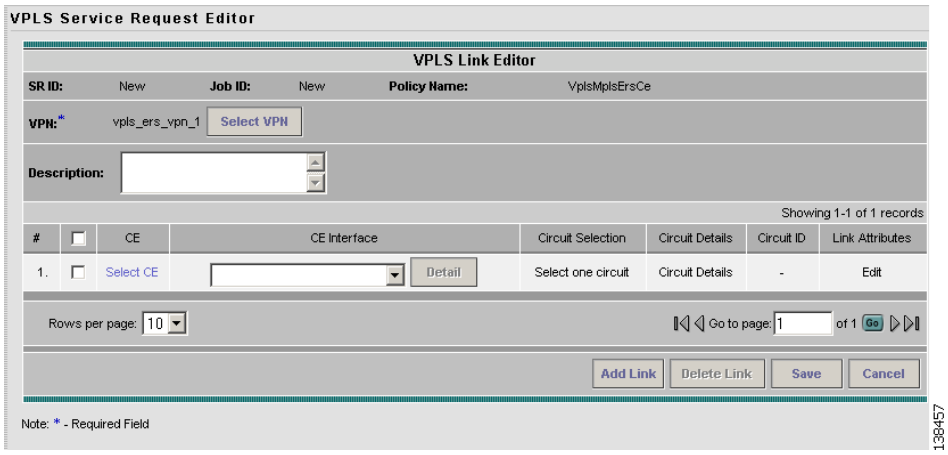
Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**. The VPLS Link Editor window appears with the VPN name displayed.

Step 4 Click **Add Link**.

You specify the CE endpoints using the VPLS Link Editor. You can add one or more links from a window like the one in Figure 9-5.

Figure 9-5 Select CE



Step 5 You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

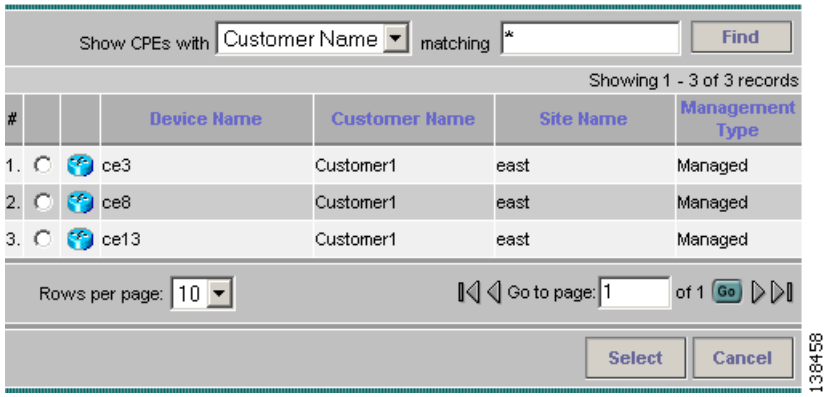
Step 6 Click **Select CE** in the CE column. The CPE for Attachment Circuit window appears (see Figure 9-6). This window displays the list of currently defined CEs.

a. From the **Show CPEs with** drop-down list, you can display CEs by Customer Name, by Site, or by Device Name.

b. You can use the **Find** button to either search for a specific CE, or to refresh the display.

c. You can set the **Rows per page** to 5, 10, 20, 30, 40, or All.

Figure 9-6 Select CPE Device



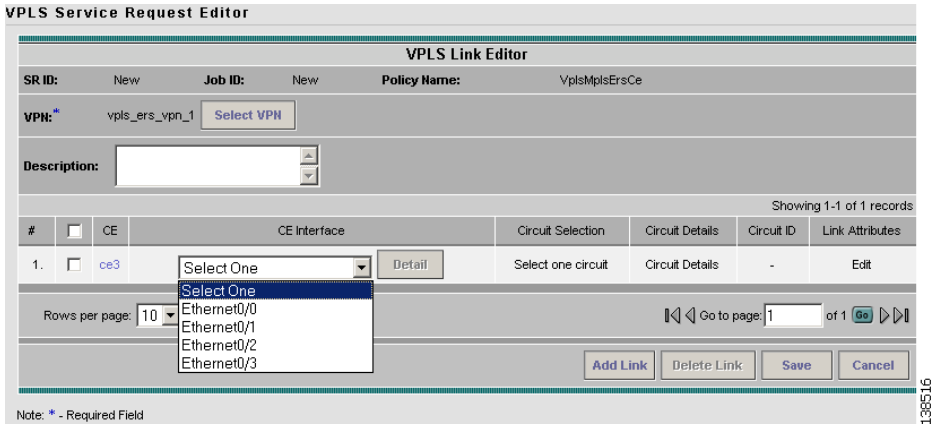
Step 7 In the Select column, choose a CE for the VPLS link.

Step 8 Click **Select**.

The VPLS Link Editor window appears displaying the name of the selected CE in the CE column.

Step 9 Select the CE interface from the drop-down list (see Figure 9-7).

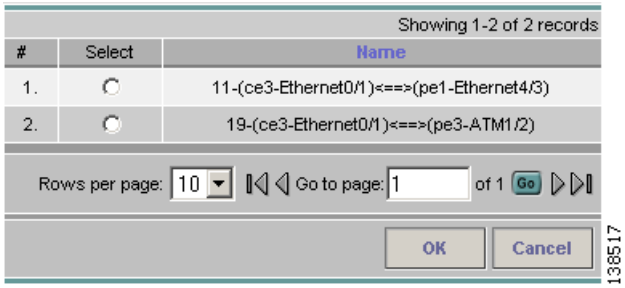
Figure 9-7 Select the CE Interface



Note When you provision an ERS service, when you select a UNI for a particular device, ISC determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

Step 10 Click **Select one circuit** in the Circuit Selection column. The NPC window appears (see Figure 9-8). If only one NPC exists for the chosen CE and CE interface, that NPC is automatically populated in the Circuit Selection column and you need not choose it explicitly.

Figure 9-8 Select NPC

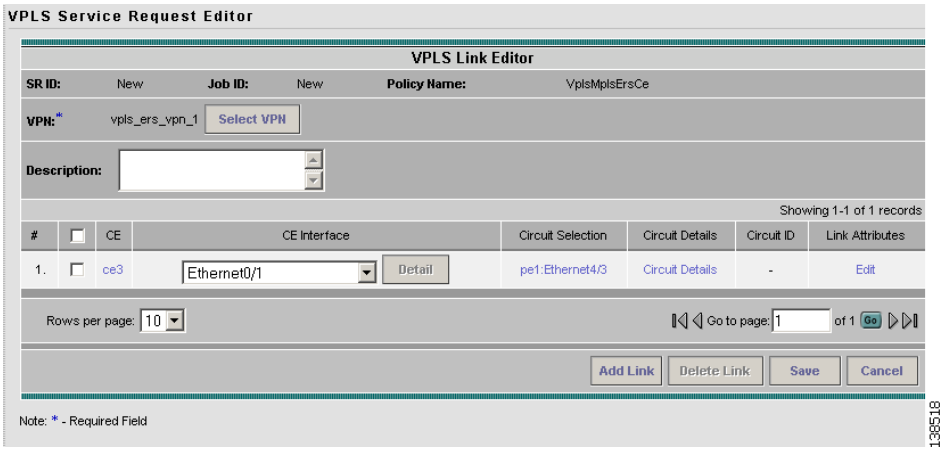


Step 11 Choose the name of the NPC from the Select column.

Step 12 Click **OK**.

Each time you choose a CE and its interface, the NPC that was precreated from this CE and interface is automatically displayed under **Circuit Selection** as in Figure 9-9. This means that you do not have to further specify the PE to complete the link.

Figure 9-9 NPC Selected



Step 13 If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC. In Figure 9-10, the CE and PE and their corresponding interfaces appear.

Figure 9-10 NPC Details

#	Source Device	Incoming Interface	Outgoing Interface	Ring
1.	ce3		Ethernet0/1	
2.	pe1	Ethernet4/3		

OK

138519

Step 14 The Circuit ID is created automatically, based on the VLAN data for the circuit.

Step 15 You can modify the values that were set by the VPLS policy, that is, the values that were marked "editable" during the VPLS policy creation.

To modify the link attributes, click **Edit** in the Link Attributes column as shown in the VPLS link editor. The Link Attributes window appears as shown in Figure 9-11

Figure 9-11 Modify CE Link Attributes

Link Attributes

Attribute	Value
CE Information	ce3
Encapsulation:	DEFAULT
UNI Information	
UNI Shutdown	☐
UNI MAC Addresses	Edit
Port Type	Access Port
Link Speed	None
Link Duplex	None
Disable CDP	☑
Filter BPDU	☑
UNI Port Security	☐
Common Attributes	
PE/UNI Interface Description:	
VLAN ID AutoPick	☑
VLAN Name	

Device Name	Role	Templates
ce3	MANAGED	Add
pe1	N_PE	Add

OK Cancel

Note: *- Required Field

138520

Step 16 Edit the link attributes.

Note If you did not select **VLANID AutoPick** in the VPLS policy, you are prompted to provide the VLAN in a **Provider VLAN ID** field as shown in Figure 9-11.

Step 17 Continue to specify additional CEs, as in previous steps, if desired.

Step 18 Click **OK**.

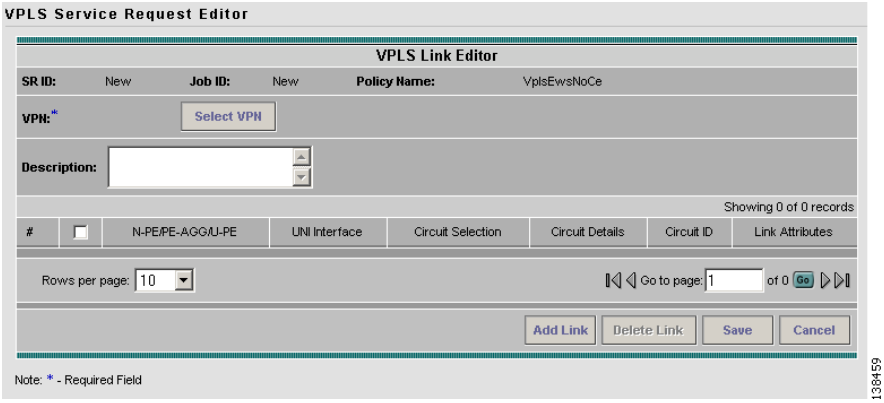
Step 19 Click **Save**.The service request is created and saved into ISC.

Creating a VPLS Service Request without a CE

This section includes detailed steps for creating a VPLS service request without a CE present.

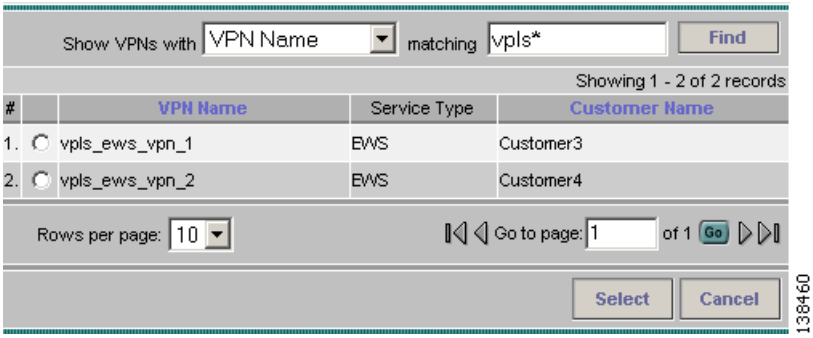
After you choose a VPLS policy, the VPLS Service Request Editor window appears (see Figure 9-12).

Figure 9-12 VPLS Service Request Editor



Step 1 Click **Select VPN** to select a VPN for use with this PE. The Select VPN window appears with the VPNs defined in the system. Only VPNs with the same service type (ERS or EWS) as the policy you chose appear. See Figure 9-13.

Figure 9-13 Select a VPN



Note The VC ID is mapped from the VPN ID. By default, ISC will "auto pick" this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you select this check box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

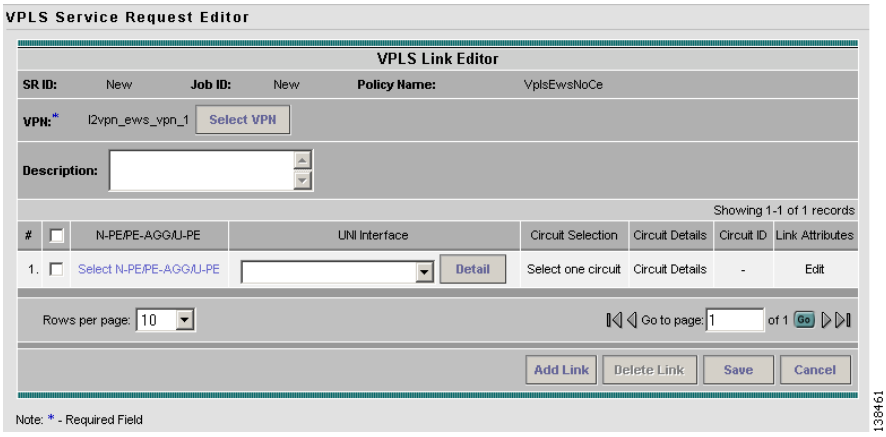
Step 2 Choose a **VPN Name** in the Select column.

Step 3 Click **Select**. The VPLS Link Editor window appears with the VPN name displayed.

Step 4 Click **Add Link**.

You specify the U-PE/PE-AGG/U-PE end points using the VPLS Link Editor. You can add one or more links from a window like the one in Figure 9-14.

Figure 9-14 Select N-PE/PE-AGG/U-PE



Step 5 You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

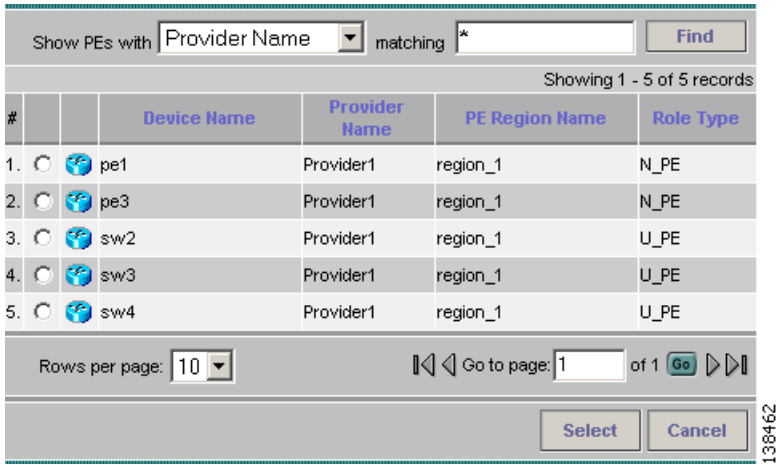
Step 6 Click **Select N-PE/PE-AGG/U-PE** in the N-PE/PE-AGG/U-PE column. The PE for Attachment Circuit window appears (see Figure 9-15). This window displays the list of currently defined PEs.

a. The **Show PEs with** drop-down list shows PEs by customer name, by site, or by device name.

b. The **Find** button allows a search for a specific PE or a refresh of the window.

c. The **Rows per page** drop-down list allows the page to be set to 5, 10, 20, 30, 40, or All.

Figure 9-15 Select PE Device



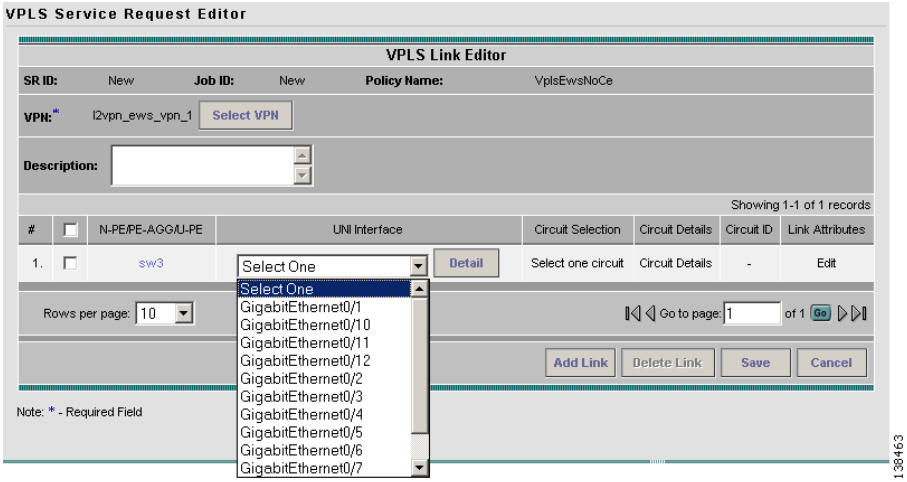
Step 7 In the **Select** column, choose the PE device name for the VPLS link.

Step 8 Click **Select**.

The VPLS Link Editor window appears displaying the name of the selected N-PE/PE-AGG/U-PE in the N-PE/PE-AGG/U-PE column

Step 9 Select the UNI interface from the drop-down list (see Figure 9-16).

Figure 9-16 Select the UNI Interface

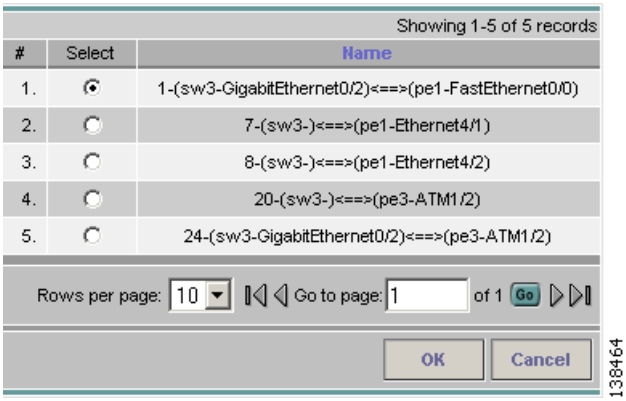


Note When you provision an ERS service, when you select a UNI for a particular device, ISC determines if there are other services using the same UNI. If so, a warning message is displayed. If you ignore the message and save the service request, all of the underlying service requests lying on the same UNI are synchronized with the modified shared attributes of the latest service request. In addition, the state of the existing service requests is changed to the Requested state.

Step 10 If the PE role type is U-PE, click **Select one circuit** in the Circuit Selection column. The NPC window appears (see Figure 9-17). If only one NPC exists for the chosen PE and PE interface, that NPC is automatically populated in the Circuit Selection column and you need not choose it explicitly.

Note If the PE role type is N-PE, the columns Circuit Selection and Circuit Details are disabled.

Figure 9-17 Select NPC

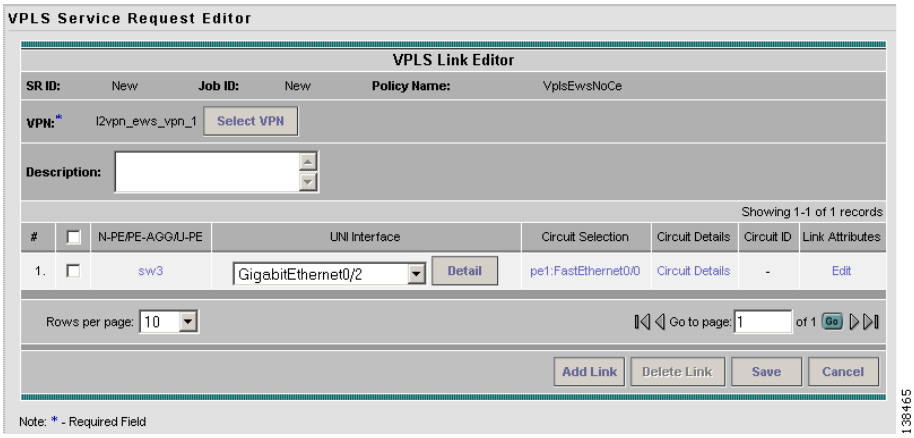


Step 11 Choose the name of the NPC from the **Select** column.

Step 12 Click **OK**.

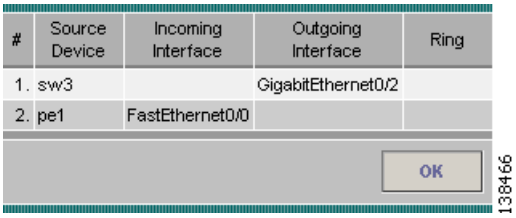
Each time you choose a PE and its interface, the NPC that was precreated from this PE and interface is automatically displayed under **Circuit Selection** as in Figure 9-18. This means that you do not have to further specify the PE to complete the link.

Figure 9-18 NPC Created



Step 13 If you want to review the details of this NPC, click **Circuit Details** in the Circuit Details column. The NPC Details window appears and lists the circuit details for this NPC. In Figure 9-19, the PE-CLE and PE and their corresponding interfaces appear.

Figure 9-19 NPC Details



#	Source Device	Incoming Interface	Outgoing Interface	Ring
1.	sw3		GigabitEthernet0/2	
2.	pe1	FastEthernet0/0		

OK

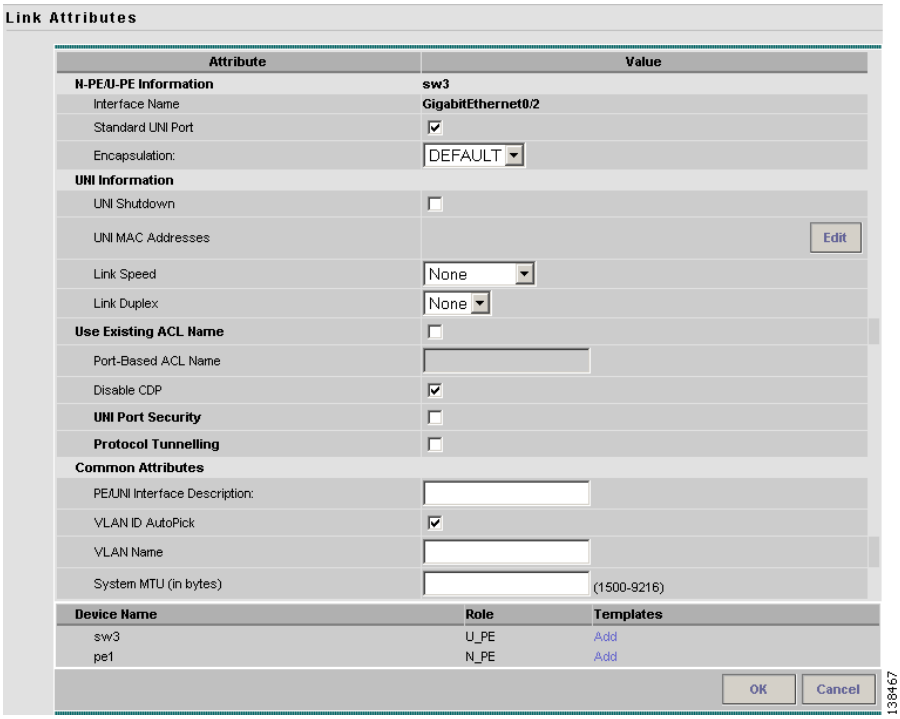
138466

Step 14 The Circuit ID is created automatically, based on the VLAN data for the circuit.

Step 15 You can modify the values that were set by the VPLS policy, that is, the values that were marked "editable" during the VPLS policy creation.

To modify the link attributes, click **Edit** in the Link Attributes column in the VPLS link editor. The Link Attributes window appears as shown in Figure 9-20

Figure 9-20 Modify PE Link Attributes



Step 16 Edit the link attributes.

Note If you did not select **VLANID AutoPick** in the VPLS policy, you are prompted to provide the VLAN in a **Provider VLAN ID** field.

Step 17 Click **OK**.

Step 18 Continue to specify additional PEs, as in previous steps, if desired.

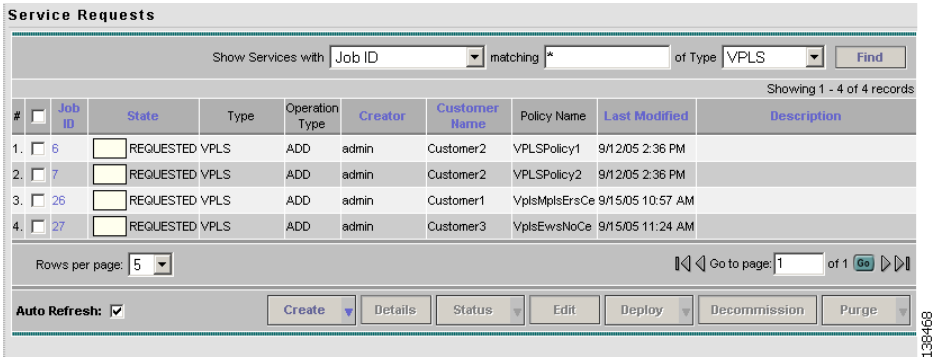
Step 19 Click **Save**. The VPLS service request is created and saved into ISC.

Modifying the VPLS Service Request

You can modify a VPLS service request if you must change the VPLS links.

Step 1 Select **Service Inventory** > **Inventory and Connection Manager** > **Service Requests**. See Figure 9-21.

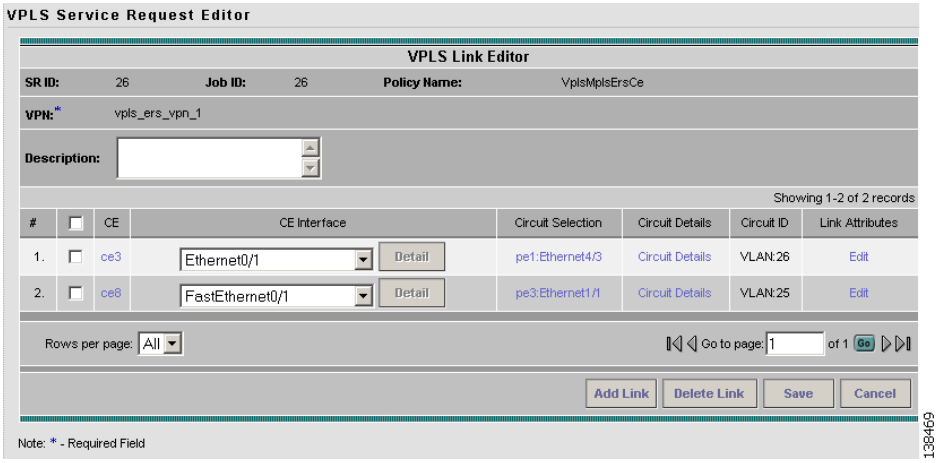
Figure 9-21 VPLS Service Activation



Step 2 Select a check box for a service request.

Step 3 Click **Edit**. The VPLS Link Editor window appears as shown in Figure 9-22.

Figure 9-22 VPLS Link Editor



You can choose any of the blue highlighted values to edit the VPLS links.

You can also click **Add Link** to add a VPLS link.

You can click **Delete Link** to delete a VPLS link.

You can enter a description for the service request in the first **Description** field. The description will show up in this window and also in the Description column of the Service Requests window. The maximum length for this field is 256 characters.

The Circuit ID is created automatically, based on the VLAN data for the circuit.

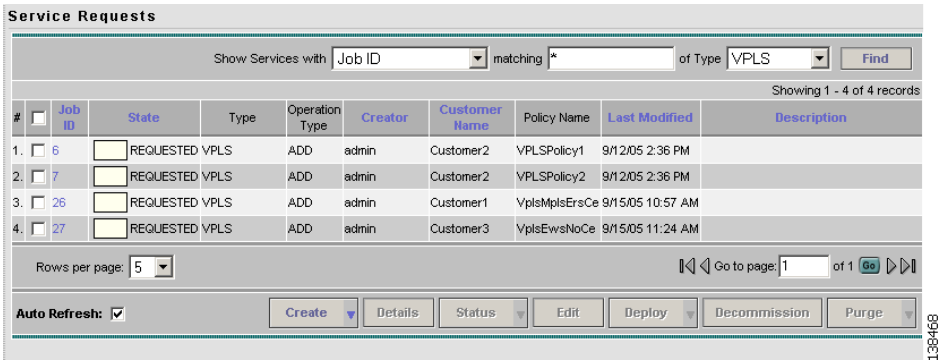
Step 4 When you are finished editing the VPLS links, click **Save**.

Saving the VPLS Service Request

When you are finished with Link Attributes for all the Attachment Circuits, click **Save** to finish the VPLS service request creation as shown in Figure 9-23.

If the VPLS service request is successfully created, you will see the service request list window where the newly created VPLS service request is added with the state of REQUESTED as shown in Figure 9-23. If, however, the VPLS service request creation failed for some reason (for example, the value chosen is out of bounds), you are warned with an error message. Go back to correct the error and click **Save** again.

Figure 9-23 VPLS Service Request Created



The VPLS service request is in Requested state. See Deploying Service Requests, page 12-1 for information on deploying VPLS service requests.

Using Autodiscovery for L2 Services

All discovery steps are integrated in a discovery workflow, controlled from the ISC GUI. This is accessed in ISC through **Service Inventory > Discovery**. The following discovery features are supported:

- File-based device discovery is supported.
- Rules-based device role assignment is supported.
- Discovery progress messages and logs are viewable in the GUI to keep track of various discovery stages.
- Bulk creation of Provider, Customer, Site, and Region objects is available through an XML data file.

For detailed steps on using the autodiscovery feature in ISC, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Generating L2 and VPLS Reports

This chapter provides information on generating L2 and VPLS reports. It contains the following sections:

Overview

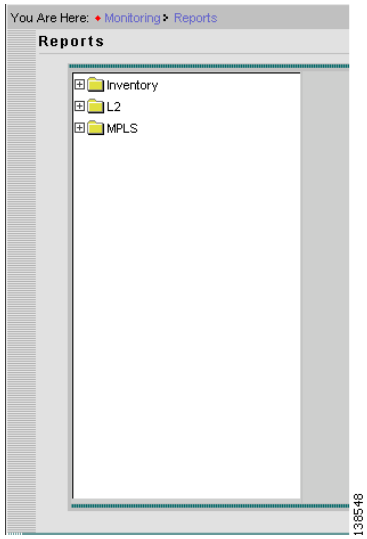
The ISC reporting GUI is used across multiple ISC modules, including L2 and VPLS. For a general coverage of using the reports GUI, running reports, using the output from reports, and creating customized reports, see "Monitoring" chapter in the *Cisco IP Solution Center Infrastructure Reference, 4.1*. The rest of this chapter provides information about the L2 and VPLS reports available in ISC.

Accessing L2 and VPLS Reports

Perform the following steps to access the L2 and VPLS reports.

Step 1 To access the reports framework in the ISC GUI, select **Monitoring > Reports**. The Reports window, appears, as shown in Figure 11-1.

Figure 11-1 Reports Window



Step 2 Click the L2 folder to display the available L2 and VPLS reports.

Step 3 Click the icon of a report to bring up the window associated with that report.

Details on each of the reports are provided in L2 and VPLS Reports, page 11-2.

L2 and VPLS Reports

This section provides details on the following L2 and VPLS reports:

- L2 EndtoEndWire Report, page 11-3
- L2 PE Service Report, page 11-6
- L2 VPN Report, page 11-6
- VPLS Attachment Circuit Report, page 11-7
- VPLS PE Service Report, page 11-9
- VPLS VPN Report, page 11-10

The following information is provided for each report:

- Description or purpose of the report.
- An illustration of the report window.
- List of filter values and descriptions.
- List of output values and descriptions.

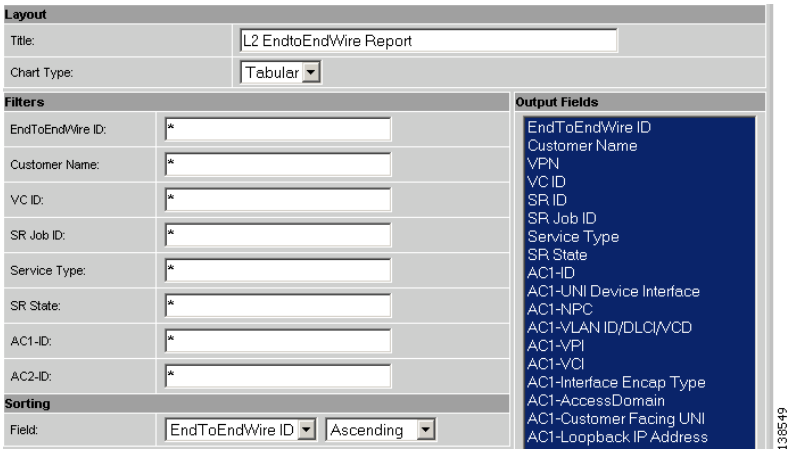
Note Several sample reports are provided in the L2 reports folder. These reports begin with the title **SAMPLE-**. These reports are provided for informational purposes only. They are untested and unsupported. You might want to use them as a basis for creating your own custom reports. See "Creating Custom L2 and VPLS Reports" section on page 11-11 for information on custom reports.

L2 EndtoEndWire Report

An L2 end-to-end wire is a point-to-point connection containing two attachment circuits. The L2 EndtoEndWire report displays the services that are running on L2 end-to-end connections. You can use this report to view all the services and respective attachment circuit attributes for each connection.

Click the L2 EndtoEndWire Report icon to bring up the window for this report, as shown in Figure 11-2.

Figure 11-2 L2 EndtoEndWire Report



Filter Values:

- **EndToEndWire ID**—End-to-end wire identification number.
- **Customer Name**—Name of the customer.
- **VC ID**—Virtual circuit identification number.
- **SR Job ID**—Service request job identification number.
- **Service Type**—Type of service. Values can be:
  - **ATM**
  - **ATM_NO_CE**
  - **FRAME_RELAY**
  - **FRAME_RELAY_NO_CE**
  - **L2VPN_ERS**
  - **L2VPN_ERS_NO_CE**
  - **L2VPN_EWS**
  - **L2VPN_EWS_NO_CE**
- **SR State**—Service request state. Values can be:
  - **BROKEN**
  - **CLOSED**
  - **DEPLOYED**
  - **FAILED_AUDIT**
  - **FAILED_DEPLOY**

  - **FUNCTIONAL**
  - **INVALID**
  - **LOST**
  - **PENDING**
  - **REQUESTED**
  - **WAIT_DEPLOY**
- **AC1-ID**—First attachment circuit (AC1) identification number.
- **AC2-ID**—Second attachment circuit (AC2) identification number.

Output Values:

- **EndToEndWire ID**—End-to-end wire identification number.
- **Customer Name**—Name of the customer.
- **VPN**—Name of the VPN.
- **VC ID**—Virtual circuit identification number.
- **SR ID**—Service request identification number.
- **SR Job ID**—Service request job identification number.
- **Service Type**—Type of service.
- **SR State**—Service request state.
- **AC1-ID**—Identification number of the first attachment circuit (AC1).
- **AC1-UNI Device Interface**—UNI device interface of the first attachment circuit (AC1).
- **AC1-NPC**—Named physical circuit for the first attachment circuit (AC1).
- **AC2-VLAN ID/DLCI/VCD**—VLAN identification number, DLCI (data-link connection identifier) or VCD (virtual circuit descriptor) of the first attachment circuit (AC1).
- **AC1-VPI**—Virtual path identifier for the first attachment circuit (AC1).
- **AC1-VCI**—Virtual channel identifier for the first attachment circuit (AC1).
- **AC1-Interface Encap Type**—Encapsulation type used for the first attachment circuit (AC1).
- **AC1-AccessDomain**—Access domain name for the first attachment circuit (AC1).
- **AC1-Customer Facing UNI**—Customer-facing UNI port of the first attachment circuit (AC1).
- **AC1-Loopback IP Address**—Loop back address for the first attachment circuit (AC1).
- **AC1-STP Shutdown Threshold**—Spanning Tree Protocol shutdown threshold (in packets/second) for the first attachment circuit (AC1).
- **AC1-VTP Shutdown Threshold**—VLAN Trunk Protocol shutdown threshold (in packets/second) for the first attachment circuit (AC1).
- **AC1-CDP Shutdown Threshold**—Cisco Discovery Protocol shutdown threshold (in packets/second) for the first attachment circuit (AC1).
- **AC1-STP Drop Threshold**—Spanning Tree Protocol drop threshold (in packets/second) for the first attachment circuit (AC1).
- **AC1-CDP Drop Threshold**—Cisco Discovery Protocol drop threshold (in packets/second) for the first attachment circuit (AC1).
- **AC1-VTP Drop Threshold**—VLAN Trunk Protocol drop threshold (in packets/second) for the first attachment circuit (AC1).

- **AC1-UNI Recovery Interval**—Recovery interval (in seconds) of the UNI port for the first attachment circuit (AC1).
- **AC1-UNI Speed**—UNI port speed for the first attachment circuit (AC1).
- **AC1-UNI Shutdown**—Shutdown status of the UNI port for the first attachment circuit (AC1).
- **AC1-UNI PortSecurity**—Status of UNI port security for the first attachment circuit (AC1).
- **AC1-UNI Duplex**—Duplex status (none, full, half, or auto) of the UNI port for the first attachment circuit (AC1).
- **AC1-Maximum MAC Address**—Maximum MAC addresses allowed on the UNI port for the first attachment circuit (AC1).
- **AC1-UNI Aging**—Length of time, in seconds, that MAC addresses can stay in the UNI port security table for the first attachment circuit (AC1).
- **AC2-ID**—Second attachment circuit (AC2) identification number.
- **AC2-UNI Device Interface**—UNI device interface of the second attachment circuit (AC2).
- **AC2-NPC**—Named physical circuit for the second attachment circuit (AC2).
- **AC2-VLAN ID/DLCI/VCD**—The VLAN ID, DLCI or VCD of the second attachment circuit (AC2).
- **AC2-VPI**—Virtual path identifier for the first attachment circuit (AC2).
- **AC2-VCI**—Virtual channel identifier for the first attachment circuit (AC2).
- **AC2-Interface Encap Type**—Encapsulation type used for the second attachment circuit (AC2).
- **AC2-AccessDomain**—Access domain name for the second attachment circuit (AC2).
- **AC2-Customer Facing UNI**—Customer-facing UNI port of the second attachment circuit (AC2).
- **AC2-Loopback IP Address**—Loop back address for the second attachment circuit (AC2).
- **AC2-STP Shutdown Threshold**—Spanning Tree Protocol shutdown threshold for the second attachment circuit (AC2).
- **AC2-VTP Shutdown Threshold**—VLAN Trunk Protocol shutdown threshold for the second attachment circuit (AC2).
- **AC2-CDP Shutdown Threshold**—Cisco Discovery Protocol shutdown threshold for the second attachment circuit (AC2).
- **AC2-STP Drop Threshold**—Spanning Tree Protocol drop threshold for the second attachment circuit (AC2).
- **AC2-CDP Drop Threshold**—Cisco Discovery Protocol drop threshold for the second attachment circuit.
- **AC2-VTP Drop Threshold**—VLAN Trunk Protocol drop threshold for the second attachment circuit (AC2).
- **AC2-UNI Recovery Interval**—Recovery interval of the UNI port for the second attachment circuit (AC2).
- **AC2-UNI Speed**—UNI port speed for the second attachment circuit (AC2).
- **AC2-UNI Shutdown**—Shutdown status of the UNI port for the second attachment circuit (AC2).
- **AC2-UNI PortSecurity**—Status of UNI port security for the second attachment circuit (AC2).
- **AC2-UNI Duplex**—Duplex status (none, full, half, or auto) of the UNI port for the second attachment circuit (AC2).

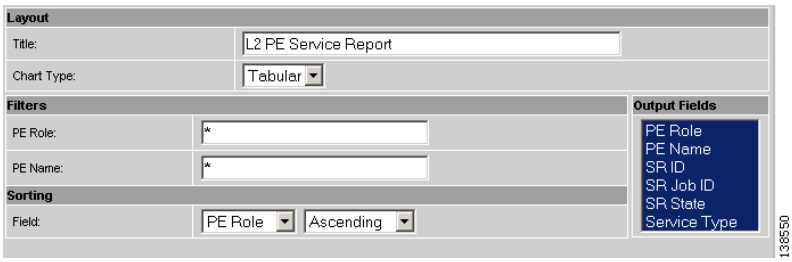
- **AC2-Maximum MAC Address**—Maximum MAC addresses allowed on the UNI port for the second attachment circuit (AC2).
- **AC2-UNI Aging**—Length of time, in seconds, that MAC addresses can stay in the UNI port security table for the second attachment circuit (AC2).

L2 PE Service Report

The L2 PE Service report allows you to select PEs and display their roles (for example, N-PE, U-PE or PE-AGG) and L2-related services that are running on them.

Click the L2 PE Service Report icon to bring up the window for this report, as shown in Figure 11-3.

Figure 11-3 L2 PE Service Report



Filter Values:

- **PE Role**—PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name**—PE device name.

Output Values:

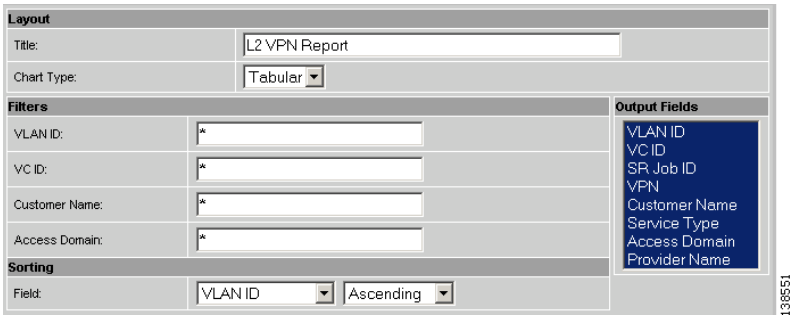
- **PE Role**—PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name**—PE device name.
- **SR ID**—Service request identification number.
- **SR Job ID**—Service request job identification number.
- **SR State**—Service request state.
- **Service Type**—Type of service.

L2 VPN Report

The L2 VPN Report provides a way to track a VLAN ID and/or VC ID back to the VPN and customer without having to iterate through every link and every VPN service. Given a VLAN ID or VC ID, the respective customer and VPN details are displayed in the report.

Click the L2 VPN Report icon to bring up the window for this report, as shown in Figure 11-4.

Figure 11-4 L2 VPN Report



Filter Values:

- **VLAN ID**—VLAN identification number.
- **VC ID**—Virtual circuit identification number.
- **Customer Name**—Name of the customer.
- **Access Domain**—Access domain name.

Output Values:

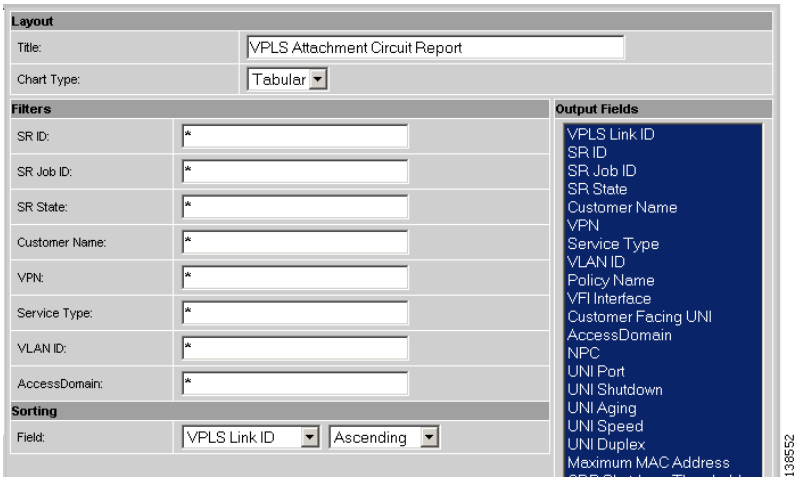
- **VLAN ID**—VLAN identification number.
- **VC ID**—Virtual circuit identification number.
- **SR Job ID**—Service request job identification number
- **VPN**—Name of the VPN.
- **Customer Name**—Name of the customer.
- **Service Type**—Type of service.
- **Access Domain**—Access domain name.
- **Provider Name**—Name of the provider.

VPLS Attachment Circuit Report

The VPLS Attachment circuit report displays details of attachment circuits for a given customer VPN.

Click the VPLS Attachment Circuit Report icon to bring up the window for this report, as shown in Figure 11-5.

Figure 11-5 VPLS Attachment Circuit Report



Filter Values:

- **SR ID**—Service request identification number.
- **SR Job ID**—Service request job identification number.
- **SR State**—Service request state. Values can be:
  - **BROKEN**
  - **CLOSED**
  - **DEPLOYED**
  - **FAILED_AUDIT**
  - **FAILED_DEPLOY**
  - **FUNCTIONAL**
  - **INVALID**
  - **LOST**
  - **PENDING**
  - **REQUESTED**
  - **WAIT_DEPLOY**
- **Customer Name**—Name of the customer.
- **VPN**—Name of the VPN.
- **Service Type**—Type of service. Values can be:
  - **VPLS_ERS**
  - **VPLS_ERS_NO_CE**
  - **VPLS_EWS**
  - **VPLS_EWS_NO_CE**
- **VLAN ID**—VLAN identification number.
- **AccessDomain**—Access domain name.

Output Values:

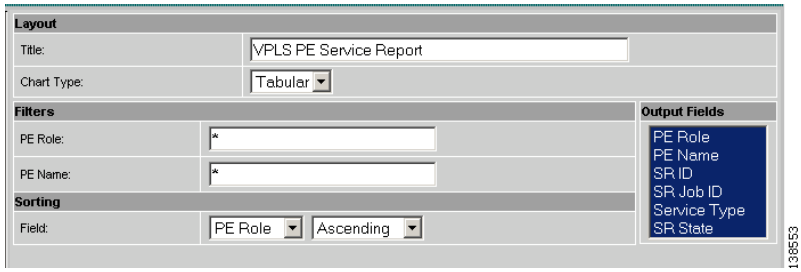
- **VPLS Link ID**—VPLS link identification number.
- **SR ID**—Service request identification number
- **SR Job ID**—Service request job identification number.
- **SR State**—Service request state.
- **Customer Name**—Name of the customer.
- **VPN**—Name of the VPN.
- **Service Type**—Type of service.
- **VLAN ID**—VLAN identification number.
- **Policy Name**—Name of the VPLS policy.
- **VFI Interface**—Virtual forwarding interface name.
- **Customer Facing UNI**—Customer-facing UNI port.
- **AccessDomain**—Access domain name.
- **NPC**—Named physical circuit.
- **UNI Port**—UNI port.
- **UNI Shutdown**—Shutdown status of the UNI port.
- **UNI Aging**—Length of time, in seconds, that MAC addresses can stay in the UNI port security table.
- **UNI Speed**—UNI port speed.
- **UNI Duplex**—Duplex status (none, full, half, or auto) of the UNI port.
- **Maximum MAC Address**—Maximum MAC addresses allowed on the UNI port.
- **CDP Shutdown Threshold**—Cisco Discovery Protocol shutdown threshold (in packets/second) on the UNI port.
- **STP Shutdown Threshold**—Spanning Tree Protocol shutdown threshold (in packets/second) on the UNI port.
- **VTP Shutdown Threshold**—VLAN Trunk Protocol shutdown threshold (in packets/second) on the UNI port.
- **CDP Drop Threshold**—Cisco Discovery Protocol drop threshold (in packets/second) on the UNI port.
- **VTP Drop Threshold**—VLAN Trunk Protocol drop threshold (in packets/second) on the UNI port.
- **STP Drop Threshold**—Spanning Tree Protocol drop threshold (in packets/second) on the UNI port.
- **Recovery Interval**—Recovery interval (in seconds) of the UNI port.

VPLS PE Service Report

The VPLS PE Service report allows you to select PEs and display their roles (for example, N-PE, U-PE or PE-AGG) and the VPLS services that are running on them.

Click the VPLS PE Service Report icon to bring up the window for this report, as shown in Figure 11-6.

Figure 11-6 VPLS PE Service Report



Filter Values:

- **PE Role**—PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name**—PE device name.

Output Values:

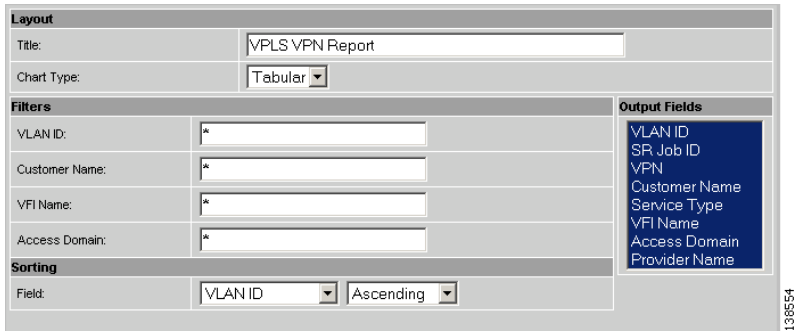
- **PE Role**—PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name**—PE device name.
- **SR ID**—Service request identification number
- **SR Job ID**—Service request job identification number.
- **Service Type**—Type of service.
- **SR State**—Service request state.

VPLS VPN Report

The VPLS VPN report provides a way to track a VLAN ID and/or VFI Name back to the VPN and customer without having to iterate through every link and every VPN service. Given a VLAN ID or VFI name, the respective customer and VPN details are displayed in the report.

Click the VPLS VPN Report icon to bring up the window for this report, as shown in Figure 11-7.

Figure 11-7 VPLS VPN Report



Filter Values:

- **VLAN ID**—VLAN identification number.
- **Customer Name**—Name of the customer.

- **VFI Name**—Virtual forwarding interface name.
- **Access Domain**—Access domain name.

Output Values:

- **VLAN ID**—VLAN identification number.
- **SR Job ID**—Service request job identification number.
- **VPN**—Name of the VPN.
- **Customer Name**—Name of the customer.
- **Service Type**—Type of service.
- **VFI Name**—Virtual forwarding interface name.
- **Access Domain**—Access domain name.
- **Provider Name**—Name of the provider.

Creating Custom L2 and VPLS Reports

The reports listed in the ISC GUI in the L2 folder are derived from an underlying configuration file. The file is in XML format. You can access the file in the following location:

$ISC_HOME/**resources/nbi/reports/ISC/l2_report.xml**

See the "Monitoring" chapter in *Cisco IP Solution Center Infrastructure Reference, 4.1* for details on how to modify report configuration files to create custom reports.

Deploying, Monitoring and Auditing Service Requests

This chapter describes how to deploy, monitor and audit L2VPN, L2TPv3 or VPLS service requests, and how to access task logs. It contains the following sections:

Deploying Service Requests

To apply L2VPN or VPLS policies to network devices, you must deploy the service request. When you deploy a service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates a configlet.

Pre-Deployment Changes

You can change the Dynamic Component Properties Library (DCPL) parameter **actionTakenOnUNIVlanList** before you deploy an L2VPN or VPLS service request. This will be necessary if the **trunk allowed vlan** list is not present on the User Network Interface (UNI). To make this change, perform the following steps.

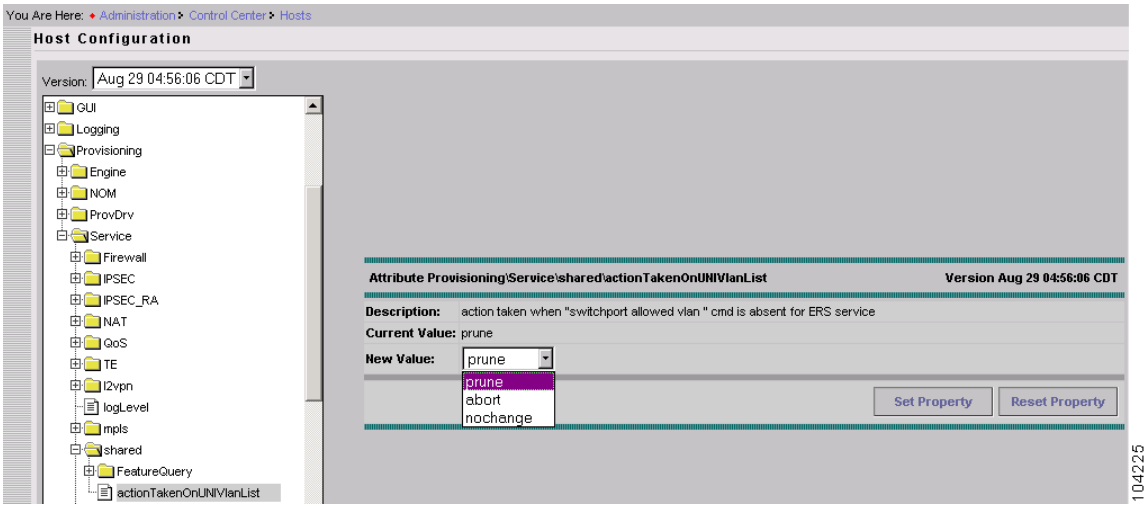
Step 1 Select **Administration > Control Center**.

Step 2 Choose the host that you want to change.

Step 3 Click **Config**.

Step 4 Select **Provisioning > Service > shared > actionTakenOnUNIVlanList**. The window shown in Figure 12-1 appears.

Figure 12-1 Change DCPL Parameter



Step 5 Choose one of the following:

- **prune** to have ISC create the minimum VLAN list. This is the default.
- **abort** to have ISC stop the L2VPN or VPLS service request provisioning with the error message: **trunk allowed vlan list is absent on ERS UNI**.
- **nochange** to have ISC allow all VLANs.

Step 6 Click **Set Property**.

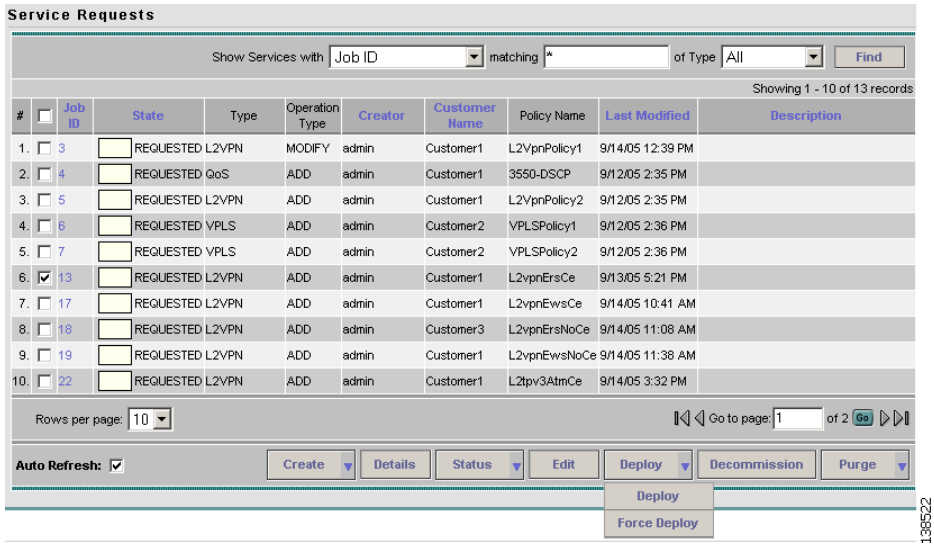
Service Deployment

After you create an L2VPN, L2TPv3, or VPLS service request and save it in the ISC repository, you can deploy or force-deploy it.

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

The Service Requests window appears as shown in Figure 12-2.

Figure 12-2 Deploy a VPLS Service Request



Step 2 Choose a service request.

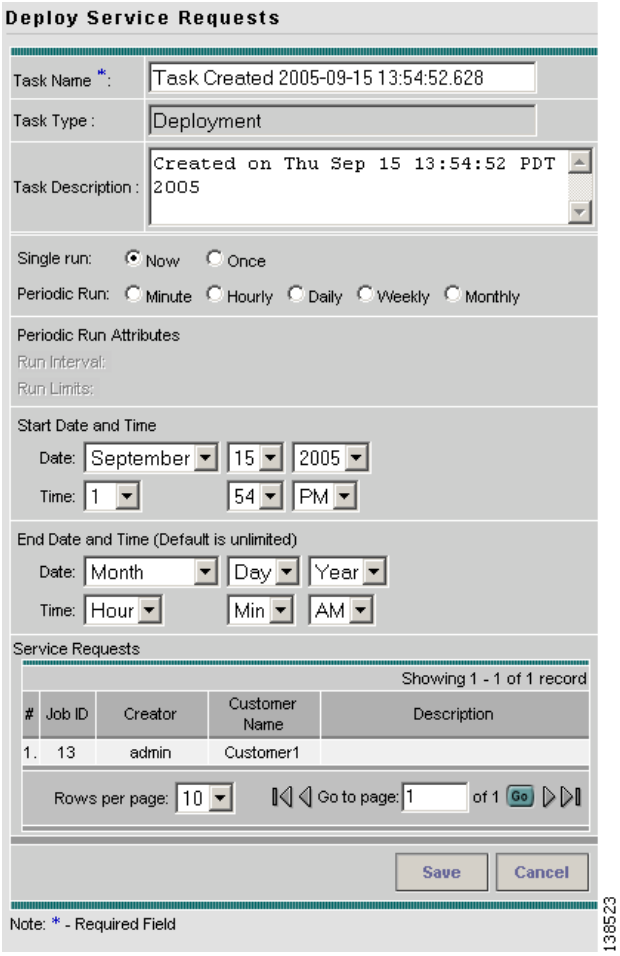
Step 3 Click **Deploy** and choose **Deploy** or **Force-Deploy**.

Use **Deploy** when the service request state is Requested or Invalid.

Use **Force Deploy** when the service request state is Deployed, Failed Deployed, or Failed Audit.

The Deploy Service Requests window appears as shown in Figure 12-3.

Figure 12-3 Schedule Service Activation



Step 4 Choose a schedule for the activation of the service.

Step 5 After you schedule the service request, click **Save**.

After you schedule the VPLS service request, you can monitor the service request that is being deployed. See Verifying L2VPN or VPLS Service Requests, page 12-4 and Monitoring Service Requests, page 12-11 for more information.

Verifying L2VPN or VPLS Service Requests

After you deploy an L2VPN or VPLS service request, you should verify that there were no errors.

You can verify an L2VPN or VPLS service request through the following:

- Transition state—The transition state of an L2VPN or VPLS service request is listed on the Service Requests window in the State column. See Service Request States, page 12-5 for more information.

- View service request details—From the Service Requests Details window, you can view the L2VPN or VPLS link endpoints and the L2VPN or VPLS configlets for this service request. See Viewing L2VPN or VPLS Service Request Details, page 12-7 for more information.
- Task Logs—Access the task logs from the Monitoring tab to help you troubleshoot a failed service request or to view more details about a service request. See Monitoring Service Requests, page 12-11 for more information.

Service Request States

A service request transition state describes the different stages a service request enters during the L2VPN or VPLS provisioning process.

For example, when you deploy an L2VPN or VPLS service request, ISC compares the device information in the Repository (the ISC database) with the current device configuration and generates an L2VPN or VPLS configlet. When the configlet is generated and downloaded to the device, the L2VPN or VPLS service request enters the **Pending** state. When the device is audited, the L2VPN or VPLS service request enters the **Deployed** state.

Figure 12-4 illustrates which service request states relate to the L2VPN or VPLS configuration auditing process, and which states relate to the provisioning process.

Figure 12-4 Service Requests States

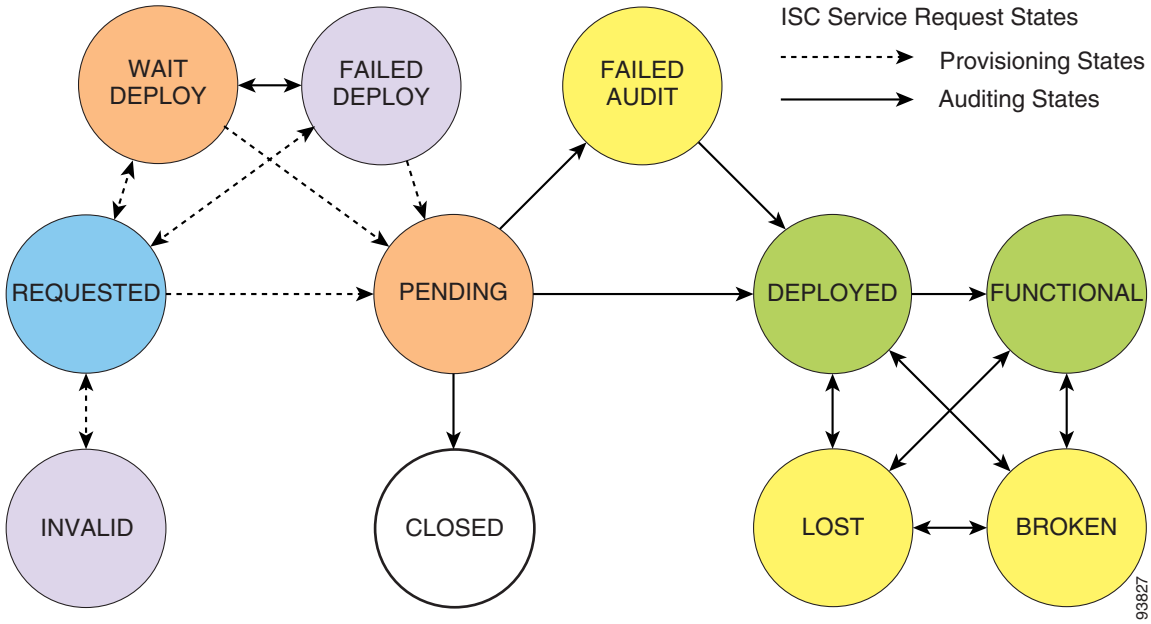


Table 12-1 describes the functions of each ISC service request state. They are listed in alphabetic order.

Table 12-1 Cisco IP Solution Center Service Request States

Service Request Type	Description
Broken (valid only for L2TPv3 and MPLS services)	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to **Broken** if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
Closed	A service request moves to **Closed** if the service request should no longer be used during the provisioning or auditing process. A service request moves to the **Closed** state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to **Deployed** if the intention of the service request is found in the router configuration file. **Deployed** indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the **Deployed** state. The **Failed Audit** state is initiated from the **Pending** state. After a service request is deployed successfully, it cannot re-enter the **Failed Audit** state (except if the service request is redeployed).
Failed Deploy	The cause for a **Failed Deploy** status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional (valid only for L2TPv3 and MPLS services)	An MPLS service request moves to **Functional** when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful.
Invalid	**Invalid** indicates that the service request information is incorrect in some way. A service request moves to **Invalid** if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to **Lost** when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the **Deployed** state, but now some or all router configuration information is missing. A service request can move to the **Lost** state *only* when the service request had been **Deployed**.

Table 12-1 Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Pending	A service request moves to **Pending** when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. **Pending** indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains **Requested**, the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. **Wait Deploy** indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the **Wait Deploy** state are then downloaded to the Cisco CNS-CE server.

Viewing L2VPN or VPLS Service Request Details

The L2VPN or VPLS service request details include the link endpoints for the service request, the history, and the configlet generated during the service request deployment operation. Use the service request details to help you troubleshoot a problem or error with the service request or to check the L2VPN or VPLS commands in the configlet.

From the Service Request Details page, you can view more information about:

- Links—the link endpoint details
- History—Service request history report
- Audit—Audit reports for the link IDs
- Configlets—View the ISC generated configlet for the L2VPN or VPLS service request

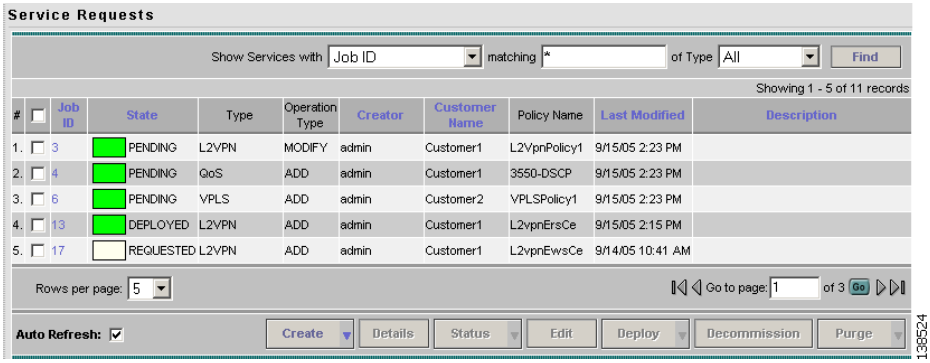
The following sections describe the links, history, and configlet details for an L2VPN or VPLS service request. The audit details are described in Auditing Service Requests, page 12-13.

To view L2VPN or VPLS service request details:

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

The Service Requests window appears as shown in Figure 12-5.

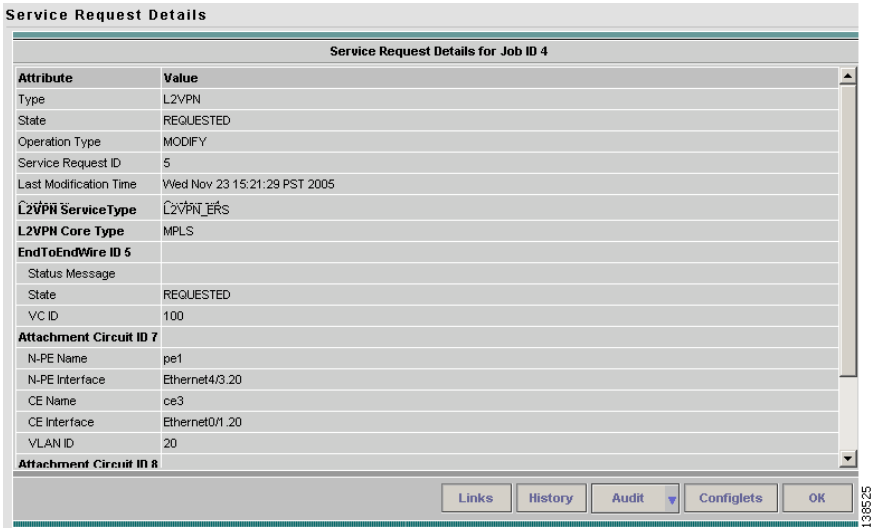
Figure 12-5 Service Requests Window



Step 2 Select the L2VPN, L2TPv3, or VPLS service request and click **Details**.

Step 3 The Service Request Details window appears (Figure 12-6).

Figure 12-6 Example Service Request Details Window



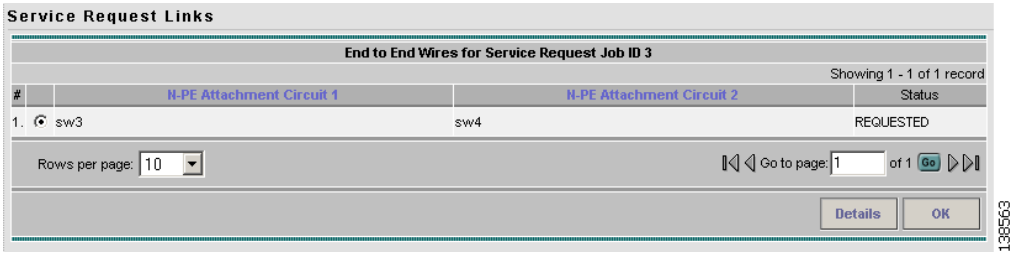
The service request attribute details include the type, transition state, operation type, ID, modification history, customer, and policy name.

Links

The service request link details include the link endpoints, PE secured interface, VLAN ID, and whether a CE is present.

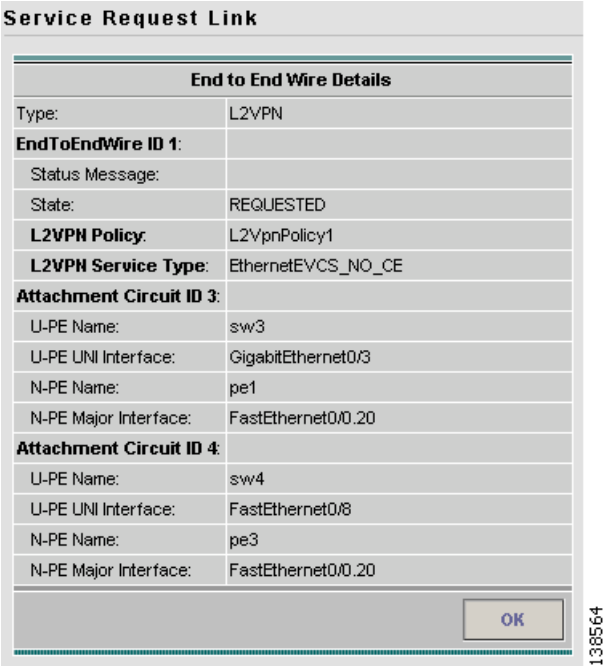
Step 1 Click **Links** on the Service Request Details window (see Figure 12-6). The Service Request Links window appears (Figure 12-7).

Figure 12-7 Service Request Links



Step 2 Choose a link and click **Details**. The Link Details window appears as shown in Figure 12-8.

Figure 12-8 Link Details Window



Step 3 Click **OK** to return to the Service Request Links window.

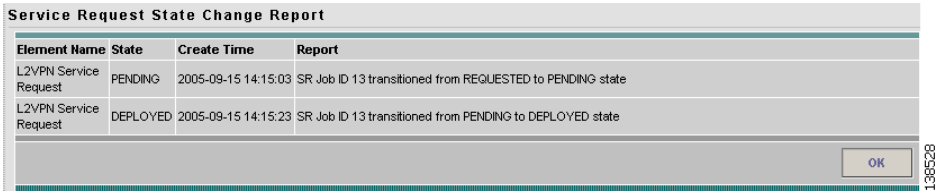
Step 4 Select another link to view or click **OK** to return to the Service Request Details window.

History

You can view history information about the service request.

Step 1 Click **History** on the Service Request Details window (see Figure 12-6). The Service Request State Change Report window appears (Figure 12-9).

Figure 12-9 Service Request State Change Report



The history reports lists the following information about the service request:

- Element Name—the device, interface, and subinterfaces participating in this service request
- State—the transition states the element has gone through
- Create Time—the time the element was created for this service request
- Report—the action taken by ISC for the element in this service request

Step 2 Click **OK** to return to the Service Request Details window.

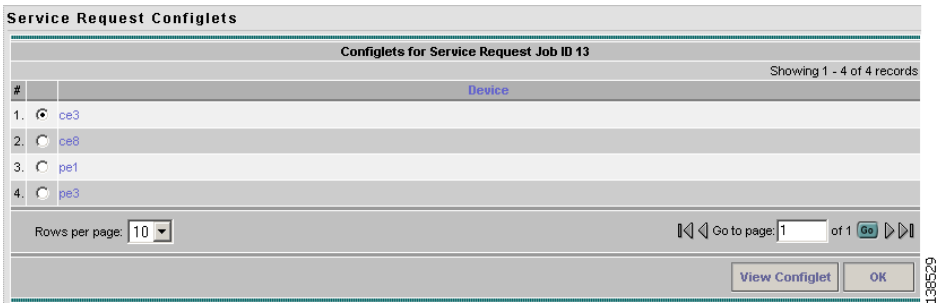
Configlets

After you deploy the service request, ISC generates Cisco IOS commands to turn on L2VPN or VPLS Services on all the network devices that participate in the service request.

To view the configlets that are generated, perform the following tasks.

Step 1 Click **Configlets** on the Service Request Details window (see Figure 12-6). You see a list of network devices for which a configlet was generated (see Figure 12-10).

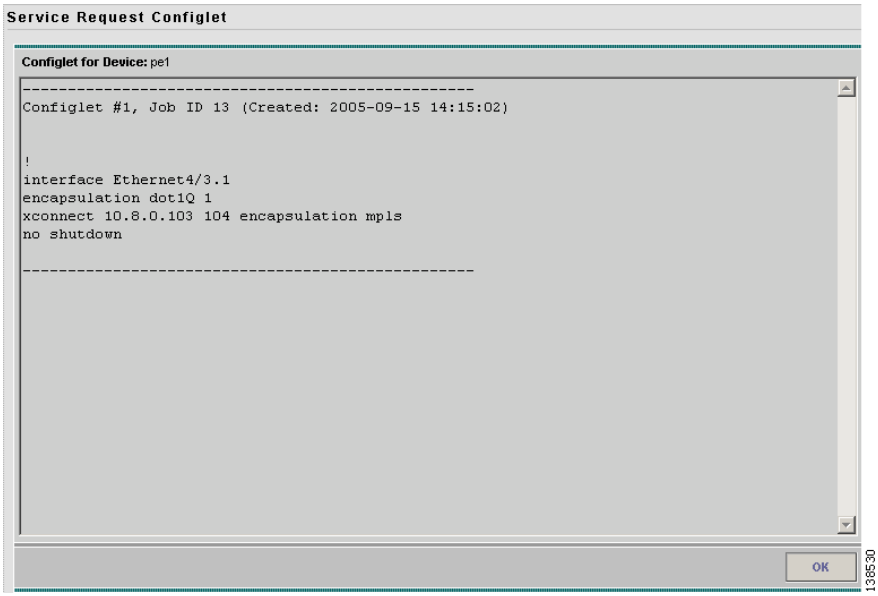
Figure 12-10 Service Request Configlets



Step 2 Select the device for which you want to view the configlet.

Step 3 Click **View Configlet**. The Configlet for Device window appears (Figure 12-11).

Figure 12-11 L2VPN, L2TPv3, or VPLS Configlet Example



The device configlet shows all commands downloaded to the device configuration during the service request deployment operation.

Step 4 Click **OK** to exit.

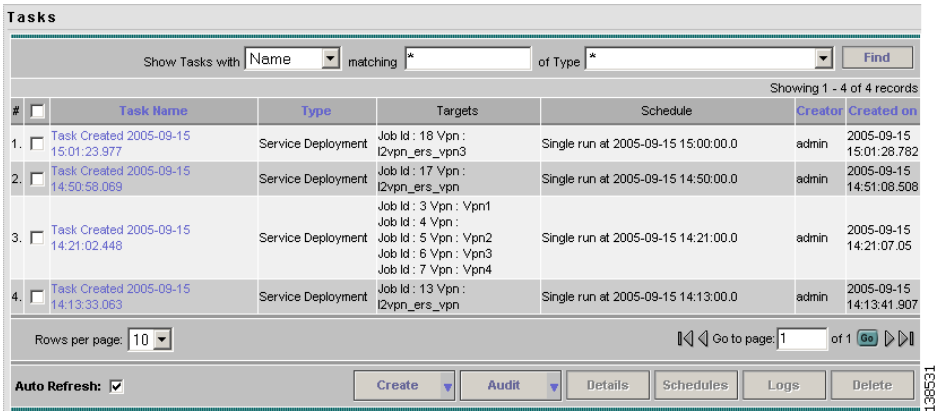
Monitoring Service Requests

To monitor an L2VPN or VPLS service request that is being deployed, you must use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request.

Perform the following steps to monitor a service request.

Step 1 Select **Monitoring > Task Manager**. The Tasks window appears as shown in Figure 12-12.

Figure 12-12 Tasks Window

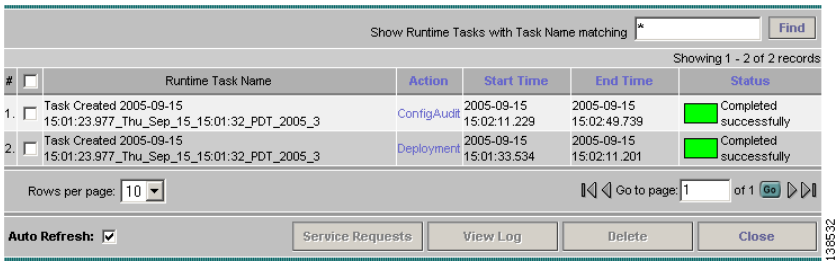


Step 2 Click **Find** to refresh the window.

The task that is executing will be the first in the list of tasks that being performed in ISC.

Step 3 Select the task you want to monitor and click **Logs**. The Task Logs window appears as shown in Figure 12-13.

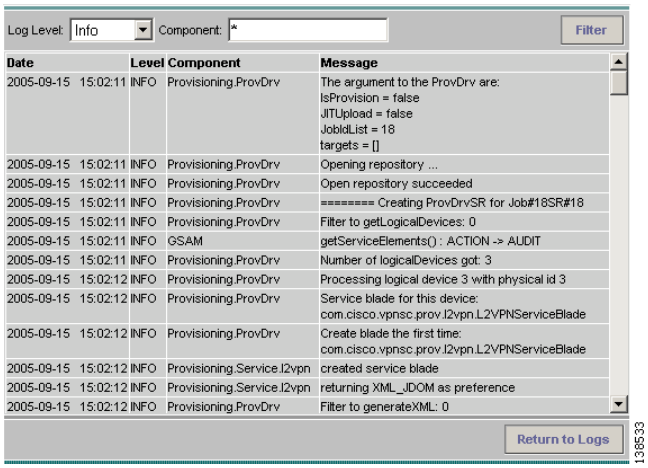
Figure 12-13 Task Logs



Step 4 Select the run-time task that you want to monitor and click **View Logs**.

A window like the one shown in Figure 12-14 appears.

Figure 12-14 Task Logs



Step 5 Select the log level from the drop-down list and click **Filter**. The log levels are All, Severe, Warning, Info, Config, Fine, Finer, and Finest.

Step 6 Click **Return to Logs**.

Step 7 Click **Close** in the Task Logs window.

Auditing Service Requests

Each time an L2VPN (including L2TPv3) or VPLS service request is deployed in the Cisco IP Solution Center (ISC), a configuration audit occurs. You can view the results of these in L2VPN or VPLS configuration audit reports. Use configuration audits and reports to verify that the network devices have the correct configuration for the services provided.

A functional audit is part of the post-provisioning check. It is only available for L2TPv3 service requests. It lets you validate the L2TPv3 circuit and session status. If the L2TPv3 wire state is functional, it indicates that traffic can be passed through successfully.

Note A functional audit can be performed only after a configuration audit is performed successfully on the service request.

Configuration Audit

A configuration audit occurs automatically each time you deploy an L2VPN or VPLS service request. During this configuration audit, ISC verifies that all Cisco IOS commands are present and that they have the correct syntax. An audit also verifies that there were no errors during deployment.

The configuration audit verifies the service request deployment by examining the commands configured by the L2VPN or VPLS service request on the target devices. If the device configuration does not match what is defined in the service request, the audit flags a warning and sets the service request to a **Failed Audit** or **Lost** state.

You can create audit reports for new or existing L2VPN or VPLS service requests.

- Audit new services—This type of audit is for service requests that have just been deployed. The audit identifies problems with the configuration files downloaded to the devices.
- Audit existing services—This type of audit checks and evaluates the configuration of deployed service requests to see if the service request is still in effect.

We recommend that you schedule a service request audit on a regular basis to verify the state of the network provisioning requests.

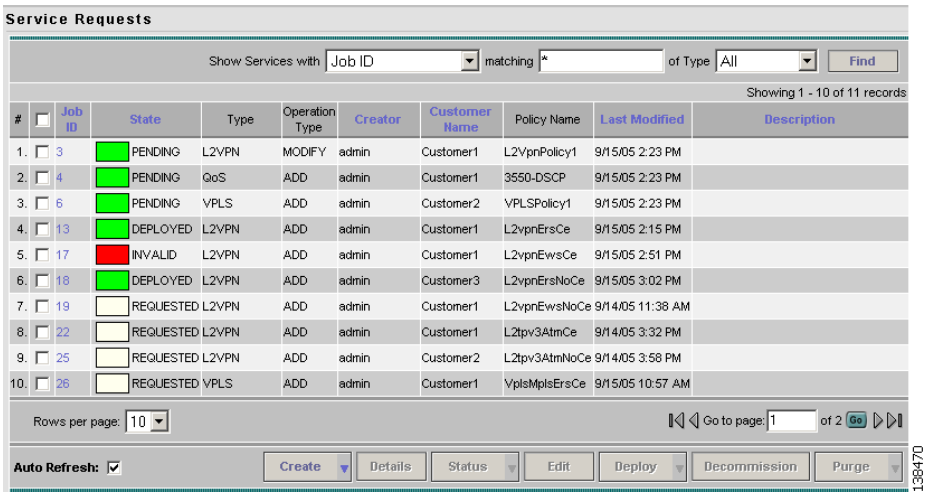
This section describes how to manually generate a configuration audit and view the audit report.

To view a configuration audit report perform the following steps.

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

The Service Requests window appears as shown in Figure 12-15.

Figure 12-15 Service Requests Window



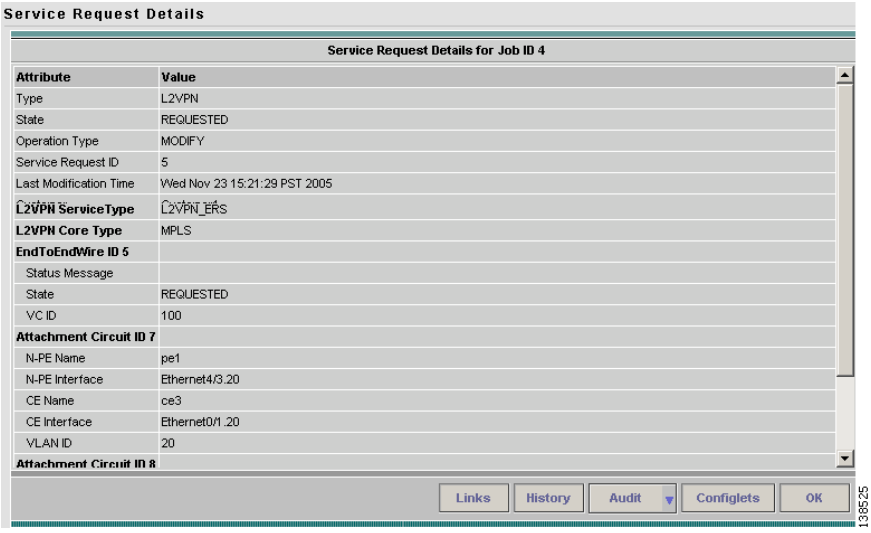
#		Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.		3	PENDING	L2VPN	MODIFY	admin	Customer1	L2VpnPolicy1	9/15/05 2:23 PM	
2.		4	PENDING	QoS	ADD	admin	Customer1	3550-DSCP	9/15/05 2:23 PM	
3.		6	PENDING	VPLS	ADD	admin	Customer2	VPLSPolicy1	9/15/05 2:23 PM	
4.		13	DEPLOYED	L2VPN	ADD	admin	Customer1	L2vpnErsCe	9/15/05 2:15 PM	
5.		17	INVALID	L2VPN	ADD	admin	Customer1	L2vpnEwsCe	9/15/05 2:51 PM	
6.		18	DEPLOYED	L2VPN	ADD	admin	Customer3	L2vpnErsNoCe	9/15/05 3:02 PM	
7.		19	REQUESTED	L2VPN	ADD	admin	Customer1	L2vpnEwsNoCe	9/14/05 11:38 AM	
8.		22	REQUESTED	L2VPN	ADD	admin	Customer1	L2tpv3AtmCe	9/14/05 3:32 PM	
9.		25	REQUESTED	L2VPN	ADD	admin	Customer2	L2tpv3AtmNoCe	9/14/05 3:58 PM	
10.		26	REQUESTED	VPLS	ADD	admin	Customer1	VplsMplsErsCe	9/15/05 10:57 AM	

Step 2 Select an L2VPN or VPLS service request for the configuration audit.

Step 3 Click **Details**.

The Service Request Details window appears as shown in Figure 12-16.

Figure 12-16 Service Request Details

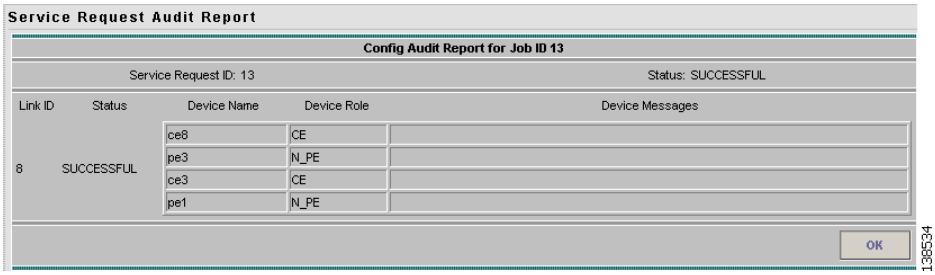


Step 4 Click **Audit**.

Step 5 Click **Config.**

The Service Request Audit window appears. Figure 12-17 shows an example of a successful configuration audit.

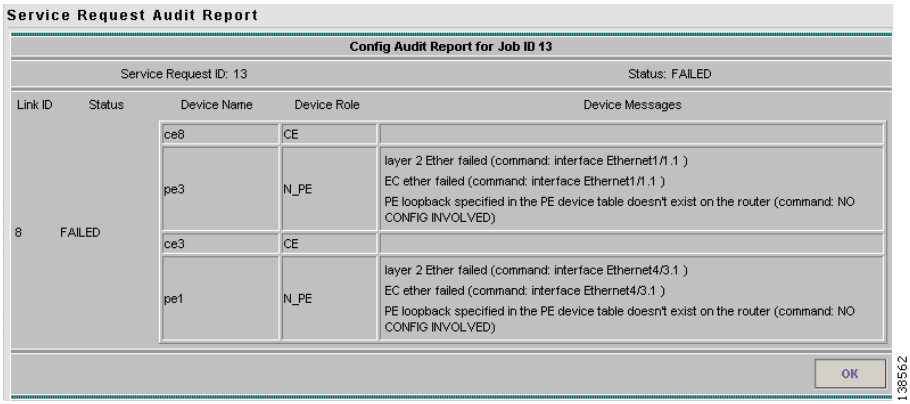
Figure 12-17 Service Request Audit Report—Successful



This window lists the device name and role, and a message regarding the status of your configuration audit.

If the audit is unsuccessful, the message field lists details on the failed audit. Figure 12-18 shows an example of a failed audit message for an L2VPN or VPLS service request.

Figure 12-18 Service Request Audit Report—Failed



The audit failure message indicates missing commands and configuration issues. Carefully review the information in the message field. If the audit fails, you must correct all errors and redeploy the service request.

Step 6 Click **OK** to return to the Service Request Details window.

Functional Audit

A functional audit verifies that the links in a service request or VPN are working correctly. The audit checks that the circuit and session between two PEs are set up correctly to pass traffic through.

Note Functional audits are performed by ISC for only L2TPv3 service requests.

Performing a Functional Audit

You perform a functional audit after a configuration audit is performed successfully. You can perform a functional audit on service requests that have states in either deployed, functional, or broken. Wait at least two minutes after a service is deployed to allow time for the circuit and session to be established. If you prematurely perform a functional audit action, a broken service request state will be the result because the session is not established yet.

To perform a functional audit, follow these steps.

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

Step 2 Select a service request.

Step 3 Click **Details**.

On the service request details page, the **Audit** button has two choices:

- **Config**
- **Functional**

Step 4 Click **Functional** to display the Functional audit report.

Creating a Task to Perform a Functional Audit

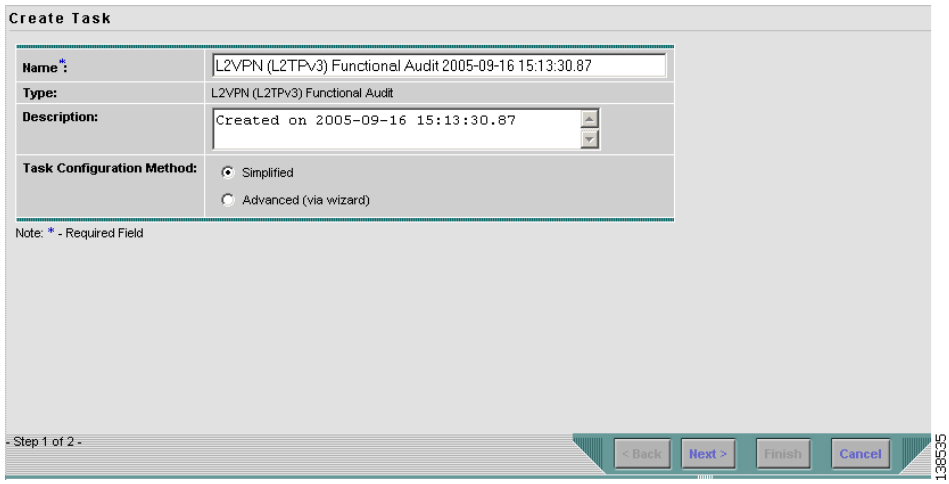
You can create a task to do a functional audit for one or more L2TPv3 service requests. To create a task to do a functional audit, perform the following steps.

Step 1 Select **Monitoring > Task Manager > Tasks.**

Step 2 Click **Audit**

Step 3 Choose **L2VPN (L2TPv3) Functional Audit** from the drop-down list. The create task window appears as shown in Figure 12-19.

Figure 12-19 Create Task



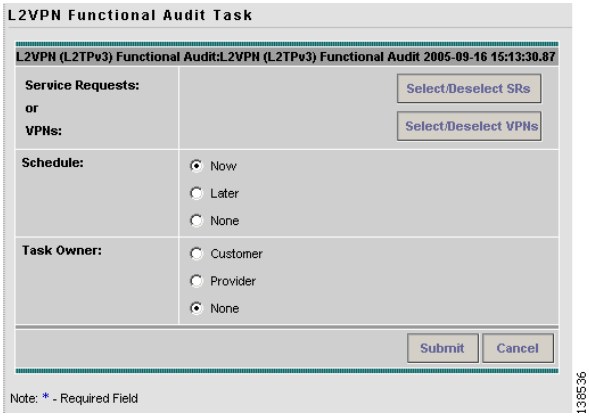
Step 4 Select a Task Configuration method. The choices are:

- **Simplified**
- **Advanced** (via wizard)

Step 5 Click **Next**.

The L2VPN Functional Audit Task window appears as shown in Figure 12-20.

Figure 12-20 L2VPN Functional Audit Task



Step 6 Click the **Select/Deselect SRs** button to select one or more service requests in Deployed, Functional, or Broken states as the targets for the task.

You can select a VPN to audit. If you select a VPN to audit, all the links that form the VPN are audited.

Note You can select either service request(s) or VPN(s) in one task, but you cannot select both in the same task.

Step 7 You can choose to schedule now or later.

Step 8 You can choose an owner for the task.

Step 9 Click **Submit**.

Step 10 You receive a Service Request Audit Report. The service request state is set to Functional if all the end-to-end wires pass the functional audit and Broken if any one of them is broken.

Why a Functional Audit Could Fail

A Functional Audit could fail for the following reasons:

- No session was found for an end-to-end wire.
- A session is not established yet.
- A UNI involved in an end-to-end wire is down.

You can also use the task logs to help you troubleshoot why a service request has failed or to find more details about a service request. It is possible to set the types of log level you want to view. Specify the Log Level and click the **Filter** button to view that information you want to view. See Monitoring Service Requests, page 12-11, for more information.

Setting Up VLAN Translation

This appendix describes how to set up VLAN translation for L2VPN ERS services. It contains the following sections:

Note Review Platform-Specific Usage Notes, page A-6 for helpful information to be aware of before you create policies and services using VLAN translation.

VLAN Translation Overview

VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. There are two types of VLAN translation—one is 1 to 1 translation (1:1), and the other one is 2 to 1 translation (2:1). This feature is available for L2VPN ERS (with and without a CE). Because ISC does not support the Ethernet interface type on L2TPv3 (the IP-based L2VPN service), VLAN translation is not available for L2TPv3. The behavior of L2VPN EWS service remains the same even though it is true that it ia possible now for one Q-in-Q port to be shared by both EWS and ERS service. VLAN translation is only for an Ethernet interface, not for other types of interfaces, such as ATM and Frame Relay.

With 1:1 VLAN translation, the VLAN of the incoming traffic (CE VLAN) is replaced by another VLAN (PE VLAN). It means the SP is now able to handle the situation where incoming traffic from two different customers share the same CE VLAN. The SP can map these two CE VLANs to two different PE VLANs, and customer traffic will not be mixed.

With 2:1 VLAN translation, the double tagged (Q-in-Q) traffic at the U-PE UNI port can be mapped to different flows to achieve service multiplexing. The translation is based on the combination of the CE VLAN (inner tag) and the PE VLAN (outer tag). Without this translation, all the traffic from a Q-in-Q port can only go to one place because it is switched only by the outer tag.

Setting Up VLAN Translation

The following sections described how to create and manage policies and service requests to support VLAN translation:

- Creating a Policy, page A-2
- Creating a Service Request, page A-3
- Modifying a Service Request, page A-5
- Deleting a Service Request, page A-6

Creating a Policy

VLAN translation is specified during policy creation for L2VPN for ERS (with and without a CE). The L2VPN (Point to Point) Editor window contains a new option called "VLAN Translation," as shown in Figure A-1.

Figure A-1 VLAN Translation Option in the L2VPN (Point to Point) Editor Window

There are three options for VLAN translation:

- **No**—This is the default choice. No VLAN translation is performed.

  Note If you select **No** and you do not want to deal with any behavior related to VLAN trans during service request creation, then deselect the **Editable** check box. This is the recommendation when you select no VLAN translation.

- **1:1**—1:1 VLAN translation. The VLAN of the incoming traffic (CE VLAN) is replaced by another VLAN (PE VLAN). The specification of the VLAN translation is done during the creation of the service request for the policy, as covered in Creating a Service Request, page A-3.
- **2:1**—2:1 VLAN translation. The double tagged (Q-in-Q) traffic at the U-PE UNI port can be mapped to different flows to achieve service multiplexing. When you select 2:1 VLAN translation, the L2VPN (Point to Point) Editor window dynamically changes to enable you to select where the 2:1 VLAN translation takes place, as shown inFigure A-2.

Figure A-2 Select Where 2:1 VLAN Translation Takes Place

The choices for where 2:1 VLAN translation takes place are:

- **Auto** (This is the default choice.)
- **U-PE**
- **PE-AGG**
- **N-PE**

If you select **Auto**, the 2:1 VLAN translation takes place at the device closest to the UNI port. The other choices come into play only when there is more than one place that 2:1 VLAN translation can be done. If there is only one place where the translation can be done, the choice is ignored.

The actual VLAN values are specified when you create a service request based on this policy. See the Creating a Service Request, page A-3.

Creating a Service Request

When you create a service request based on an L2VPN ERS policy, the VLAN options can be changed if they were set to be editable in the policy. You can overwrite the policy information for the VLAN translation type and the place where translation occurs. This flexibility allows the following provisioning:

- One AC can have 2:1 VLAN translation, while the other AC can have no VLAN translation or 1:1 VLAN translation.
- The VLAN translation for one AC can be on the UNI box, while the translation for the other AC can be on the PE-AGG.

Note Note these modifications can happen only when a new service request is created. They are not allowed during the modification of an existing service request.

The specification of the VLAN translation happens during the creation of the service request within the Link Attributes window. At that point, you can specify which VLAN is translated to which VLAN. The Link Attributes window is accessed after the UNI port is selected on the Attachment Tunnel Editor window. Because you can set the VLAN translation type after the UNI selection, the UNI port display list does not exclude any type for the UNI port. This is because:

- The UNI port list has to include the regular trunk port, in case you later (on the Link Attributes window) decide to perform no VLAN translation or 1:1 VLAN translation.
- The UNI port list has to include an EWS (Q-in-Q) port, in case you decide to do 2:1 VLAN translation.

Even though you have all the ports to start with for VLAN translation, you must select specific types of ports, based on the type of VLAN translation. More specifically:

- For no VLAN translation and 1:1 VLAN translation, you must select an empty port or a trunk port as the UNI.
- For 2:1VLAN translation, you must select an empty port or a Q-in-Q port as the UNI port.

To help determine the proper port to use, you can click the **Details** button on the Attachment Tunnel Editor window to display the port type and associated service with that port.

The following sections show how the VLAN translation is defined on the Link Attribute window for the different types of VLAN translation.

No VLAN Translation

When you choose no VLAN translation, no additional information needs to be provided.

1:1 VLAN Translation

When you choose 1:1 VLAN translation, the window dynamically changes, as shown in Figure A-3.

Figure A-3 CE VLAN to be Translated From

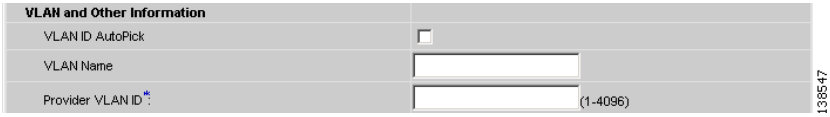
In the empty field, you must enter which CE VLAN is to be translated from. The VLAN number must be a number from 1 to 4096.

The PE VLAN that the CE VLAN is to be translated can be "auto picked" or manually entered. Select the **VLAN ID AutoPick** check box above (on the Link Attributes window), as shown in Figure A-4, to have PE VLAN automatically assigned.

Figure A-4 Automatic Selection of the PE VLAN

If you deselect the **VLAN ID AutoPick** check box, as shown in Figure A-5, the window displays a Provider VLAN ID, where you can manually enter the PE VLAN.

Figure A-5 Manual Selection of the PE VLAN

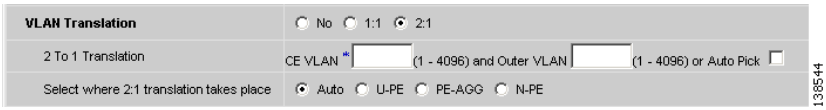


Upon completion of the service request creation, ISC does an integrity check before saving the service request. For 1:1 VLAN translation, ISC rejects the service request if the CE VLAN has been used for another 1:1 VLAN translation on the same port.

2:1 VLAN Translation

When choosing 2:1 VLAN translation, the window dynamically changes, as shown in Figure A-6.

Figure A-6 2:1 VLAN Translation Window



Note If the UNI port has been provisioned with EWS service, the outer VLAN value is grayed out, as shown in Figure A-7.

Figure A-7 2:1 VLAN Translation with Outer VLAN Grayed Out

In 2:1 VLAN translation, there are three VLANs involved:

- "A"—The CE VLAN to be translated from. You specify this in the "From CE VLAN field." For out-of-range translation, a value of "*" (asterisk character) should be provided
- "B"—The PE VLAN that is the outer VLAN of the Q-in-Q port. You specify this in the "Outer VLAN" field. You can select this VLAN manually by entering a value, or you can select the **AutoPick** check box to have one automatically assigned.
- "C"—The PE VLAN that the "A" and "B" VLANs are translated to. You specify this in the "VLAN and Other Information" section above (on the Link Attributes window). See Figure A-4 and Figure A-5 in 1:1 VLAN Translation, page A-4.

You must specify VLAN "A" (the CE VLAN) and VLAN "C" (the PE VLAN translated to). For VLAN "B" (the Q-in-Q outer VLAN), what to specify depends on the UNI port type:

- If it is an empty port, you must specify VLAN "B."
- If it is an existing Q-in-Q port, then VLAN "B" has been defined, and it cannot be changed at this point.

Some additional comments on 2:1 VLAN translation:

- For 2:1 VLAN translation, if you build an ERS service on an empty port, then this UNI port will be provisioned as an ERS service. If you later add an EWS service to the same port, the EWS service will overwrite the previous ERS provisioning. The major difference between ERS and EWS is the L2PT BPDU treatment. For ERS, BPDU is blocked. For EWS, BPDU is tunneled.
- As an ERS service, the 2:1 VLAN translation can share the same port, just like a regular ERS port.
- An ERS 2:1 service can be added on top of an existing EWS service.

Upon completion of the service request creation, ISC does an integrity check before saving the service request. For 2:1 VLAN translation, ISC rejects the service request if the CE VLAN and outer tag PE VLAN combination has been used for another 2:1 VLAN translation on the same port.

Modifying a Service Request

For both 1:1 and 2:1 VLAN translation, you can perform the following modifications on an existing service request:

- Change to a new CE VLAN to be translated from.
- All other normal changes for a service request are permitted.

However, the following modifications are not allowed:

- You cannot change the VLAN translation type for a given AC. For instance, you cannot change from 2:1 to 1:1 VLAN translation.
- You cannot change the place where 2:1 VLAN translation occurs.

Deleting a Service Request

During service request deletion, the following resources are released:

For 1:1VLAN translation:

- The CE VLAN becomes available to be translated again.
- The PE VLAN is released.
- If the link being deleted is the last link on the UNI port, then this port is set to new.

For 2:1 VLAN translation:

- The CE VLAN becomes available to be translated again.
- The “translated to” PE VLAN is released.
- If the link being deleted is the last “CE-PE” pair on this UNI port, and there is no EWS service on this port, then this port is set to new. In addition, the outer VLAN is released.

Platform-Specific Usage Notes

VLAN translation is available on 7600 and 3750 ME platforms. The 7600 and 3750 ME have different ways to support VLAN translation. Not only is the command syntax different, but so is the place where the VLAN translation is carried out. On the 7600, for 1:1 VLAN translation, the operation is done on the PFC card. For 2:1 VLAN translation, the operation is done on the uplink GE-WAN (OSM module). On the 3750 ME, however, both translations occur on the uplinks (ES ports).

VLAN Translation on the 3750

Be aware of the following points when performing VLAN translation on the 3750.

- The 3750 where VLAN translation occurs should be designated as a U-PE or PE-AGG role, not N-PE.
- VLAN translation on the up link (ES) port should be performed on the Gigabit 1/1/1 or Gigabit 1/1/2 port.
- If a 1:1 VLAN translation occurs on a ring that is made of 3750 PEs, all the 3750s use the ES port as uplink ports (the “east and west” ports) to connect other ring nodes.

VLAN Translation on the 7600

Be aware of the following points when performing VLAN translation on the 7600.

- 1:1 VLAN translation always occurs on the UNI port. However, not every Ethernet interface will support 1:1 VLAN translation. Such support is dependent on the line card.
- 2:1 VLAN translation always occurs on the GE-WAN port. The port must be an NNI uplink port.
- 2:1 VLAN translation only occurs on a 7600 that is a U-PE or a PE-AGG, not an N-PE. The reason is when the 2:1 VLAN translation is performed on the GE-WAN interface, this interface can no longer perform L3VPN and L2VPN service using the translated new VLAN. The L3/L2VPN service has to be provisioned on another (N-PE) box.

Failed Service Requests When Hardware Does Not Support VLAN Translation

For the 1:1 VLAN translation feature, a service request goes to the **Fail Deployed** state if the target hardware (line card) does not support the VLAN translation. The reason the service request goes to the **Fail Deployed** state instead of **Invalid** is that ISC does not know beforehand whether a particular line card will accept or reject the VLAN translation CLI commands. In this case, ISC attempts to push down the commands and the deployment fails. An **Invalid** status means ISC detects something wrong (in advance) and aborts the provisioning task. No CLI is pushed down in that case. This is a general behavior of ISC when a given hardware does not support a feature. In these cases, it is the user's responsibility to select proper hardware to support the intended service.

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

V

W